A Triple Key Resource Sharing Technique for Enterprise Cloud

V. Ashok kumar
Assistant Professor, Department of CSE,
Srikalahasteeswara Institute of Technology (SKIT), Srikalahasti-517640,
Endowments Department, Government of Andhra Pradesh, India.
e-mail: ashokcse.skit@gmail.com

Abstract: The cloud is a competitive alternative to the general distributed resource sharing scheme with less cost and efficient and less maintenance overhead so most of the enterprises are choosing it. The cloud is the service being delivered from remote sites. Weather it is public, private, hybrid, community or inter-cloud, the physical location of the devices at the end points are servers, storage devices, computing devices, networking equipments and security systems that we interact with mobiles, computers, tablets using some applications from inside and outside of the enterprise. The enterprises have to register for the required resources in the cloud and can be utilized by the different members. It is problematic to maintain security and user privacy within the enterprise with traditional strategy. In my proposed system an efficient resource sharing is provided by using a technique ERST with three keys called Enterprise key, Manager key and member key along with the Biometric authentication.

Key words: *- Distributed, Cloud Computing, Inter-Cloud, Enterprise, Manager, Member, Cryptography, security, integrity and privacy.*

*****

I. INTRODUCTION

The cloud is the service being delivered from remote sites. As public and private industry budgets continue to shrink, executives are plotting new strategies to become more efficient and cost effective. Cloud computing has gleaned a lot of attention over the past several years as a means to reduce IT expenditures, improve scalability and reduce administration over head. As savings amount and efficiencies increases, cloud computing will continue to grow. Most of the enterprises are already operating their applications or infrastructure in a cloud environment. Now a day's most of the personal and general purpose services are also provided to personal cloud user by the cloud service providers. Up to 2015 the top 10 cloud services[6] are Rack space, Amazon Web Services (AWS), Site Ground, Storm On Demand, Microsoft Azure, Digital Ocean, Liquid web, Net magic Solutions, Ctrls and Servint.

1.1. Definition of cloud Computing

The National Institute of Standards and Technology has defined Cloud computing[2] as "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". (Mell & Grance, 2011, p. 2).

There is little consensus on how to define the Cloud [3][4]. I add yet another definition to the already saturated list of definitions for Cloud Computing:

A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the internet. Cloud Computing is anything that provides hosted services over the internet [5]. These services are sharing to the end users. The main uses of cloud are data storage, process and management services on the internet rather than having local servers. The service provider has to look up all the issues related to the cloud. The end-user doesn't require any server to maintain, simply requesting the services from the cloud and pay for using it.

II. CLOUD COMPUTING ENVIRONMENT

NIST also defines five key and essential characteristics, three service models and four deployment models are shown in below [2].

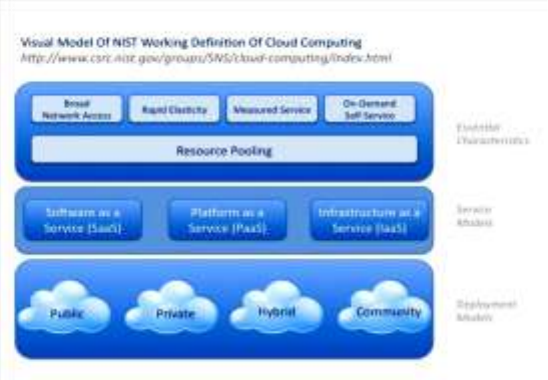
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

Figure 1: NIST defined Essential characteristics, Service models and Deployment models.

2.2. Characteristics of Cloud

According to National Institute of Standard Technology [2] (NIST, U. S. Department of Commerce), cloud has five essential characteristics as follows.

1. On demand self service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

NIST categorizes Cloud computing into a Service Model and a Deployment Model.

2.3. Service Models of Cloud Computing

As per NIST mainly the Service Model consists of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as shown below along with the services provided by the cloud with challenges Security, integrity and privacy at different levels **[2]**.

This "stack" of functionality begins with Infrastructure as a Service where consumers utilize hardware only. Moving up the stack is Platform as a Service. This layer offers the consumer an application environment where programming libraries and software can be used for development. At the top of the stack is Software as a Service. The consumer utilizes the Cloud providers' application and has no access to the infrastructure or Operating System platform.

Apart from the above three main service models there several services oriented cloud models categorized based on the services provided by the clouds and some of them are listed below:

1. Storage-as-a-Service (SaaS)
2. Database-as-a-Service(DaaS)
3. Information-as-a-Service (InfaaS)
4. Process-as-a-Service (PraaS)
5. Software-as-a-Service (SaaS)
6. Platform-as-a-Service (PaaS)
7. Integration-as-a-Service (IntaaS)
8. Security-as-a-Service (SeaaS)
9. Management/Governance-as-a-Service (MaaS)
10. Testing-as-a-Service (TaaS)
11. Infrastructure-as-a-Service (IaaS), etc.

2.4. Cloud Deployment models

Cloud has four deployment models. These are public cloud, private cloud, community cloud, hybrid cloud. They are briefed as follows.

2.4.1. *Public cloud*: The public cloud can utilize for general public, anyone can use it.

2.4.2. *Private cloud*: Private cloud is meant solely for an organization.

2.4.3. *Community cloud*: Community is for special community composed of several organizations with shared concerns.

2.4.4. *Hybrid cloud*: Hybrid cloud is a combination of the clouds. (I.e. public, private or community clouds)

2.4.5. *Inter-Cloud*: Inter-cloud or 'cloud of clouds' is a term refer to a theoretical model for cloud computing services based on the idea of combining many different individual clouds into one seamless mass in terms of on-demand operations. The inter-cloud would simply make sure that a cloud could use resources beyond its reach, by taking advantage of pre-existing contracts with other cloud providers.

Physical resources of its infrastructure, or is requested to use resources in a geography where it has the inter-cloud scenario is based on the key concept that each single cloud does not have infinite physical resources or ubiquitous geographic footprint. If a cloud saturates the computational and no footprint, it would still be able to satisfy such requests for service allocations sent from its clients.

III. RELATED WORK

The enterprises are free from the trouble of local maintenance of resources. But there will be considerable risk to provide security, privacy and integrity to the resources at the side of cloud service provider. Specifically the cloud services are managed by the cloud service providers are may not be fully trusted by users while using the service and vice-versa. There may be some confidential things business plans and company resources are personal to the respective organizations in the cloud. To maintain security, privacy and integrity for their resources at the cloud side by sitting at the client side is not an easy task due to the fallowing challenging issues:

- ➢ The guarantee of identity privacy of enterprise resources for example, an enterprise can manage the others in the cloud by doing wrong transactions in other enterprises in the cloud without being traceable. Therefore traceability, which enables the cloud manager (i.e., manager at cloud service provider side) to reveal the real identity of a person is also highly desirable to the enterprises.
- ➢ The guaranty of identity privacy of a member within the enterprise and accessing the resources from inside or outside of the enterprise, for example an employee of an enterprise can do wrong transactions by wasting the resources without being traceable. Therefore, traceability, which enables the manger (company manager or employee of the organization) to reveal the identity of a member or user is also highly desirable.
- ➢ It is necessary, that any user, either an enterprise user or a personal cloud user could be able to enjoy the services by the resources which are allocated to them. More concretely, each user in the cloud is able to access the resources shared by the organization. Compared with single owner system[3], multi owner secure system is more efficient.
- ➢ cloud service manager, enterprise manager, team manager, members, users and personal cloud users are usually dynamic in practice, i.e. new one is

joining with proper registration and approval process and current account revocation for one who is leaving from the organization. With the dynamic nature of the accounts it is very difficult to provide security, privacy and integrity to the resources in the cloud.

Several service techniques [7] and Cryptographic methods [8][1] for resource sharing on not trusted servers of the cloud have been proposed. In these approaches, resources owners use encryption method and distribute the corresponding decryption keys to authorized users. Thus, unauthorized users as well as cloud services cannot know the content of resources because they have no knowledge of the decryption keys. The protection of computer based resources that include hardware, software, data, functions a people against misuse or natural effects such as system security. System security can be divided into four related issues: Security, Integrity, Privacy and Confidentiality.

IV. SYSTEM DESIGN

4.1. Overall System Design

In designing a solution modal for the problem, it is a process of identifying inputs, outputs and explains function of the system. System design is the high level strategy for solving the problem and building a solution modal. In this session I present my proposed model for secure resource sharing in the Enterprise cloud by using three keys at different levels of individual enterprises. The enterprises are providing services to the users by taking services from different clouds and these services can be accessible anywhere (i.e. inside and outside of the enterprise.). Nowadays we are using Inter-cloud (Cloud of Clouds). An Enterprise cloud service provider can provide service to the other enterprises, enterprise users and personal cloud users. An Enterprise will have a manager for maintaining the overall enterprise resources allotted from the cloud and can have a number of teams with a manger to each team along with team members.

Who ever may be, to get the cloud services enterprises, managers, users and personal user has to register in the cloud with some standard authentication procedure. Each category of people will have a separate level of registration with different challenges to achieve different goals at different clouds from home the actual services were rendered. After the successful completion registration and verification process the Keys will be distributed directly to the user by using secured channel through e-mail or mobile. The three types of keys in my proposed for each and every enterprise cloud user are as follows:

1. Enterprise Key - the key allotted to the individual enterprises by cloud service provider.
2. Manager Key - the key allotted to the individual manager in each and every enterprise.
3. Member Key - the key allotted to the members of different teams in an enterprise.

In case of personal cloud users there will be only one user so that, it will be treated as one user enterprises and three keys will be allotted to the same user. One user can play different roles (i.e. Entrepreneur, Manager and Member) in the enterprise and the resources allocation should be handled by the cloud service provider. The overall registration and key distribution is shown in the billow system model.

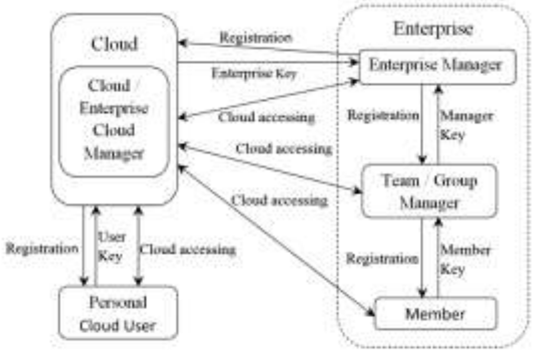

Figure 2: Triple Key Cloud Security Model

4.2. Design Goals

Design goals of the proposed system include user access control, shared resource confidentiality, traceability and efficiency in the cloud as follows:

User access control: Who ever may be the user, an Entrepreneur, Manager or Member the requirement of user access control is twofold. First, authorized users are able to use the allotted resources in the cloud for doing transactions. Second, unauthorized users cannot access the cloud resources at any time and revoked users will be incapable of using cloud again once they are revoked.

Shared resources confidentiality: Resource confidentiality requires the unauthorized user including the cloud is incapable of Traceability: Anonymity guarantees that group members can access the cloud without revealing his/her real identity. For example, an inside attacker may steal and share a mendacious resources to derive substantial benefit. Thus, to tackle the inside attack, the Cloud manager should have the ability to reveal the real identities of Resource owners.

Efficiency: The efficiency is defined as follows: Any Enterprise member can do transactions and share permitted cloud resources allocated to the enterprise with others in the company by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can access all the resources permitted to him before his participation without contacting with the enterprise owner and it is same in the case of Cloud Manager, Team Manager up to their level access in the cloud.

PROPOSED TECHNIQUE: TK-RST

5.1. *Overview*

To solve the challenges presented above, we propose a dynamic resource sharing technique for dynamic managers, members and users in the enterprise cloud. The main contributions of TK-RST include: We propose a triple key resource sharing technique (TK-RST) for enterprise cloud. It implies that by using any of these three Keys, i.e. Enterprise key, Manager Key and Member key, any member in the enterprise can securely utilize and share the resources with others by the not trustable cloud. Our proposed system is able to support dynamic enterprise members in the cloud efficiently. Specifically, new permitted members can directly access the provided level of cloud resources that are allocated to enterprise before their participation without contacting with cloud enterprise owners. User (Enterprise Manager, Team Manager and Member) revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving user access control to members, which guarantees any member in the cloud anonymously utilize the permitted level of cloud resource. Moreover, the real identities of transaction owners can be revealed by the cloud manager when disputes occur.

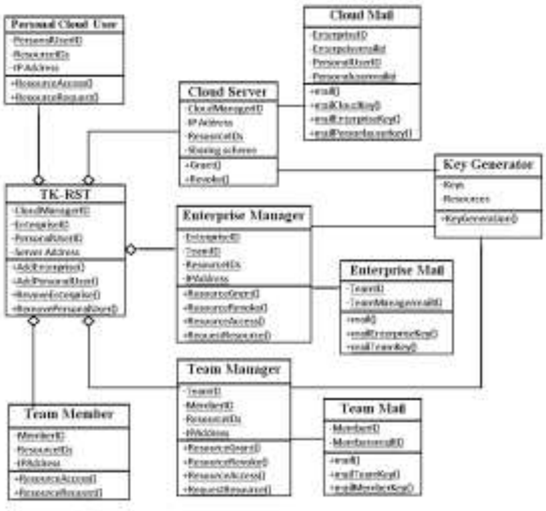

Figure 3: Class Diagram

5.1. *Schema Description*

The TK-RST in cloud has been divided into five modules enterprise manager, team manager, team member, cloud Server and key generator. These are briefed as follows:

- *Enterprise manager*: Enterprise manager take charge of system parameters generation, enterprise registration, team registration, team manager registration and revealing the real identity of a team manager who is creating disputes in resource usage. In the given example the enterprise manager is acted by the administrator of the company or CEO of the company. Therefore we assume that the enterprise manager is fully trusted by the other parties.
- *Team Manager*: Team manager taken charge of system parameters generation for his team, team member registration, team member revocation and revealing the real identity of a member who is creating disputes. In the given example the team manager is acted by the team head of the particular team created by the enterprise manager. Therefore, we assume that the team manager is fully trusted by the other parties regarding to that team.
- *Team member*: Team members are a set of registered users those who can access the allocated resources to make a transaction for company in the cloud server and share the resources with others in the same team. In our example, the program plays the role of team member. Note that, the team membership is dynamically changing due to the new member registrations i.e. new program participation in the company and revocation of existing employee i.e. resignation of a program in the team or transfer of an employee to another team in the same company.
- *Cloud Server*: Cloud is operated by CSP's and provides priced abundant cloud services. However, the cloud is not fully trusted by the users since the CSP's are very likely to be outside of the cloud users trusted domain. We assume that the cloud services are honest but curious. That is, the cloud server will not maliciously misuse the resources allocated to the users or modify the transactions done and services provided to the user due to the protection of service auditing schemes, but will try to know the transactions, resources and the identities of the cloud users.
- *Key generator*: Any member can access the resources allocated to him and share these resources with others in the organization by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users don't need to update their private key or re-encryption operations. New granted users can use all the allocated resources to their level to do work are learn from previous transaction before his participation without contacting the enterprise owner or resource owner.

V. RESULTS AND DISCUSSION

The proposed TK-RST technique of sharing resources in enterprise cloud server is demonstrated using the private cloud setup with open stack. For convince I took data as service and transactions on this data are controlled by my proposed technique TK-RST for an enterprise cloud having only one enterprise. XAMPP (Apache, Tomcat and MySQL) to host the services at Server, Bootstrap for user interface and Net Beans is also used for most of the coding part. At the client side also Bootstrap is used for building client side functionality and user interface that are used in demonstration of the proposed work. I used cloud mail services for mail communication to distribute various keys to the user.

XAMPP is a small and light Apache distribution containing the most common web development technologies in a single package. Its contents, small size, and portability make it the ideal tool for students developing and testing applications in PHP and MySQL. XAMPP is available as a free download in two specific packages: full and lite. While the full package download provides a wide array of development tools, this article will focus on using XAMPP Lite which contains the necessary technologies that meet the Ontario Skills Competition standards. As the name implies, the light version is a small package containing Apache HTTP Server, PHP, MySQL, phpMyAdmin, Openssl, and SQLite.

Twitter Bootstrap is the most popular front end frameworks rrently. It is sleek, intuitive, and powerful mobile first front-end framework for faster and easier web development. It uses HTML, CSS and JavaScript.

NetBeans IDE is a free, open source, popular (with approximately 1 million downloads), integrated development environment used by many developers. Out of the box, it provides built-in support for developing in Java, C, C++, XML, and HTML. And this author especially likes the support for editing JSPs, including syntax highlighting, HTML tag completion, JSP tag completion, and Java code completion.

At front user will have login page. New user has to register first to get secret key and existing user can login in by using his unique user id, password and secret key. Enterprise has to register in Enterprise Cloud, Manager has to register in Enterprise and Member has to register in a team of the enterprise. The main functions are as follows:

- ❖ Login & Registration (User ID, Password and Secret Key)
- ❖ Enterprise Cloud page with Enterprise management functions
- ❖ Team Manager page with Team management functions
- ❖ Member page with Member functions.

All the above modules are tested and it is proved that my proposed TK-RST technique is good with three layers of security for enterprise cloud.

VI. CONCLUSION

In this paper, I designed a triple key resource sharing technique, for dynamic enterprises in the cloud. In this TK-RST, a user is able to use the resources along with others in the cloud without revealing identity privacy to the cloud. Additionally, this TK-RST supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new members can directly share the allocated resources in the cloud before their participation. Moreover, the resource management overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

VII. FUTURE ENHANCEMENTS

As future work, we would like to extend the type resources being hosted in the cloud server. In our project I tested only on text document data services, which can be further extended to different type of resources in the enterprise cloud.

REFERENCES

[1] Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, "Security on Cloud Using Cryptography", IJARCSSE, Volume 5, Issue 3, March 2015.

[2] NIST Cloud Computing Special publication, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, July 201.

[3] Sun Microsystems, “Introduction to Cloud Computing Architecture,” White paper, 1st Edition, June 2009, pp. 1-40.

[4] “Twenty Experts Define Cloud Computing”, SYS-CON Media Inc, http://cloudcomputing.sys-con.com/read/612375_p.htm, 2008.

[5] “What is Cloud Computing?”, Whatis.com. http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci1287881,00.html, 2008.

[6] “Twenty Experts Define Cloud Computing”, SYS-CON Media Inc, http://cloudcomputing.sys-con.com/read/612375_p.htm, 2008.

[7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius:Securing remote untrusted storage,” in Proc. of NDSS, 2003, pp.131-145

[8] T. Esther Dyana, S. Maheswari, "A Secure Data Storage and Trustworthy Resource Sharing In Cloud Computing Environment", IJARCET, Volume 4 No.4, April 2015.

AUTHOR

V. Ashok kumar was born in Srikalahasti, Andhra Pradesh, India on May 22, 1982, Since 2006, he has been working as an Assistant Professor, Dept. of CSE, Srikalahasteeswara Institute of Technology, Srikalahasti, India. He received B.Tech (CSE) in 2005 from SKIT, Srikalahsti, M.Tech in 2010 from School of IT, JNTUH, Hyderabad. His research interests Virtualization Techniques and Cloud Computing.