International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30607-30614

http://www.ripublication.com

Data Auditing In Federated Cloud Environment

K.Brindha, S. Sudha, R.Sujatha
Assistant professor (Senior),
SITE, VIT University, Vellore,

Abstract

In current scenario, it becomes difficult to manage the demand of all RaaS (Resource as a service) by a clientin a single cloud. This problem could be overcome by a federated cloud. The great challenge of federated cloud computing are satisfying the client needs, data privacy and security. With the help of cloud, the clients can store and access the data as per their needs. This ensures security regarding the authorization of the client's data. Keeping the data in secured way is one of the important services of the cloud. In this paper we propose one privacy preserving public auditing scheme for federated cloud.

Keywords: RaaS, federated cloud, authorization, security, auditing, scheme.

Introduction

A federated cloud model interconnects the various computing devices scattered on distributed physical locations and are managed by cloud broker [2]. It provides cloud users easy access to the widest range of resources and services available, and gives cloud vendors a platform for delivering high-value services to cloud environments. Based on the business needs the data owner the emerging cloud trend enables him (DO) to stores on large scale and utilize computing resource by dynamically expanding or contracting based on their business needs. DO include both, enterprises and individual. Data owners cannot only store their data in the cloud but also enjoy more benefits such as reducing burden of hardware, software, storage, cost and personal maintenance, and universal data access and so on [4]. Cloud infrastructure are more reliable and powerful than end user computing devices, but it susceptible to externaland internal threats which affects data integrity. Auditing is an important solution for trace-back, security breaches, data accesses, application activities [5]. One of the main issues with cloud data storage is data integrity and verification on remote server [6]. As the data owner find difficultly in keeping their data for longer period of time. Downloadingthe data file is not the only solution for verification

because it requires more cost for transmission as well as it is insufficient to detect data damage and data corruption [11].
Some of the attacks of cloud computing can affect data privacy and integrity. A lot of research papers deal with proving integrity on cloud storage and introduce solutions to reduce the attack on data integrity and privacy [1].Thus some auditing protocols ensure integrity and authenticity of the outsourced data. The auditing protocol achieves the integrity of data and authenticity in a low communication and computation complexity. The auditing protocols areclassified into public auditing protocol and self-auditing protocol according to type of auditors [4]. Ari Juels, Burton S. Kaliski proposed a self-auditing protocol [9] which performs secure auditing of the outsourced data. Considering the user's limited computation and communication capabilities, Cong Wang, Qian Wang and KuiRen, Wenjing Lou proposed public auditingprotocol [13].

A public auditing protocol is a collection of KeyGen, TagBlock, GenProof, Check proof algorithms. KeyGen is used to generate the key andTagBlock is used to generate metadata by user. GenProof is used to generate a proof of possession by the cloud server and Check proof is used to validate the proof of possession by Third party auditor[13].It is very difficult for the data owner to audit periodically the outsourced data, so that users can delegate the TPA,who has capabilities and expertise in auditing the outsourced data. He has to check the data correctness without accessing local data and he cannot read the user's data during auditing process. The remainder of the paper is organized in following sections: Section 2 describes the federated cloud storage structure, section 3 summarizes public auditing scheme for federated cloud, and section 4 concludes the paper.

Federated Cloud Structure

Architecture of federated cloud involves five entities: Cloud broker, Data owner, Cloud service provider, Third party auditor and Authorized applications. The broker's responsibility is to save data owner's time by researching services from different providers and providingdata owner the information about how to use cloud computing to support business goals. A cloud broker is also granted with the authorities to negotiate contracts with cloud providers on behalf of the Data Owner. The broker may provide the customer with an application program interface (API) and user interface (UI) that hides any complexity and allows the customer to work with their cloud services as if they were being purchased from a single vendor. The broker is sometimes referred to as a cloud aggregator [1]. The Cloud also provides the customer with additional services, facilitating the encryption and transfers the customer data to the cloud and assisting it with data lifecycle management.

Data Owner may be an organization or a person who stores large amount of data in the cloud. The Cloud Service provider has technical experts who work in implementing the new technology and improving the network infrastructure to bring in the productivity and performance. CSP concentrates on customer needs and requirements for architecture, design, implementation, migration and so on. Third party auditor (TPA) is the delegation of DO who has capabilities to monitor and

manage the outsourced data and expose the risk of cloud storage service for DO. He is responsible in the audit functions. He is responsible for checking the integrity of stored data at regular intervals [5].

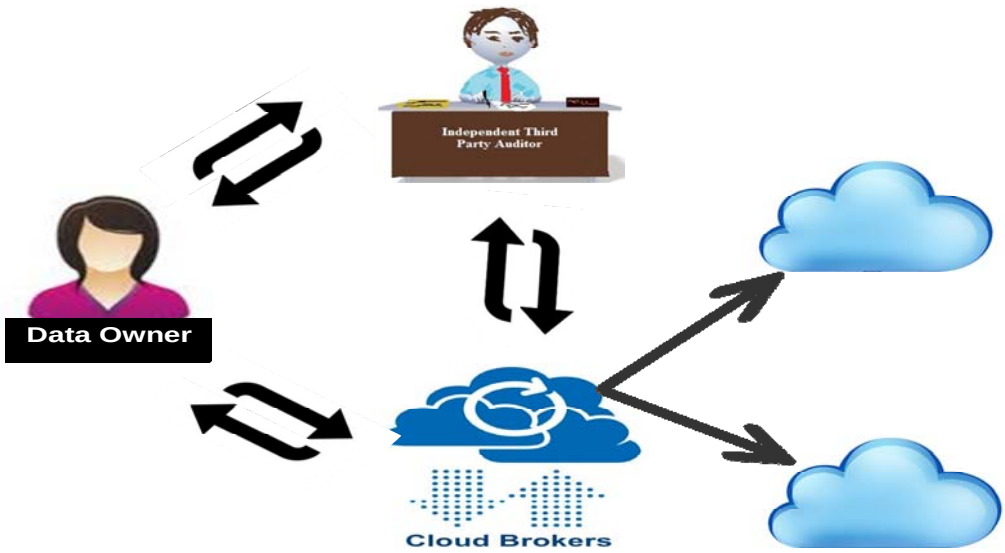

Figure 1: Federated Cloud Structure

Public Auditing Technique

The public auditing scheme is designed for checking data integrity in afederated cloud. It mainly involves four processes such as key generation, meta data creation, data transmission and metadata verification.

Key Generation

Data owner generate the public key and private key using RSA. For security purpose DO chooses two integers P , Q at random and be a equal bit length. Compute n = P * Q , n is used as modulus for both private and public keys. Using Euler's totient function, compute $\varphi(n) = \varphi(P)\varphi(Q) = (P - 1)(Q - 1)$. Select a public exponent PU such that $1 < PU < \varphi(n)$ and compute Private key d is multiplicative inverse of e (modulo($\varphi(n)$)).

Key_generation ()
{
Choose 2 random integers P and Q of similar bit length
Compute n = P * Q
Compute $\varphi(n) = \varphi(P)\varphi(Q) = (P - 1)(Q - 1)$ i.e. e and $\varphi(n)$ are co-prime
Select a public exponent e such that $1 < PU < \varphi(n)$ i.e. e and $\varphi(n)$ are co-prime
Compute private key PR = PU (modulo($\varphi(n)$))$^{-1}$
}

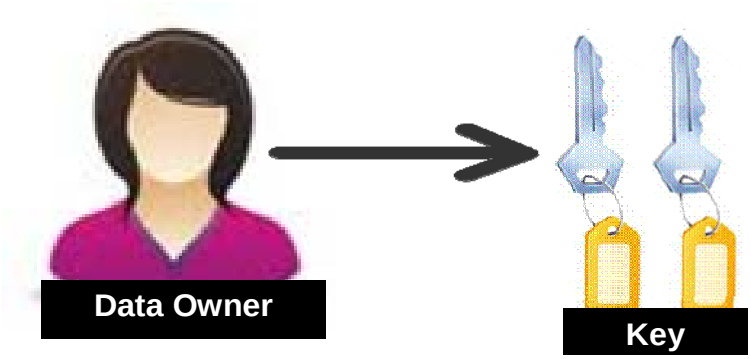

Figure 2: Key Generation

MetadataCreation

DO divide the file M into n blocks M1,M2……Mn. Hash code is generated for each and every file block using HMAC algorithm and the resultant code is encrypted by DO's private key PR.

```
Metadata_creation(File blocks, PR)
{
 File M divided into n blocks M1, M2,……..Mn
 for (i = 1 to ndo)
{
Hash code(i)= HMAC(Mi)
Tag(i)= PR(Hash code(i))
}
}
```

Figure 3: Metadata Creation

Data Transmission

DO sendsa request to cloud broker forusing storage service. Based on the type of service and needs the cloud broker interfaces with the Service Provider (SP) and send acceptance confirmation to DO. Data owner transmits the combined fileblock, tag and index to cloud storage and pair oftag & block index to Third party Auditor for verification purposes.Cloud broker updates the storage allocation table with DO id and other storage details.

```
Data_transmit()
{
for (i = 1 to n do)
CS = Mi || Tag(i) || i
TA = Tag(i) ||i
}
```

Figure 4: Data Transmission

Metadata Verification

DO can check the data integrity on outsourced data by TPA. When TPA receives an audit request from DO for verfication of certain file blocks, it sends an audit message which contain DO's id and position of file blocks.Cloud broker gives a response to TPA with the same. TPA decrypts the Tag block with DO's public key PU and compares this code with metadata received from the DO.

```
Metadata_verification()
{
for (i = 1 to k ) do
{
Vcode = PU(Tag(i)) = PU(PR(Hash code(i)))
if (Vcode == Hash code(i))
data integrity maintained in a file block i
}}
```

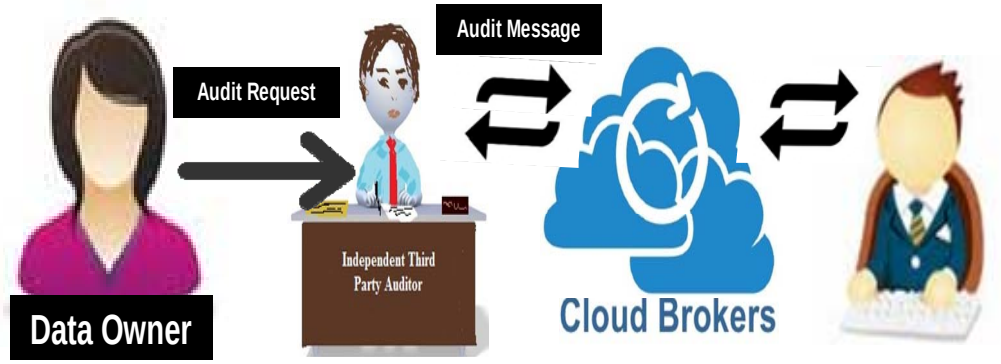

Figure 5: Auditing

Conclusion

The federated cloud structure is an emerging infrastructre paradigm . It provides interface to multi cloud service. As marketis growing, theattacks on storage data is also growing. The proposed auditing scheme provides provable assurance and efficient auditing on the correctness of outsourced data.The digitial signature ensure the data owner's identity and HMAC helps in maintaing integrity of outsourced data. The Thrid party auditing provides cost effective and transparent method for establishing trust between DO and Cloud broker.The audit report of TPA helps the DO to evaluate their risk on oursourced data and also beneficial for the cloud broker in improving their services on multi cloud structure.

References

[1] SaranyaEswaran, Dr.SunithaAbburu, 2012, Identifying data integrity in the cloud storage, International Journal of Computer Science Issues, March 2012, Vol.9, Issue 2, 403-408

[2] Francesco Palmieri, Luigi Buonanno,SalvatoreVenticinque,Rocco Aversa, Beniamino Di martino, 2013, A distributed scheduling framework based on selfish autonomous agents for federated cloud environments, Elsevier Future Generation Computer Systems, 2013, 1461-1472

[3] Cloud computing Use Cases white paper.

[4] Xuchun-xiang, He xiao-hu, Daniel Abraha, September 14-16, 2012, Cryptanalysis of auditing protocol proposed by wang et al for data storage security in cloud computing, Third International Conference, ICICA 2012 Proceedings part - II, Chengde, China,Communications in Computer and Information Science Vol 308, 422-428

[5] Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S.Yaou, Ho.G.An, and Chang-Jun Hu, 2013, Dynamic Audit Services for Outsourced Storages in Clouds, IEEE Transactions on service computing, April-June 2013, vol.6, No.2, 227-238.

[6] Qian Wang, Cong Wang, KuiRen, Wenjing Lou and Jin Li, 2011,Enabling Public Auditability and Data Dynamics for Storage Security in Cloud computing, May 2011, IEEE Transactions on Parallel and Distributed Systems, Vol 22, No.5, 847-858.

[7] Cong Wang, Sherman S.M.Chow, Qian Wang, KuiRen, Wenjing Lou, 2013, Privacy – Preserving Public Auditing for Secure cloud Storage, IEEE Transaction on Computers, Vol 62, No.2, 362-375.

[8] Tao Zou, Jian Wu, Changsheng wan , 2012, A Light Weight Public Auditing Scheme for proof of storage, 2012,Information Science and Service Science and Data Mining (ISSDM), Oct. 2012 6th International Conference on New Trends in, Taipei, 133-136.

[9] Ari Juels, Burton S. Kaliski, 2007,PORs : Proofs of Retrievability for Large Files, CCS'07 : Proceedings of the 14th ACM conference on Computer and Communications security,New York ,Oct. 2007, 584-597.

[10] G.AtenieseEt.Al., 2007, Provable Data Possession at Untrusted Stores,CCS'07: Proceedings of the 14th ACM conference on Computer and Communications security, Oct. 2007, New York,598-609.

[11] C. Wang Et.Al., 2010, Towards publicly auditable cloud data storage services, Network, IEEE, July-August 2010, vol: 24, No.5, 19-24.

[12] Attas, Dalia; Batrafi, Omar, 2011, Efficient integrity checking technique for securing client data in cloud computing, International Journal of Electrical & Computer Sciences, Oct 2011, Vol.11, No.5,43-48.

[13] Cong Wang, Qian Wang and KuiRen, Wenjing Lou, 2010, Privacy – Preserving Public Auditing for Data storage Security in Cloud computing, INFOCOM, proceedings IEEE, March 14-19, 2010, San Diego, CA,1-9.

[14] TejashreePaigude, T.A.Chavan, 2013, A Survey on Privacy Preserving Public Auditing for Data Storage Security, International Journal of Computer Trends and Technology, Vol. 4, No.3,412-417.

[15] R.Nilavathy, 2013, Data Integrity and Data Dynamics with Secure Storage Service in Cloud, Proceeding of the International Conference on Pattern Recognition, Informatics and Mobile Engineering, Feb 21-22, 2013, 125-130.

[16] MuralikrishnanRamane and Bharath Elangovan,2012, A Metadata Verification Scheme for data auditing in cloud environment, August 2012, International Journal on Cloud computing Services and Architecture, Vol 2. No.4, 53-62.

[17] AbhishekMohta and Lalit Kumar Awasthi, 2012, Cloud Data Security while using Third party Auditor, International Journal of Scientific and Engineering Research, June-2012, Vol.3, No.6,1-6.