International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 925-929
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A COMPLETE PUBLIC AUDITING FOR DATA SHARING IN HYBRID CLOUD USING TRI DEGREE COALITION (TDC) ARCHITECTURE

[1]R.G.Suresh Kumar, [2] Dr.T.Nalini , [3]V.Saranya
[1]Research Scholar,
Vels University,Pallavaram, Chennai.
[2]Professor,
, Bharath University, Chennai.
[3]M.Tech(CSE),
RGCET, Puducherry

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 data privacy and user identity 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 share theservers to handle applications. It is compared to computing resources rather than having local grid computing as that in which the idle processing cycles in a network are connected to solve problems that is too intensive to be solved by any stand-alone machine. Cloud computing provides different services which are delivered to organizations through interconnected networks or with the internet [1].Cloud computing aims at high performance and power to achieve millions of computation per second. To enable thisvirtualization technology are also used to maximize the performance of cloud computing [2]. There are various characteristics of cloud computing. 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. Users are unaw[illegible] 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 [3].

Cloud computing basically offers three service models to its users. IaaS provides a virtual server instance, so that the users can migrate the workloads to a VM. Amazon Web Service (AWS) is an example of IaaS. PaaS provides the platform for manage and run the web application without the complex.SaaS model distributethe applications through the Internet—as a service. The users can access the software through internet without installing and maintaining in local. Cloud also provides four major deployment models for its users. 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 sold on-demand and the users pay only for the services they consume. In community cloud the infrastructure is shared by different vendors having the same rule consideration which 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 the mix of public cloud services and private cloud services.An organization uses private cloud for sharing sensitive applications and public cloud for large bursty workloads [5].

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 to maintain customer's data security and privacy with necessary regulations [6].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 auditing on cloud data. Auditing is done by the TPA on the cloud data by the user to validate the integrity of the cloud data without revealing the user identity [illegible] have been

introduced in literature which will be dealt in the further chapters in this paper and the drawbacks in each mechanism are also discussed.

2. RELATED WORK

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.

Krishna Kumar L et al. in the paper "Preserving Privacy Policy – Preserving Public Auditing for Data in the Cloud"[9] proposed a technique called Homomorphic Encryption. In this system data is shared in the format of images and file types. An agreement is laid between the data owner and cloud and the integrity is maintained. But the order in storing the data may be altered if data is splitted and stored. Also there is possibility of modifying the uploaded encrypted data.

In "Traceability Mechanism for Sharing Data in Cloud", Kedar Jayesh Rasal 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 isKDC 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. But the process of signing is decrypting with user secret key, so the hacker may use blinded version of encrypted message with user public key.

In "Provable Data Possession at Untrusted Stores", G.Ateniese et al. [12] suggested PDP(Provable Data Possession) scheme. The scheme permits verifier to verify the integrity of data which is stored in untrusted stores by using homomorphic authenticators and sampling strategies based on RSA. It helps to perform data auditing in the cloud. But this scheme issuitable for auditing only static data.

In "Privacy-Preserving public Auditing for Data Storage Security in Cloud Computing", C. Wang et al. [13] proposed random masking to protect the confidential information from the hacker. But this scheme did not provide the identity privacy. In "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", Boyang Wang et al. Suggested the mechanism called ORUTA. In this mechanism public auditing was performed without retrieving the identity of the user by using Homomorphic Authenticable Ring Signature (HARS). Data privacy anduser identity is also maintained. But the splitting of data by HARS scheme may lead to loss of data during auditing and also this scheme focuses only in public auditing of static group.

3. PURPOSE OF PUBLIC AUDITING

The data are stored by the user 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 for the data which is 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. Public auditing is done in which verifiability for the stored data in the cloud is performed by third party on the user request. In literature, TPA is used for public auditing [14]. The mechanisms used in literature preserve the identity of the user and the data privacy from TPA. But with minimal information provided to the TPA and by retrieving certain amount of data the integrity of data is audit by the TPA. But it is certain that the TPA may get compromised with the unauthorized user. And also with the partial information given to the TPA it is only able to perform partial auditing. In order to perform complete auditing and to prevent the TPA from getting compromised, the TDC architecture proposed in this paper can be used. The architecture performs complete auditing without the presence of TPA and also the integrity of data and data privacy are preserved.

4. EXISTING ORUTA MECHANISM

The new privacy preserving auditing mechanism called Oruta is used for shared data in untrusted cloud in the existing system. It utilizes ring signatures to build the homomorphic authenticators, As a result TPA is able to verify the shared data integrity without reacquiring the whole data and also the user identity of who signed in each block is kept secret from TPA. Oruta uses random masking to maintainthe data privacy for the shared data in cloud during public auditing and use the index hash tables to support dynamic operations on shared data. A dynamic operation includes update, insert anddelete operation on single block in shared data. The Oruta mechanism consists of three entities - TPA , cloud server and users and two types of users in a group - Original users and group users. Both users are members of the group. They are allowed to modify the shared data which is created by original user by the access control policies. Signatures and shared data are stored in the cloud server.

Oruta is designed to perform audit for integrity of shared data in the cloud with only for static groups. Which means the group is pre-defined and also the membership of users in the group is not changed during the shared data is created in the cloud. The original user is accountable for share the data before outsourcing to the cloud. When the user wants to check integrity of shared data, the auditing request will send to TPA. Then TPA generates an auditing report to user based on result of the verification [14].

5. 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.

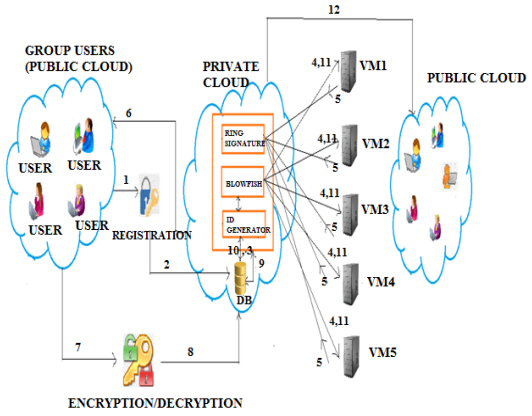
The user can now upload a file. The user sends the file to be uploaded along with the signature and OTPD. The file gets encrypted and it passes to the private cloud. The TDC verifies the signature and details of the user. If the signature matches and if it is a valid user then the private cloud generates the file ID and key for the file. Then the file, signature and file key are uploaded in the public cloud by the private cloud. The OTPD received is valid only for that particular session. So again if the user needs to perform any modifications on stored data in the cloud, the user's needs to request again private cloud for OTPD. The dynamic operations such as add, delete, modify can be performed on the stored data in the public cloud. To reduce the data loss during auditing and some other operations, data is not splitted into blocks. The reverse process takes place for retrieving and modifying the file. Complete auditing is done by preserving the identity of the user signing the data and maintaining the secrecy of the sensitive information. Also during auditing the data from the cloud is not obtained to perform auditing. The private cloud utilizes the information stored to perform complete auditing. This reduces the computation cost. The TDC architecture provides three levels of security as follows

Level 1: The level 1 of security is provided by the ID generator. Upon receiving the file the ID generator checks the OTPD of the user with the OTPD stored in the database
Level 2: The level 2 of security is provided by the blowfish by generating and storing the keys in the VM and providing the keys for signature generation
Level 3: The level 3 of security is provided by the ring signature. The signature is generated for the keys obtained from VM. Like OTPD, this signature is valid only for the current session.

6. 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.

6.1 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

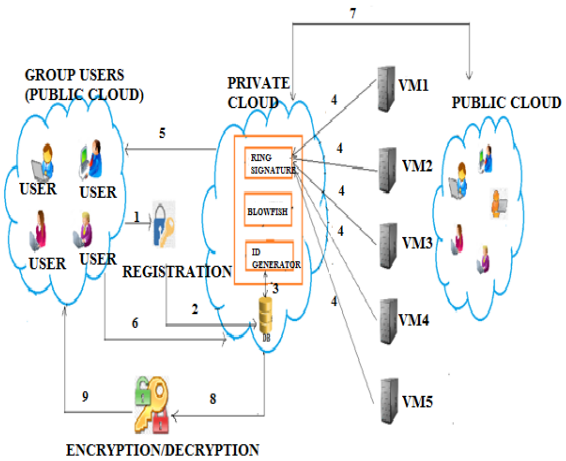


Fig 3 – TDC System Architecture (Downloading Phase)

6.2 Downloading Phase

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 cloud in public and retrieve the file based on the corresponding file ID
Step 8: TDC passes the file for decryption
Step 9: The decrypted file is sent to the user

6.3 Auditing Phase

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

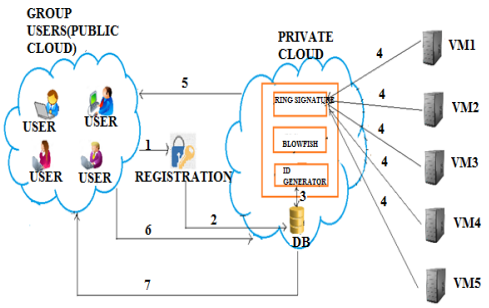


Fig 4 – TDC System Architecture (Auditing Phase)

8. CONCLUSION

The proposed Tri Degree Coalition (TDC)Architecture overcomes the drawbacks of the existing systems and also preserves the efficiency of the system while achieving objectives. The architecture provides complete auditing by preserving user's identity,maintaining the privacy of the data, 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 mismanagement 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. 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] Randeep Kaur , Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, pp. 171-176, March 2014.

[2] K. Hemapriya, J. Deepa, S. Kaviarasan, "Optimized Data Center in IaaS Using Cloud Computing Systems, International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 4, Issue 5, pp. 2974-2980, May 2015.

[3] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication, September 2011.

[4] Sumit Khurana, Anmol Gaurav Verma, "Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS", International Journal of Electronics & Communication Technology (IJECT), Vol. 4, Issue Spl. 3, pp. 29-32, April-June 2013.

[5] Ch Chakradhara Rao, Mogasala Leelarani, Y Ramesh Kumar, "Cloud: Computing Services and Deployment Models", International Journal of Engineering and Computer Science (IJECS), Vol 2, Issue 12, pp. 3389-3392, December 2013.

[6] Kuyoro S.O., Ibikunle F., Awodele O., "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Vol 3, Issue 5, pp. 247-255, 2011.

[7] Swapnali Sakore, Rukmini Raut, Vaishali Shinde, "Privacy Preserving Public Auditing for Shared Data in the Cloud", Proccedings of 20th IRF International Conference, pp. 19-21, 22nd February 2015.

[8] N. Deivanayaki, J.Amu Bebina, "Enhanced Oruta Mechanism for Verifying Shared Data Integrity with Data Freshness and Traceability over the Cloud Data", International Journal of innovative Research and Development, Volume 4 issue 2, pp. 166-169, February 2015.

[9] Krishna Kumar L, Deepa P sivan, "Preserving Privacy Policy-Preserving Public Auditing for Data in the Cloud", International Journal of Engineering Science Invention, Volume 3 Issue 11, pp. 06-09, November 2014.

[10] Kedar Jayesh Rasal, Prof Sandip A. Kahate, "Traceability Mechanism for Sharing Data in Cloud", International Journal of Computer Science Engineering and Technology, Vol 5, Issue 4, pp. 86-89, April 2015.

[11] Boyang Wang, Sherman S.M. Chow, Ming Li, Hui Li, "Storing Shared Data on the Cloud via Security-Mediator", IEEE 33rd International Conference on Distributed Computing Systems, pp. 124-133, 2013.