Indian Journal of Advancd Research in Electrical, Electronics
and Instumentation Engineering (IJAREEIE)
Vol.2.No.1 2014 pp 12-16.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

CERTIFIED SECURE STORAGE SERVICES FOR OUTSOURCED DATA IN CLOUD

Blessty Sweetline T[1],SathiyaPriya K[2]
CSE Department, SRM University
[1]bsweet.sweetline@gmail.com [2]sathiyapriya.k@ktr.srmuniv.ac.in

ABSTRACT:

Cloud computing is all over the world and presents animperative value proposition for its end users. However issues like privacy and security are still grey areas when it comes to public cloud. In order to secure the data in the cloud, auditing mechanisms have been schemed earlier but such storages are still vulnerable to impersonation attacks by Fraudulent Cloud Service Providers. It is necessary to ensure that the data are in safe hands. This paper proposes a Certified Secure Service for the storage of outsourced data in the cloud by using a Certificate Authority to verify the Cloud Service Providers and also by presenting Third-Party Dynamic Auditing for the data in the storage. Thereby the service ensures combined security for the data placed in the outsourced storages,protecting the data in the storage as well as during the process of outsourcing.

Keywords- Certified Secure Service, Third-Party Dynamic Auditing, Fraudulent Cloud Service Providers

1. INTRODUCTION

Various distinct technologies are combined to build cloud computing systems and securing all components of a typical cloud is a complex job. Security is the top concern for cloud users and it is the one of the issues that need to be addressed in order to allow faster growth of cloud computing. This paper focusses security towards one of the cloud services called Storage-As-A-Service(StaaS). StaaS corresponds to the physical storage centres or to the databases which store information.Data security is of deliberate concern because of the following reasons unearthed. Firstly, the end user's data is being stored in infrastructures which might be vulnerable to attacks affecting the integrity of data. Secondly user's data are provided to a Cloud Service Providers(CSP) whomay have some responsibility for handling the information safely but not all.

In order to secure the data in the cloud,dynamic auditing allowing security to ensure data integrity and data privacy have been formulated. But previous systems have been focussed only on providing security for the data that is outsourced. The approaches do not focus in protecting the data from falling in the hands of an impersonator. Hence the Certified Secure Storage Service is an approach toward a holistic defended storage system for the outsourced data.

2. RELATED WORK

Learning from the previous works as described in [7], this paper considers the following techniques to extract a strong approach for securing the outsourced data. To make certain that the results returned for a query by a server are correct and complete, Xie et al. proposed Query integrity[4] so that instead of auditing results sent by the server, a small amount of records can be inserted automatically into the database and an audit can be carried by analysing the inserted records in the query results. Integrity auditing uses deterministic functions to embed fake tuples in the outsourced data. Yet the approach introduces query overhead at the server side as the additional fake tuples need to be processed.

Blind Aggregate Forward (BAF) [1] provides security for audit logs. Audit logs require forward security i.e. attacker cannot forge log entries accumulated before compromise. BAF does not depend on online trusted third party support and yields publicly verifiable forward secure and aggregate signatures with low or near zero computational costs. BAF is a classic solution for secure logging but BAF does not apply the time factor to be publicly verifiable, and eventually achieves limited verification.

To provide publicly verifiable system, Ateniese et al. proposed a model [6] that generates probabilistic proofs of possession by sampling random sets of blocks from the server thereby reducing I/O costs. It is the responsibility of the client to make sure that the data in the server is genuine.The verification is done without retrieving the data to the client side but this approach requires the server to access the entire file, which is not feasible when dealing with enormous amounts of data.

Efficient Provable Data Possession [3] proposed by Zhu et al. is a cooperative PDP scheme in hybrid clouds to meet the needs of scalability for service and data migration.Taking into consideration the existence of cloud service providers to cooperatively store and maintain the client's data, the need to download data is avoided. The overheads are reduced when the values of optimal value are increased. But it is mandatory to select the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers and this imposes a difficulty as it is critical to select the number of sectors for each and every block.

Another method introduces an effective Third Party Auditor (TPA) for auditing data in the cloud. Thisapproach is used so that the end users are relieved from performing the audit in the system [5]. The public auditor checks both the integrity of the data file and the server's possession of a previously committed decryption key. Public Key based Homomorphic Linear Authenticator (HLA) scheme is used. Scheme involves privacy-preserving auditing protocol and batch auditing. This scheme works for encrypted files alone and is at the disadvantage of requiring auditor statefulness and bounded usage, which possibly brings anonline burden to users when the keyed hashes are used up.

A dynamic audit system[2] was also proposed for providing auditing with support for dynamic operations from the client side and protocols are provided to ensure data integrity and privacy, but the system is still vulnerable to attacks and does not adhere to security during the process of outsourcing. Hence it is essential that the systems developed provide security for the data from internal and external attacks.

3. PROPOSED SYSTEM

As listed in the previous section of related works, the systems existing are focussed on single point security issue of protecting data that is in the outsourced storage. As a result if the security of the data is provided, privacy is compromised or if both are ensured then the system is vulnerable to attacks from outsiders. Thus the system proposed in this paper is an integrated design using Third-Party dynamic auditing along with a certifying method for shielding the data against impersonation attacks.

Dynamic audit service [2] is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. It supports dynamic data operations and timely anomaly detection using fragment structure, random sampling, and index-hash table (IHT). Also an interactive proof system (IPS) with the zero knowledge property is introduced to provide public auditability without downloading raw data and protect privacy of the data. Data owner stores the large number of data in cloud after encrypting the data with private key and sends public key to third party auditor (TPA) for auditing purpose. TPA is in clouds and maintained by a CSP. An Authorized Application (AA), who holds a data owners secret key (sk), manipulates the outsourced data and updates the associated IHT stored in TPA.

Cloud users access the services through the AA. Auditing is to secure the outsourced storage against data anomalies and to keep the data updated. The certification is to certify the Cloud Service Provider so that the CSP is the right authority for holding the data.

A. Key and Tag Generation

In the invoke of the Key Generation operation, a private key(sk) and a public key(pk) are generated for the client or Data Owner. RSA algorithm is used to generate the keys. The Data owner uploads the data or file which is pre-processed using the secret key (sk) into fragments to form a fragment table. Using the fragment table and the secret key in the TagGen Algorithm as in [2], the Public Verifiable Parameters (PVPs) and tags are generated. The PVPs are given to the Third Party Auditor and the Tags to the CSP.

B. Auditing

Security audit is an important solution enabling trace- back and analysis of any activities including data accesses, security breaches, application activities, and so on. 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 easier and affordable way for the users to ensure their storage correctness in the cloud.

Moreover, 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. 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.

Auditing involves verification of the data at the CSP's server by the TPA and checking of the data to assure if it is correct and for timely anomaly detection. TPA issues a "random sampling" challenge[2] to audit the integrity and availability of the outsourced data in terms of verification information involving PVP and (IHT) stored in TPA through an Interactive proof protocol of Retrievability.

C. *Dynamic Data Operations*

Authorized Applications (AA) are allowed to update, insert or delete blocks of a file using the algorithm for dynamic operations based on the scheme proposed by Yan Zhu et. Al[2]. Dynamic data operations are accompanied by dynamic and a periodic auditing performing audit for the modified file.

D. *Replay Attack*

A replay attack also known as a "man-in-the-middle attack," is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. It is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. For example, messages from an authorized user who is logging into a network may be captured by an attacker and resent (replayed) the next day. Even though the messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid logon messages is sufficient to gain access into the network as a legitimate user.

4. SYSTEM ARCHITECTURE

The architecture for certified secure storage service as shown in Fig 1.1 explains the entities and their functionality in the cloud. A Data Owner (DO) uploads a file to the cloud. A Third Party Auditor (TPA) audits the file through dynamic audit services. An Authorised Application (AA) server in the cloud provides the interface to access the data for a client. Name servers hold the data provided to the cloud by the Cloud Service Provider (CSP). A legitimate CSP who is impersonated by a fraudulent CSP is prevented from accessing data in the cloud. A Certificate Authority is introduced to provide authentication for the CSPs and replay attack is prevented. This system ensures security for the data stored in the cloud through dynamic auditing as well as protects data from being accessed by malicious CSP.

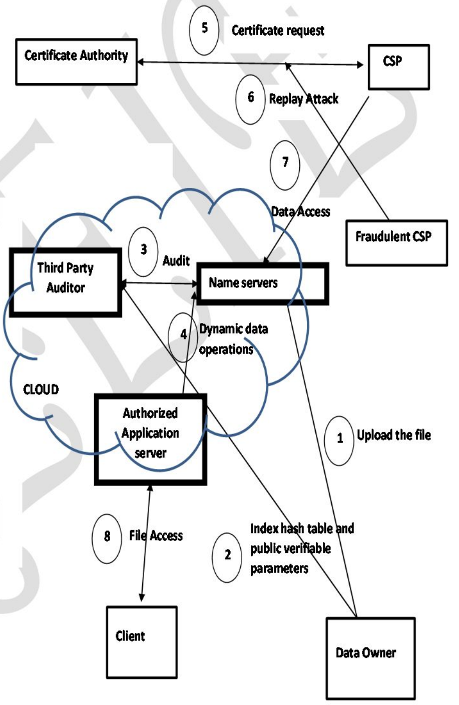


Figure 1 – Certified Secure Storage Service Architecture

5. PROPOSED SYSTEM FORMULATION AND MODULES

A. *File Updation*

An outsourced file from a Data Owner is split into 'n' blocks $\{m_1,m_2,\ldots.\ m_n\}$ with each block m_i split into 's' sectors$\{m_{i.1},m_{i.2},\ldots.,m_{i.s}\}$. The fragment structure as shown in Fig 4, consists of n block-tag pair (m_i,σ_i) where $\sigma_i$is a signature tag of a block 'm'generated by some secrets $\tau = (\tau_1,\tau_2\ldots..,\tau_s)$[Referred also as PVP]. Periodic sampling checking is done to avoid whole checking and to detect anomaly detection in timely manner. The fragment table as shown in Fig 4 provides probabilistic audit as well: Given a randomly chosen challenge (or query) Q= {(i,vi)}i€I, where I is a subset of the block indices and vi is a random coefficient, an efficient algorithm is used to produce a constant-size response (µ1, µ2,….. µs, σ') where µi comes from all {mk.i,vk} k€I and σ' is from all{ σk, vk} k€I..

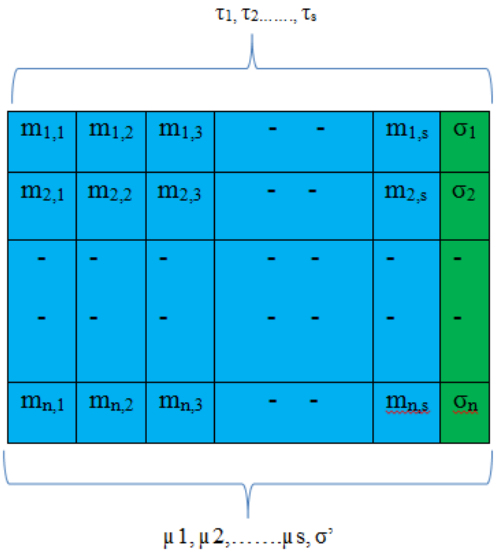
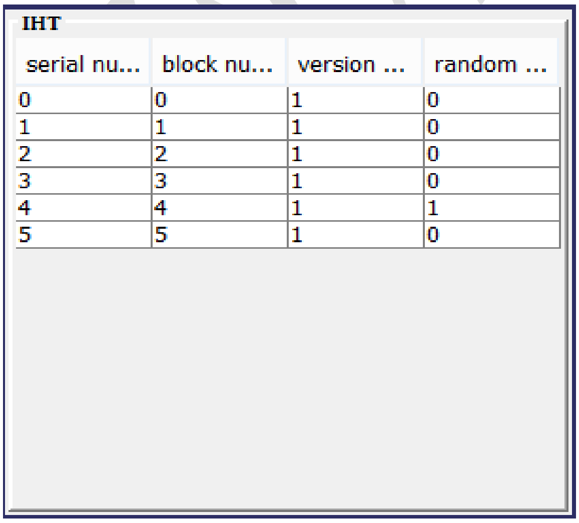

τ1, τ2……., τs
m1,1 m1,2 m1,3 - - m1,s σ1
m2,1 m2,2 m2,3 - - m2,s σ2
- - - - - - -
- - - - - - -
mn,1 mn,2 mn,3 - - mn,s σn
µ 1, µ 2,…….µ s, σ'

Figure 2 Fragment Structure

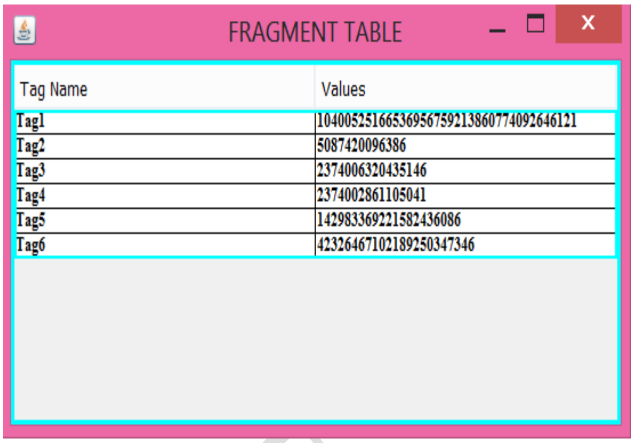
Another structure is the Index Hash Table as shown in Fig 3. Index Hash Table contains four columns for serial number, block number, version number and random integer. As the data dynamically changes, each record of the IHT is used to produce a hash value which in turn is used for developing the signature tag $\sigma_i$by the secret key sk.

Block-tag pairs and PVPs as shown in Fig 5, are stored in CSP and TPA respectively. MAC based or RSA schemes are used for convergence of s blocks to generate secure signature tag.


IHT

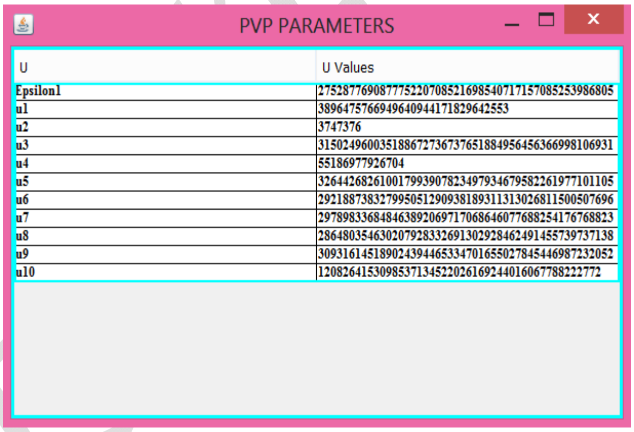
serial nu...	block nu...	version ...	random ...
0	0	1	0
1	1	1	0
2	2	1	0
3	3	1	0
4	4	1	1
5	5	1	0

Figure 3 – Index Hash Table


FRAGMENT TABLE

Tag Name	Values
Tag1	10400525166536956759213860774092646121
Tag2	5087420096386
Tag3	2374006320435146
Tag4	2374002861105041
Tag5	142983369221582436086
Tag6	42326467102189250347346

Figure 4 – Fragment Table


PVP PARAMETERS

U	U Values
Epsilon1	275287769087775220708521698540717157085253986805
u1	3896475766949640944171829642553
u2	3747376
u3	315024960035188672736737651884956456366998106931
u4	55186977926704
u5	326442682610017993907823497934679582261977101105
u6	292188738327995051290938189311313026811500507696
u7	297898336848463892069717068646077688254176768823
u8	286480354630207928332691302928462491455739737138
u9	309316145189024394465334701655027845446987232052
u10	12082641530985371345220261692440160677882222772

Figure 5 – PVP Parameters

B. *Periodic Auditing*

Once the data owner has uploaded the file in the cloud, the TPA checks the integrity of the uploaded file anytime. Thus the 3-move interactive proof protocol [2] is used among the TPA and cloud service provider for auditing purpose. 3- Move interactive protocols are commitment, challenge and response. At first the TPA queries the CSP for the verification process and initializes the interactive proof protocol. The cloud service provider selects some set of the random keys and random blocks and sends it the TPA using the commitment protocol. Next the TPA chooses some set of secret keys and blocks and sends them to the CSP by using the challenge protocol. After which cloud service provider calculates the response and sends it to the TPA. The verifier TPA checks whether the response is correct. By doing so the auditing is performed among the CSP and TPA.

C. *Dynamic Data Operations*

Dynamic data operations are handled among the data owner and authorized application server. The dynamic operations are handled in blocks. Data owner will send the request to the Authorized Application server to modify the file. Upon receiving the modification information, AA also receives the public verifiable parameter from the TPA. Then the AA calls the Insert, Delete and Update algorithm to modify the file. The modified file is sent to the TPA and CSP in order to verify the validity. After receiving the modified file, CSP will invoke the check algorithm [2]. It verifies the update or insert or delete operations based on the update, insert and delete algorithms [2]. Finally the verification information is sent to the TPA. It modifies the audit record after the confirmation message from the CSP.

D. Certificate Authentication

When the cloud service provider accesses the data in the cloud, the CSP has to get the certificate from the certificate authority. An attacker may intercept messages during the authentication of a service provider with the certificate authority, and replay the messages in order to masquerade as a legitimate service provider. There are two points in time that the attacker can replay the messages. One is after the actual service provider has completely disconnected and ended a session with the certificate authority. The other is when the actual service provider is disconnected but the session is not over, so the attacker may try to renegotiate the connection. The first type of attack will not succeed since the certificate typically has a time stamp which will become obsolete at the time point of reuse. The second type of attack will also fail since renegotiation is banned in the latest version of cryptographic checks that have been added. Certificate Authority issues

- Timestamp or nonce

This helps to generate a synchronization mechanism b/w the message requester and receiver. Current clock time plus a message authentication code (MAC) together forms the time stamp.

- Session tokens

Tokens are based on a hash generated to be used once during the session. This avoids future tries using the same token. Algorithm for hash key generation can be MD5 or SHA-1.

6. RESULTS AND DISCUSSION

The paper presents a defended system for outsourced storages against impersonation attacks by an outsider in addition to an audit system for protection of the cloud data from the unfaithful behaviour of the CSP. Certified Secure Storage Service as put forth in this paper enhances security in the phase of protection for data stored in the cloud and while presenting data to the Cloud Service Provider. The service keeps the user free from the burden of assuming that the CSP is legitimate and instead certifies that the CSP is indeed legitimate. The system is a combinatory solution addressing some of the major security issues enabling cloud service providers to inculcatedata integrity, data privacy and authenticated servicingin the storage services they provide.

7. FUTURE ENHANCEMENTS

The solution proposed can be built into stronger versions by implementing protection mechanisms against various possible unresolved network attacks that might be a threat to the security of cloud storages.

REFERENCES

[1]A.A. Yavuz and P. Ning, *“BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems,”* Proc. Ann.Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.

[2] Yan Zhu, Gail-JoonAhn, Hongxin Hu, S. S. Yau, H. G. An, Chang-Jun Hu, *"Dynamic Audit Services for Outsourced Storages in Clouds,"* IEEE Transactions on Services Computing , vol. 6, no. 2, pp. 227-238, April-June 2013, doi:10.1109/TSC.2011.51.

[3].Zhu.Y, Wang.H, Hu.Z, Ahn.G-H, Hu.H, and Yau.S.S, *“Efficient Provable Data Possession for Hybrid Clouds,”* Proceedings of the 17th ACM Conference on Computer and Communication Security, pp. 756-758, 2010.

[4] Xie.M, Wang.H, Yin.J and Meng.X, *“Integrity Auditing of Outsourced Data”* Proceedings of the 33rd International Conference on Very Large Databases (VLDB), pp. 782-793, 2007.

[5] Wang.C, Wang.Q, Ren.K and Lou.W, *“Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”* Proceedings of the IEEE INFOCOM, pp. 1-9, 2010.

[6] Ateniese.G, Burns.R.C, Curtmola.R, Herring.J, Kissner.L, Peterson.Z.N.J, and Song.D.X, *“Provable Data Possession at Untrusted Stores,”* Proceedings of the 14th ACM Conference on Computer and Communication Security, pp. 598-609, 2007.

[7] Blessty Sweetline.T *“Survey On Securing Outsourced Storages In Cloud”*, International Journal of Research in Engineering and Technology(IJRET), eISSN: 2319-1163 | pISSN: 2321-7308, Vol 3, Issue 1,2014, pp 175-177.