International Journal of Computer Applications Technology and Research
Volume 3– Issue 2, 100 - 104, 2014, ISSN: 2319–8656

Insuring Security for Outsourced Data Stored in Cloud Environment

Durga Priya.G
Department of Information Technology
Sri Sairam Engineering College
Chennai-45, India

Soma Prathibha
Department of Information Technology,
Sri Sairam Engineering College
Chennai-45, India

Abstract -- The *cloud* storage offers users with infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. Inspite of these advantageous factors, there are several deterrents to the widespread adoption of cloud computing remain. Among them, security towards the correctness of the outsourced data and issues of privacy lead a major role. In order to avoid security risk for the outsourced data, we propose the dynamic audit services that enables integrity verification of untrusted and outsourced storages. 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. In the proposed system data owner stores the large number of data in cloud after e encrypting the data with private key and also send public key to third party auditor (TPA) for auditing purpose. TPA in clouds and it's maintained by CSP. An Authorized Application (AA), which holds a data owners secret key (sk) and manipulate the outsourced data and update the associated IHT stored in TPA. Finally Cloud users access the services through the AA. Our system also provides secure auditing while the data owner outsourcing the data in the cloud. And after performing auditing operations, security solutions are enhanced for the purpose of detecting malicious users with the help of Certificate Authority.

Keywords : Data Security, Certificate Authority, Audit service, Cloud storage, Dynamic operations, Data verification.

1. INTRODUCTION

CLOUD Computing is generally a virtual servers available over the Internet.According to NIST[14], CLOUD computing can be defined as "It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models." Services[14] of cloud computing are 1.SaaS(Software as a Service), 2.PaaS(Platform as a Service), and 3.IaaS (Infrastructure as a Service). *SaaS*: run on distant computers "in the cloud" that are owned and operated by others and that connect to users' computers via the Internet and, usually, a web browser. *PaaS*: provides a cloud-based environment with everything required to support the complete life cycle of building and delivering web-based (cloud) applications—without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting.

IaaS: provides companies with computing resources including servers, networking, storage, and data centre space on a pay-per-use basis.

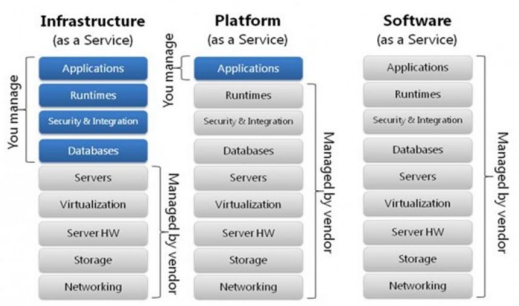


Figure 1: Cloud Services[13]

Cloud Computing has three Deployment models. They are Public cloud, Private cloud, and Hybrid cloud. *Public clouds* are owned by companies and users don't need to purchase hardware, software which are owned and managed by providers. *Private clouds* are owned by single company and take advantage of many of cloud's efficiencies, while providing more control of resources and steering clear of multi-tenancy. *Hybrid cloud:* uses a private cloud foundation combined with the strategic use of public cloud services.

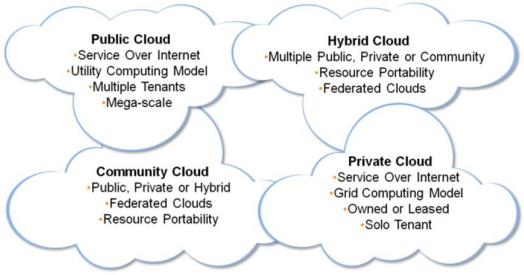


Figure 2: Deployment models[13]

Among these deployment strategies, the public clouds face a huge drawback, which is called to be as security issue. The issues are threats to data, loss of data integrity, confidentiality, and reliability and so on. These are the hindrances that stop the growth of cloud computing technology. This occurs in public cloud because, entities like Cloud Service Provider (CSP), Third Party Auditor (TPA) are involved which may act disloyally to the data's in the cloud. For example, to increase the profit margin by reducing cost, it is possible for CSP to discard rarely accessed data without being detected in a timely fashion. Similarly, CSP may even attempt to hide data loss incidents so as to maintain a reputation. Therefore, although outsourcing data into the cloud is economically for the cost and complexity of long-term large-scale data storage, it's lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud user. In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. However, the fact that users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional cryptographic primitives for the purpose of data integrity protection. Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files. The cloud computing is deployed by data centres running in a simultaneous, cooperated and distributed manner. Hence ensuring security for outsourced data in cloud is the most important task of all.

2.RELATED WORK

Many mechanisms have been proposed to ensure the security of cloud users and for their data. Yet once the malicious users acquire the security credentials they can pose as genuine users and hack the data**.** In this section, will discuss about the work carried out in the area of cloud security. In [1] Dynamic audit sources provide the user with performance of the audit services but it doesn't make an effort to verify if the user is genuine or not. Though privacy preserving [2] works more efficiently but it's only for encrypted files. The effectiveness of this lies in the hands of auditors, whose statefulness must not affect it, also the limited number of auditors matter. A random spot verification mechanism is developed in [3], which correctly identifies where there has been modification and it is efficiently resilient to changes and malicious attacks. But the inefficiency largely attractive is attributed to the randomness. If an identity based mechanism is used [4], can avoid key revocation and key escrow problems but other types of problems are not concentrated here. While building PDP technique on [6] symmetric key, it will considerably reduce the cost and bulk encryption but it is not very safe when it comes to public users. And can considerably try to provide security by auditing the data [7] which is inserted, it overloads the client side as all the auditing is done there. Hence this is useful for smaller data insertions. This can also be implemented by creating probabilistic proofs of data possessed[8] , this way the user can be sure of the data he has uploaded and the data that has been retrieved. This approach's efficiency is reduced by the large volume of data loaded and verified.

3.PROPOSED WORK

Audit service is constructed based on the techniques, fragment structure[1], random sampling[1], and index-hash table[1], supporting provable updates to outsourced data and timely anomaly detection. Also propose a method based on probabilistic query and periodic verification for

improving the performance of audit services. Security solutions also introduced to avoid the malicious users while outsourcing in the cloud. Audit system can support dynamic data operations[1] and timely anomaly detection[1]. Security is provided for dynamic data operations and detects the malicious cloud service provider, when accessing the data in the cloud. We also Detect the malicious identity while the data owner outsourcing in the cloud. First the data centres are configured and then while outsourcing the data onto cloud, authentication for data owner is performed. After performing this verification, a file that has to be uploaded is chosen. From the selected file, we generate Public Verifiable Parameters (PVP), Index Hash Table (IHT), and Tags. PVP and IHT are sent to TPA and Tags are sent to CSP for security purpose. Once the data owner uploads the file in the cloud, the TPA is checking the integrity of the uploaded file at any time.

Table 1: Index Hash Table[1]

No.	B_i	V_i	R_i
0	0	0	0
1	1	2	r'_1
2	2	1	r_2
3	4	1	r_3
4	5	1	r_5
5	5	2	r'_5
...	...	...	...
n	n	1	r_n
n+1	n+1	1	r_{n+1}

Thus the 3-move interactive proof protocol is used among the TPA and cloud service provider for the auditing purpose. 3- Move interactive protocols are commitment, challenge and response.

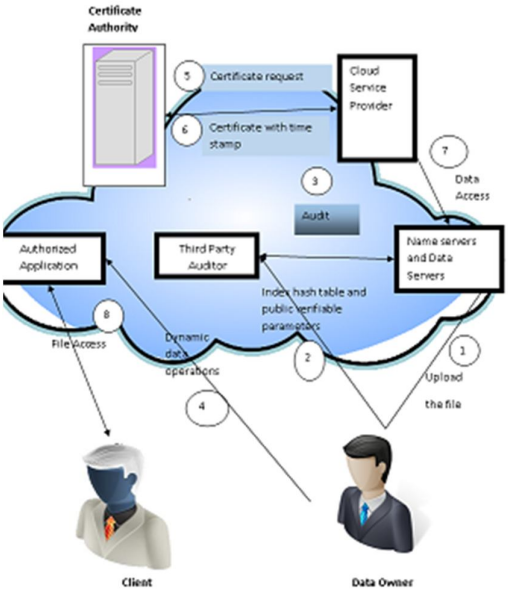


Figure 3: System Architecture

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 random keys and random blocks and sent it the TPA using the commitment protocol. Next the TPA chooses some set of secret keys and blocks and sends to the CSP by using the challenge protocol. After which cloud service provider calculates the response and send to the TPA. The verifier TPA checks whether the response is correct. By doing so the auditing is performed among the CSP and TPA.

3.1 KeyGen(1^k)[1]:

1.Bilinear map group system=(p,G,G_T ,e)
2.Collision resistant hash function= H_k
3.chooses a random $\alpha,\beta \in_R Z_p$ and computes $H_1 = h^{\alpha}$ and $H_2 = h^{\beta} \in G$.

3.2 TagGen(sk,F)[1]:

1.Splits the file F into n×s sectors
2.chooses s random $\tau_{1, \ldots} \tau_s \in Z_p$ (secret of the file)
3.computes $u_i = g^{\tau i} \in G$ and $\xi^{(1)} = H_{\xi}$ ("Fn")
4.where $\xi=\Sigma^s_{i=1} \tau_i$ and Fn is the filename.
5.Finally sets $u=(\xi^{(1),} u_1 ,\ldots, u_s)$ and outputs $\psi=(u, \chi)$ where χ is the index hash table.

4.IMPLEMENTATION

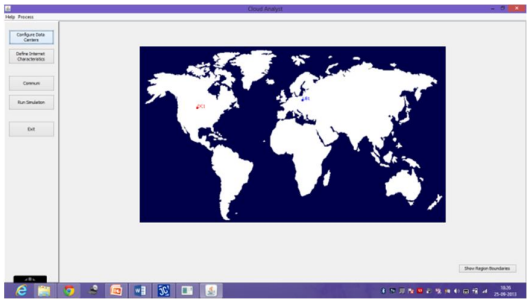
This system is implemented in CLOUD ANALYST. CloudAnalyst[14] is a framework which enables seamless modelling, simulation and experimenting on designing Cloud computing infrastructures.

CloudAnalyst is a self-contained platform which can be used to model data centres, service brokers, scheduling and allocation policies of a large scaled Cloud platform.

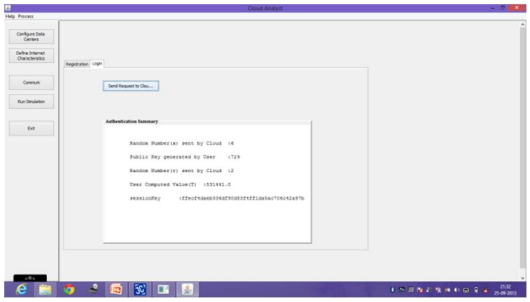
It provides a virtualization engine with extensive features for modelling the creation and life cycle management of virtual engines in a data centre. The CloudAnalyst is built directly on top of CloudSim framework leveraging the features of the original framework and extending some of the capabilities of CloudSim.

The modules are developed using Java in JCreator which is a Java IDE. This interface is similar to that of Microsoft Visual Studio.

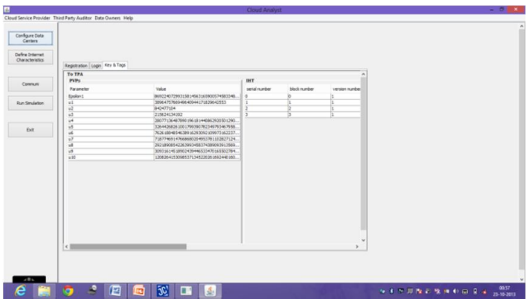
a. It depicts the configuration of data centres.
b. Data Owners identity is authenticated with the help of secret key and public key.
c. Index Hash Table and Public Verifiable Parameters are generated and sent to Third Party Auditor
d. Commitment is performed between CSP and TPA. This action is initiated by CSP
e. Response is sent to CSP from TPA.
f. After performing Check operation, Auditing was completed.



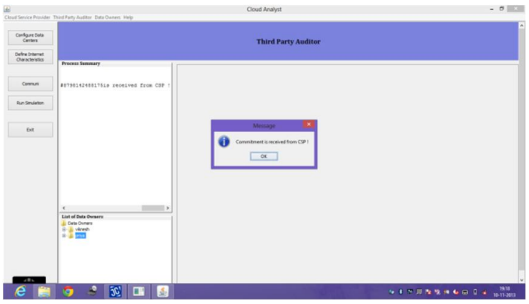
a. Data Centres in Cloud Analyst



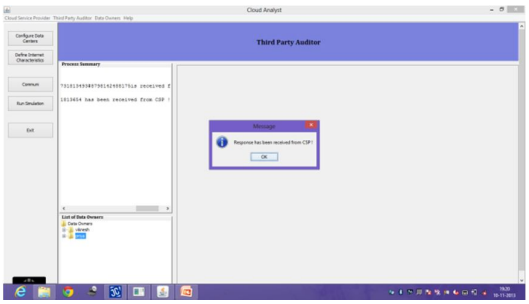
b. Authentication of Data Owner



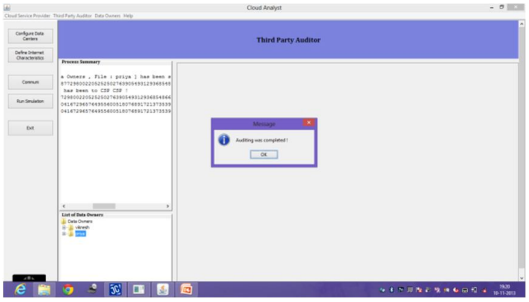
c. Generating PVP and IHT



d. Commitment- Auditing Services



e. Response- Auditing Services



f. Check - Auditing Services

5. CONCLUSION

Outsourcing has become critical to business operations and vital for businesses to sustain their competitive advantages. Maintaining security in IT outsourcing is important for maintaining the growth of IT outsource services. Thus proposed approach provides the security outsourcing services by enabling periodic audit and dynamic operations. Also the verification is provided for the cloud service provider to access the data in the cloud. Hence the malicious cloud service providers are removed from the system.

6.REFERENCES

[1] Yan Zhu,Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G.An and Chang-Jun Hu" Dynamic Audit Services for Outsourced Storages in Clouds."

[2] M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.

[3] 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.

[4] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[5] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10, 2008.

[6] C.C. Erway, A. Ku¨ pc¸u¨ , C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security, pp. 213-222, 2009.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology Advances in Cryptology (ASIACRYPT '08), J. Pieprzyk, ed., pp. 90-107, 2008.

[8] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang "A Study of User- Friendly Hash Comparison Schemes" Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114,2009.

[9] A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.

[10] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758,2010.

[11] M. Xie, H. Wang, J. Yin and X. Meng, "Integrity Auditing of Outsourced Data" Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp.782-793,2007.

[12] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" Proc. IEEE INFOCOM, pp. 1-9, 2010.

[13] www.googleimages.com

[14] www.wikipedia.com