International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 191-196
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

PRESERVING IDENTIFY THE USER AND PRIVACY OF DATA USINGCLOUD

Keerthikha.M.S[1],S.Divya Lakshmi[2],
[1]Assistant Professor, [2]Assistant Professor, BIST,BIHER,Bharath University,
[1]keerthikha@bharathuniv.ac.in, [2]divya@bharathuniv.ac.in

Abstract: Storing and sharing of data in hybrid cloud is most commonly used but it poses many challenges of maintaining the secrecy of the data and anonymity of the user signing the data from the malicious users during public auditing. In literature many mechanisms have been introduced that works in achieving these challenges. ORUTA (One Ring to Rule Them All) is one such mechanism that works on privacy preserving public auditing. But ORUTA does not focus on dynamicity, traceability, freshness property and it mainly concentrates on static group. It also provides only partial auditing.The system proposed in this paper aims at fulfilling dynamicity, preserving identity of user and privacy of data. It also provides complete public auditability in hybrid cloud. The privacy of data and identity of the user signing the data is kept confidential and it is also safeguarded from adversaries internal and external to the group. This is achieved by using the Tri Degree Coalition (TDC) Architecture and Virtual Machines (VM). The system aims at providing the following characteristics: Extensive auditing, unforseeability, shared data privacy, user's identity, dynamicity, trackability, originality. The efficacy of the system is also maintained.

Keywords: Hybrid Cloud, ORUTA, Public Auditing, Privacy, Identity, TDC, VM, Dynamicity, Trackability.

1. Introduction

Cloud computing is a computing that shares servers to handle applications. It is compared to computing resources rather than having local grid computing as that in which the unused processing cycles in a network are harnessed to solve problems that are too intensive to be solved by any stand-alone machine. Cloud computing is an internet based computing where different services are delivered to organizations through the internet [1]. Cloud computing aims at providing traditional supercomputing or high performance computing power to accomplish tens of trillions of computations per second.

To enable this, cloud computing uses network of large groups of servers running low-cost consumer PC technology with specialized connections to spread data processing chores across them. Usually, virtualization techniques are used to maximize the power of cloud computing [7-9]. There are various characteristics of cloud computing. The major characteristics includes: On-demand self-service, Ubiquitous network access, Resource pooling, Rapid elasticity[1-6], Measured service. On-demand self service is the process of supplying the resources to the users on pay-per-use basis without having the intervention of the user. Ubiquitous network access refers to accessing of resources and computing facilities using thin or thick clients. In resource pooling the resources are pooled and provided to the users. Users are unaware of the location of the resources and the resources are distributed, re-distributed to them based on their need. Rapid elasticity is one in which the cloud computing provides an illusion of accumulation of infinite resources and providing it to the users on demand. Cloud computing has the ability to elastically handle peak traffic and simultaneous demands. In measured service cloud computing demands cost to the users only based on their usage of resources [10-15].
Cloud computing basically offers three service models to its users. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS provides a virtual server instance and storage including Application Programming Interfaces (APIs) to its users so that the users can migrate the workloads to a VM. Amazon Web Service (AWS) is an example of IaaS. PaaS provides host development tools on their infrastructures. Users access those tools using APIs over the Internet. Major PaaS providers are Salesforce.com's Force.com, Amazon Elastic Beanstalk, Google App Engine. SaaS model delivers software applications over the Internet. Users access SaaS applications and services via Internet from any location [4].

Cloud also provides four major deployment models for its users. The deployment model includes Private cloud, Public cloud, Community cloud, Hybrid cloud. Private cloud is maintained within an organization and it delivers business data centers to internal users. It preserves security and control over organization data. In public cloud the services are delivered by a third-party provider over the internet. Public cloud services are sold on-demand and the users pay only for the services they consume. In community cloud the cloud infrastructure is

shared by several organizations having the same policy considerations. This reduces the costs as compared to a private cloud since it is shared by a larger group. Community cloud is more than a private cloud and less than a public cloud. Hybrid cloud is a combination of public cloud services and private cloud with automation between the two. Companies use private cloud for sharing sensitive applications and public cloud for large bursty workloads [16-19].

Cloud computing has various challenges in which security takes the major concern and need to be addressed. Cloud computing security processes should be capable of addressing the security controls which will be incorporated by the cloud provider to maintain customer's data security, privacy and compliance with necessary regulations [20-21]. Users store much sensitive information in the cloud that is pose to threat by many malicious users. The users require that the integrity of their data must be maintained and also the identity of the user sharing the information must be confidential and should not be exposed to the unauthorized users. To perform this activity of maintaining the integrity cloud performs public auditing on the data stored in the cloud. Public auditing is done by the Third Party Auditor (TPA) on the data stored by the user to verify the integrity of the data without revealing the identity of the user to the TPA. Various auditing mechanisms have been introduced in literature which will be dealt in the further chapters in this paper and the drawbacks in each mechanism is also discussed.

The rest of the paper is organized as follows. Chapter II consists of various related work, Chapter III provides the need for public auditing, Chapter IV deals with the existing ORUTA mechanism, Chapter V tells about the system model of ORUTA, Chapter VI is about the proposed TDC architecture, Chapter VII is about the TDC system architecture and its three phases, Chapter VIII concludes the paper and Chapter IX deals with the future enhancement.

2. Related work

In "Privacy Preserving Public Auditing for Shared Data in the Cloud", SwapnaliSakore et al. [7] proposed SPEKE (Simple Password Authenticated Exponential Key Exchange) algorithm. In this paper privacy is accomplished by splitting data into various blocks and storing the blocks in multiple clouds so that more protection is provided. The keys for encryption and decryption are stored in the key storage area. During decryption the data is decrypted only when the user enters the One Time Password (OTP) sent to his mail. Data blocks are independently signed by the owner and integrity checking is done by retrieving only random combination of the blocks. But the system in this paper is dependent on network traffic and encryption is difficult since data owners share data under policy over attributes from multiple authorities. Traceability of data is not maintained.

In "Enhanced Oruta Mechanism for Verifying Shared Data Integrity with Data Freshness and Traceability over Cloud Data", N. Deivanayaki et al. [8] proposed a Digital Signature technique. Data privacy is improved in this paper by using Traceability ORUTA. The freshness of data is provided by preserving the identity privacy. Freshness enables retrieving only recent updated data. Achieving data freshness is necessary to prevent misconfiguration errors. Data integrity in this paper is achieved and system is expected to reach fine grade of data validity and quality. But in this system the signature is stored in the public cloud which may be easily hacked by unauthorized users, because data in public cloud is subject to access by both authorized and unauthorized users.

In "Traceability Mechanism for Sharing Data in Cloud", KedarJayeshRasal et al. [10] Key Distribution Center (KDC) has been proposed. KDC is used to reduce risk of key exchange. The verifier does not learn any information about the user. The system supports batch auditing and traceability. To maintain privacy KDC issues tickets to the users. The major drawback of the system is KDC may become a single point of failure. Every user and group manager must trust KDC for proper functioning of the architecture and KDC works only if users have registered previously. The ticket used by KDC expires within particular time. So again the users have to re-request for ticket for accessing particular service. The tickets that are re-issued are transparent to other users and may be hacked.

In the paper "Storing Shared Data on the Cloud via Security-Mediator", Boyang Wang et al. [11] proposed a Security Mediator (SEM) and Blind Signature technique. The SEM is obtained from the organization and it signs on behalf of all its members. SEM is maintained by the organization and as to who should use the data storage is based on the interest of the organization. This approach decouples the anonymity of protection. SEM avoids the bottleneck and single point of failure. But the usage of blind signature causes blinding attack and since signing process is equivalent to decrypting with signer's secret key, an attacker may provide blinded version of a message encrypted with signer's public key.

3. Purpose of public auditing

Users store the data in the cloud to reduce the overload at the local server. Also they share the data stored among others in the organization or in the group. But they require that data stored must be kept intact and must not be altered and while retrieving the data they require most recent update of data to be received. The users often require auditing of their data stored in the cloud. But this auditing cannot be performed by the users and they require a Third Party to perform auditing. The users in

turn require that the privacy of data and identity of the user must be preserved from the Third Party.

3.1 Existing oruta mechanism:

Oruta, a new privacy preserving auditing mechanism for shared data in untrusted cloud has been used in the existing system. Oruta utilizes ring signatures to construct homomorphic authenticators so that TPA is able to verify the integrity of shared data without reacquiring the entire data and also the identity of signer in each block is kept private from TPA. Oruta also supports batch auditing which can audit multiple shared data concurrently in a single auditing task.Oruta uses random masking to support data privacy during public auditing and takes advantage of index hash tables to support fully dynamic operations on shared data. Dynamic operations includes insert, delete or update operation on single block in shared data. The Oruta mechanism consists of three entities: the cloud server, TPA and users. There are two types of users in a group: Original users and number of group users. Original user and group users are both members of the group. Group members are allowed to access and modify shared data created by original user based on access control policies. Shared data and signatures are both stored in the cloud server.

3.2 System model of existing oruta:

The system model used in Oruta works as follows:
The users store the blocks of data and ring signatures in the cloud server. These users can modify the block of data with their private key S~~k~~ and other users public key P~~k~~.
When the users of the group either the original user or other users want to check the integrity of the data stored in the cloud, they send an auditing request to the TPA with Public Aggregate Key (PAK) and all the users' public key.
The TPA in turn sends the auditing message to the cloud server. TPA selects the blocks of data for which integrity has to be checked and generates a random value for these blocks. It sends the blocks and random value generated to the cloud server.
Cloud server upon receiving the audit message chooses the needed particular blocks of data and sends the auditing proof to the TPA. The cloud server generates a value for the aggregated elements by choosing a random element. It masks the blocks of data so that TPA will not identify the content inside the block. Cloud server also aggregates the ring signatures stored by the users and chooses the identity of shared blocks. Cloud server passes all these information to the TPA along with auditing proof.
The TPA after receiving the auditing proof verifies the information with the data it posses and send the auditing report to the users [14].

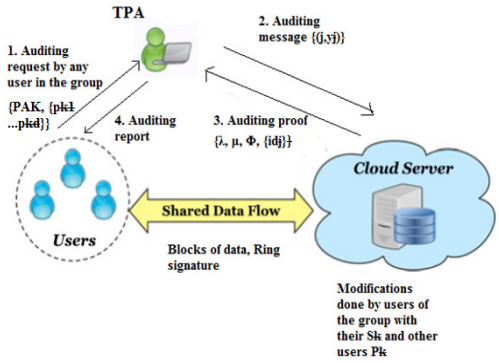

Figure 1. System Model of Existing ORUTA

j – Set of blocks**yj -**Random values generated by the TPA for the set of blocks
λ – Value calculated by the cloud server for the aggregated elements by choosing a random element
μ – Masked blocks
Φ – Aggregate of ring signatures
idj – Identity(index) of the shared blocks
AK – Public Aggregate Key
pk1...pkd – Public key of all the users

4. proposed TDC architecture

The Tri Degree Coalition (TDC) architecture aims at fulfilling dynamicity, traceability, and freshness property. The architecture provides complete public auditability in hybrid cloud. The architecture includes various mechanisms and algorithms to provide integrity of data and maintaining the identity of the user along with the above mentioned properties. The TDC Architecture coordinates to provide integrity of data and maintaining the identity of the user. The architecture also aims to achieve the identity preserving public auditability. In this architecture, the users joining the group have to register themselves with their information with the private cloud. After receiving, the information is stored in the private cloud. The ID generator verifies whether it is valid user information. If it is valid then ID generator (Linear Congruential Generator) generates the One Time Password (OTPD) for that user. Parallely the blowfish algorithm generates keys for the signature and stores the keys in the Virtual Machine (VM). The VM passes the keys to the ring signature which generates the signature for the keys. Then TDC passes the OTPD and signature to the user.

5. TDC system architecture

The TDC architecture provides three levels of security and performs complete and secure modifications and auditing. The architecture also helps to reduce the computation cost and increases the efficiency. The

architecture is described for Uploading phase, Downloading phase and Auditing phase.

Uploading Phase:

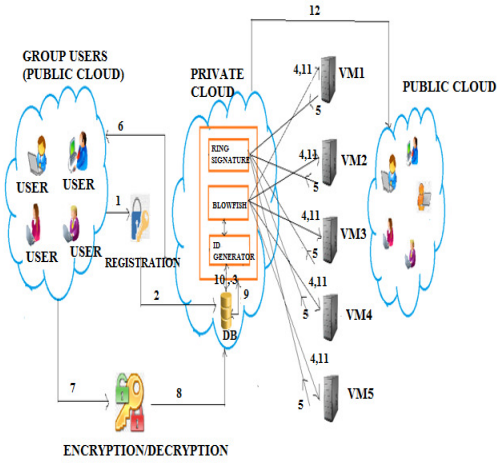

Figure 2 . TDC System Architecture (Uploading Phase)

The working of architecture for uploading phase is as follows:

Step 1: Users register with their details
Step 2: The details are stored in the private cloud
Step 3: ID generator verifies the details of the user and then generates OTPD for the user and copy of OTPD is stored in the private cloud
Step 4: The blowfish algorithm generates keys for the ring signature and stores the keys in the VM
Step 5: VM passes the keys to the ring signature to generate the signature and copy of signature is stored in the private cloud
Step 6: TDC sends the OTPD and signature to the user
Step 7: The user can upload the file after receiving the OTPD and signature from the TDC. The user passes the same along with the file for uploading
Step 8: The file gets encrypted and the encrypted file along with the OTPD and signature moves to the TDC (Private Cloud)
Step 9: After receiving the file TDC verifies the OTPD and signature for the valid user to upload the file
Step 10: The ID generator generates the file ID and copy of it is stored in the private cloud
Step 11: The blowfish algorithm generates the key for the file and stores in the VM and copy of it is sent to the private cloud by the VM
Step 12: The TDC (Private Cloud) embeds the file ID, key of the file, signature along with the encrypted file and uploads to the public cloud

The working of architecture for downloading phase is as follows:

Step 1: Users register with their details
Step 2: The details are stored in the private cloud
Step 3: ID generator verifies the details of the user and then generates OTPD for the user and copy of OTPD is stored in the private cloud
Step 4: The ring signature retrieves the keys for generating the signature from the VM and generates signature. A copy of the signature is stored in the private cloud
Step 5: TDC send the OTPD and signature to the user
Step 6: The user can download the file after receiving the OTPD and signature from the TDC. The user passes the same along with the file name for downloading
Step 7: The TDC verifies the OTPD and signature along with the file name and if it is a valid user, then it retrieves the file ID from the private cloud and passes the file ID to the public cloud and obtains the file for the corresponding file ID
Step 8: TDC passes the file for decryption
Step 9: The decrypted file is sent to the user

Auditing Phase:

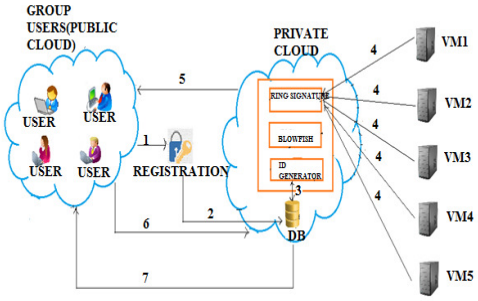

Figure 3. TDC System Architecture (Auditing Phase)

The working of architecture for auditing phase is as follows:

Step 1: Users register with their details
Step 2: The details are stored in the private cloud
Step 3: ID generator verifies the details of the user and then generates OTPD for the user and copy of OTPD is stored in the private cloud
Step 4: The ring signature retrieves the keys for generating the signature from the VM and generates signature. A copy of the signature is stored in the private cloud
Step 5: TDC send the OTPD and signature to the user
Step 6: The user can now send auditing request to the private cloud (TDC) along with the received OTPD and signature
Step 7: TDC verifies the details of the user, file modification details from the private cloud and send the auditing details to the user

6. Conclusion

The proposed Tri Degree Coalition Architecture overcomes the drawbacks of the existing systems and also help to maintain the efficiency of the system while achieving the objectives. The architecture provides complete auditing by preserving user's identity and maintaining the privacy of the data. It provides a high level of security and filters the unauthorized users at the initial stage itself. Each level of the architecture provides an additional security to the user's data.

There is no chance for malpractice because the OTPD and signature can be utilized only once and all the modifications and auditing must go through the architecture which provides three level of security.Thus the proposed architecture fulfils all the objectives designed for the proposed system and also overcomes the drawbacks of existing techniques.

Future enhancement

The time taken to perform auditing and other modifications is more because the users' request has to pass through three levels of security to obtain the response. But the response is a complete auditing and full security to user's data. But the existing oruta mechanism do not provide complete auditing and full security to user's data even though it consumes more time.But still this factor is taken as a limitation and will be considered as future enhancement of this project.

References

[1] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[2] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[3] BrinthaRajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[4] BrinthaRajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[5] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[6] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[7] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[8] Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.