User/Group Policies, Secured TTP and Customization of SLA in Cloud Computing

G. A. Patil, Singhania University, Rajasthan, India.
Dr. V. A. Athavale, Gulzar Group of Institutes, Ferozepur, Punjab, India.
Mukesh M. More, Assistant Professor, MMCoE, Pune, Maharashtra, India.

Abstract *Cloud Computing has been considered as the future structure of IT Enterprise. Cloud computing is recognized as an alternative to traditional information technology due to its essential resource sharing. In particular, resource sharing may contain hardware, software & data of user. Cloud Computing moves the user`s data, user applications & databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique situation brings many new security challenges. The proposed scheme concentrates on confidentiality issues of data by modifying and applying different authentication and encryption techniques. The data security has become requirement of cloud computing. The security can be provided by defining user/group policies for cloud users, by providing security in trusted third party (TTP) & using customizable service level agreements. So the user can trust on cloud environment & act as trusted user using the defined user/group policies like one to one, one to many, many to many & many to one. The proposed scheme also focuses on customization of service level agreement (SLA), which will provide better usage of cloud computing resources..*

Keywords—*Data security, SLA, user/group policies, Cloud computing, data sharing, access control.*

I. INTRODUCTION

In cloud computing, the cloud service providers (CSP), are able to provide various services to cloud computing users with the help of available infrastructure. This leads to migrating the local data management systems into cloud servers; thereby users can use high-quality services and save major investments on theirlocal infrastructures [14]. One major security concern is authentication, which is the process of validating whoyou are to whom you claim to be. The data stored on clouds are in the control of cloud vendors. This is the reason why many cloud users are demanding for a trust building between end users and cloud vendors. Availability, integrity, consistency and confidentiality of data are prime issues in data security policies. One of the most important services provided by cloud providers is data storage. An organization allows its users in the same group to store and share files in the cloud, resulting in reduction of local data storage management and maintenance. Risk is involved towards confidentiality of those stored files. Cloud computing providers are not trusted by users. Data stored in the cloud may be sensitive, confidential and important such as financial data, personal data, business data, etc. To maintain data confidentiality, there is a need of encryption of data, and then upload the encrypted data into the cloud. Cloud computing is an emerging trend to deploy and maintain software and is being adopted by the industry such as Amazon, Google, IBM, Microsoft and others. Several prototype applications and platforms, such as the IBM “Blue Cloud” infrastructure, the Google App Engine, the Amazon Cloud, and the Elastic Computing Platform [8], have been proposed. When users store data on local storage then that data is in control of user himself/herself. When the data is stored over cloud, the cloud vendors have unlimited access to this data. They can read, write, modify and can do many operations on data. The cloud vendors ask users to trust their service and they will provide protection policies for data hosted on cloud. But what if data get compromised? The vendorholds the full access to data, as we store it in vendor`s environment.

Many intelligent people and organization are asking for trust relation between user and cloud vendor. The concept of cloud computing is built on new architecture. The new architecture comprises of a variety of new technologies, such as Hadoop, Hbase which enhances the performance of cloud systems but brings in risks at the same time. In the cloud environment, users create many dynamic virtual organizations by co-operative relationship of trust between organizations & users rather than individual level. Three levels of defence structures exist in which each layer performs its own responsibility to ensure data security [1]. The first

layer is responsible for user authentication based on digital signature and certificates. The second layer is responsible for user data encryption by applying certain encryption techniques. The third layer is providing data recovery mechanism. But system is not assuring policies for trust relation & moreover the data is under the control of the cloud providers.

Presently, in user polices the cloud user can share the data to another cloud user. The person sharing the file has the only authority to edit the file, while the person accessing the shared data can only read the file. If the person accessing the file wants to make some changes, he has no authority or right to do so. Doing so may impact all the users of cloud environment. The process is very lengthy as the person needs to give his idea to cloud provider which may result in discrepancy as the idea cannot be applied exactly. Hence there is need to change the user policies. Receiver user of cloud can change the file with access permissions given by file owner/sender.

Cloud data storage security, has been always an important aspect of quality of service to ensure the correctness of user's data in the cloud [2]. Cloud users data is usually processed remotely in unknown machines that users do not own or operate. Hence, users fear of confidentiality of data leakage (particularly financial and health data) and loss of privacy. This causes a significant barrier to the wide adoption of cloud services [3].

Service Level Agreement (SLA) is an agreement between consumers and providers [4]. Also, SLA focuses on mechanisms for managing SLAs in cloud computing environment using Web Service Level Agreement Framework [5]. Windows Azure has separate SLAs for compute and storage [6]. For compute, Azure guarantees that when you deploy two or more role instances in different fault and upgrade domains, users Internet facing roles will have external connectivity of at least 99.95% of the time. Additionally, Azure will monitor all of usersindividual role instances and guarantees that 99.9% of the time it will detect within two minutes when a role instance process is not running and initiates corrective action (Windows Azure Service Level Agreement). Recently, the importance of ensuring the remote data integrity has been highlighted by the research works mentioned in [9]–[13].

The remainder of this paper is organized as follows: Section II introduces the user & group policies for accessing data items stored in cloud computing environment. It also discusses the guidelines of building the policies for users & groups of users. Section III discusses the secured trusted third party (TTP) model. Section IV presents the parameters to be considered for customizable service level agreement. Finally, Section V concludes and discusses future work.

II. USER/GROUP POLICIES

This module concentrates on deciding user and group policies and also implementation of these policies to provide shared as well as private access to data stored over cloud environment. To implement this mechanism DFS (Distributed File System) like Hadoop, HBase is used to provide accessibility to data depending on whether the user is a group user or individual user. Figure 1 shows user/groups accessing data items through TTP.

Since there is no solution to broadcast or multicast data to specific multiple users, there is need of forming groups of users in cloud environment. Previously data can be shared only in One to One form, but data cannot be shared in groups in cloud environment. A policy is designed, where the data can be shared in following ways: One to Many, Many to One, Many to Many. If access to some or all items is to be controlled, then the repository should provide limited access based upon user type/status(general public, research organization, membership, and administrative staff).

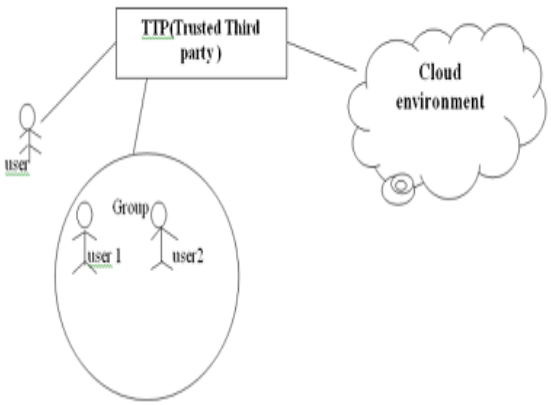

Fig. 1. User Group & Trust model.

The users of cloud computing environment can be categorized as mentioned below.

1) User - is the user entity of cloud environment who has authority to access cloud services. He can create & store file in cloud environment & publish data to other users of same cloud environment. He can receive the files from other users of same cloud environment & use the files with permissions given to him by the owner of the file

2) User Group - is collection of users. Group is made up of number of users. Every User Group has Group Administrator & many users. Users of user group have authority to create files and share in cloud environment.

3) Group Administrator - is a user belonging to the user group. He has authority to create new users in cloud environment, which belong to his group. Also he can delete users, update user information and all rights that of a user.

4) Group User - is the user of cloud environment and may belong to any user group. He can access services of the cloud environment. He can create file in cloud environment & publish data to other users of same cloud. He can receive the file from other users of different user groups also & use the file with permissions given to him by the file owner. Group user may belong to other groups.

5) System Administrator - is user of cloud environment. He has authority to create Groups, Delete Groups, Update Group Information, Create user, Delete User, Update User Information and allocate users to specific groups.

The following are the permissions and rights that can be assigned to the users.

a. Create: user of cloud has authority to create files in cloud.

b. Update: User of Cloud has authority to update existing file created by other users of cloud.

c. Delete: User of Cloud has authority to remove existing file.

d. Share: User of Cloud has authority to share file among cloud users (i.e. 1To1, 1toM, Mto1 MtoM).

The Policies for User communication among different groups are as follows.

1. One to One: In this model, user of cloud environment creates the file & can share it to a specific user. The communication is between one specific user of system to other specific user & not between specific user to any other group, Group Administrator or System Administrator.

2. One to Many: In this, one user can create a file, and may publish to group. Depending on permissions given by owner of the file, group user can access the file with permission. One general user may access data declared as public /private, provided that user has read access to data. If the user is owner of data then he /she has read, write and modify access permissions. Group user can create the file, delete the file, update the file and share the file.

3. Many to One: Group user can create file, created file is published to user of cloud environment. Specific user need not belong to same group. In this, Group users can access same data created by member of group which is declared as private to group. If data declared is public then any user of cloud (including other group users) can access the data. If the user of group is owner, then he/she should have read, write and update permission.

4. Many to Many: In this model, one group of cloud environment shares the files to the other group of cloud environment. Users of group /individual user can access public/private data. The owner of that data should be either from group or individual user and he has read, write and modify access rights.

III. SECURED TRUSTED THIRD PARTY

For the need of trust between cloud consumers and cloud providers we propose the message to be stored in TTP should be in the encrypted form. If the message stored at TTP is in plain text format, then TTP is vulnerable to attacks or he can also misuse the information. For this, suitable algorithms can be used to encrypt & decrypt messages.

Authentication mechanism used by TTP (Trusted Third Party) stores the keys in plain text format. These keys are used by Authentication mechanism to validate users over cloud. Suitable cryptographic techniques are required to provide security in TTP for messages sent by the user. TTP data is used for authenticated users over cloud at the time of registration, the user details i.e. Pass-code is encrypted by using suitable encryption algorithm which will be stored at cloud user database.

Fig. 2 depicts security mechanism to be adapted in trusted third part, thereby securing the cloud computing environment to some extent. The cloud user can create and upload file in the cloud

through the TTP. Trusted third party receives the data sent by the cloud user; it applies encryption mechanism and uploads the same on the cloud.

Finally, cloud providers have user data in encrypted format. Encrypted data will not be accessed by users of cloud. So, data is secure in the cloud environment.

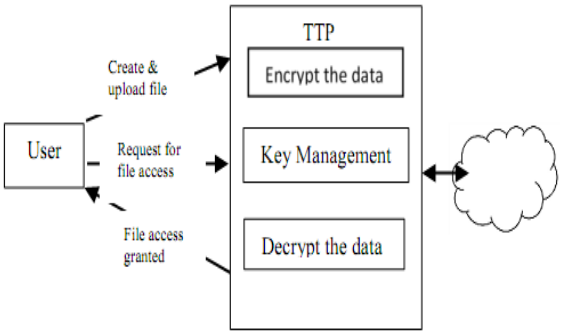

Fig. 2. Security in Trusted Third Party.

Cloud provider has data in encrypted format, this encrypted data is decrypted by using appropriate decryption algorithm at trusted third party, whenever a authenticated cloud user requests to access the file. If cloud user is willing to share data to other cloud users, there should be facility to share cloud user data. Encrypted data is shared among many cloud users. Shared data will be accessed in original form by cloud users through the TTP. The framed grouppolicies will be of help to group users to share the files.

IV. CUSTOMIZATION OF SERVICE LEVEL AGREEMENT

A service-level agreement (SLA) is a part of a service contract where a service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time of the service. A service-level agreement is an agreement between two or more parties, where one is the customer and the others are service providers. This can be a legal binding, formal or an informal contract. Contracts between the service provider and other third parties are often (incorrectly) called SLA.

User and group (organization) hold different requirements and needs. The SLA for individual user and group (organization) should vary. Also individual user and group (organization) may demand customization of SLA policies. This module concentrates on implementing SLA policies as per demands from individual cloud user & group (organization). In this section we propose how customization of service level agreements can work. The considered entity is named as Storage space, which is used by database management system like PostgreSQL, MySQL and Oracle. In this storage space, cloud user can store her databy creating table spaces in cloud. MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack. FOSS-open source projects that require a full-featured database management system often use MySQL.

Cloud computing environment provides many services to users like individual user & organizations. The services provided by cloud are IaaS, PaaS, SaaS, DaaS, etc. Especially, cloud provides services like CPU power, Network Bandwidth, RAM, Storage, SQL Database, Operating System, Office Suite, etc. All these services are provided to cloud user by signing service level agreement. Most of SLA`s are fixed. SLA will not change duringservice period of user. Now a day, there is no solution to change the SLA. To achieve this modification / changeable SLA, we have proposed customization of SLA concepts. To design customizable SLA, we consider service of cloud as stable storage. Stable storage gives space to store user's data in table format. Initially, weconsider any user of cloud can generate two storage spaces free of cost. If cloud user required more spaces then he need to purchase storage space by paying related amount to cloud provider.

Cloud user can use the given storage space to store data and create the data tables for web development. Cloud user can use this space to store data of web client. This storage space may be used to store data like medical data, commercial data, radar, GPS, etc.

Cloud computing environment provides number of services to cloud client. Storage space service is one of them. Services having fixed amount of quantity and price are provided by commercial cloud provider. In case of normal cloud user, if she wants to use unlimited amount of service, cloud provider does not permit. Cloud user has to pay entire amount which is required to pay for using the demanded service. And it is mandatory to agree on the SLA or by default, it is agreed upon. By customizing service level agreement, user of cloud computing environment can use resources efficiently. The price of customized service level agreements would be very less and affordable to the cloud user.

The SLA basic policies include –

1. Service year - 365 days from date of SLA claim.

2. Annual uptime precent- Annual Uptime Percentage is calculated by subtracting from 100% the percentage of 5 minute periods during the Service Year in which cloud environment was in the state of Region Unavailable.

3. Region Availability.

4. Storage Space

5. Data security.

Customizable SLA include -

1. Service year should vary. In Service year, the accessing period is decided by user. In this user can pause the current service, again user can resume the service of cloud environment.

2. Eligible Credit period (Monthly/Yearly Billing)-The Eligible Credit Period is a single month, and refers to the monthly billing cycle in which the most recent Region Unavailable event is included in the SLA claim.

3. Service Credit- is the percentage of the monthly service fees for the Service that is credited to customer for a validated Claim.

4. Customized Storage Space

5. Enhancement to above basic policies is based on the cloud environment policies.

The entire experimentation is done on Heroku Cloud and the results are documented.

V. CONCLUSION

Cloud computing is an emerging computing model that requires more research attention. In this paper, we have presented the user and group policies for accessing data items and defined policies like one to one, one to many, many to many and many to one. The user is able to share data securely with other users and groups. The user and group policies dependent on the policies of the organization. The secured TTP model aims to provide security to the cloud environment by using suitable encryption algorithms. The experimentation on the proposed customizable SLA was limited only to storage space service. It can be extended to other services also for the parameter like service year, annual uptime percent, etc.

REFERENCES

[1] Cong Wang, Qian Wang, and KuiRen, "Ensuring Data Storage Security in Cloud Computing" Department of ECE, Illinois Institute of Technology, 2008.

[2] Dai Yuefa, Wu Bo, GuYaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing" International Workshop on Information Security and Application, 2009.

[3] Richard Chow, Philippe Golle, MarkusJakobsson, RyusukeMasuoka, Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", ccsw'09 Nov 13, 2009 Chicago, USA.

[4] Pankesh Patel, AjithRanabahu, AmitSheth, "Service Level Agreement in Cloud Computing" Knoesis Center, Wright State University, USADA-IICT, Gandhinagar, INDIA.

[5] Linlin Wu and RajkumarBuyya, "Service Level Agreement (SLA) in Utility Computing Systems".

[6] Microsoft Windows Azure Compute Service Level Agreement (SLA).

[7] Microsoft Windows Azure Storage Service Level Agreement (SLA).

[8] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[9] Juels and J. Burton S. Kaliski. "PORs: Proofs of Retrievability for Large Files", Proc. of CCS '07, pp. 584-597, 2007.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. of Asiacrypt '08, Dec. 2008.

[11] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. Of CCS '07, pp. 598–609, 2007.

[13] Qian Wang "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" 2011

[14] Xuefeng Liu, Yuqing Zhang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud"

[15] IEEE transactions on parallel and distributedsystems, vol. 24, no. 6, June 2013.