An Effective Third Party Auditing in Private Cloud using Kerberos

Indra Priyadharshini S[1] Akila K[2] Sathish Kumar[3]
[1,2]Assistant Professor [3]System Analyst
[1,2,3]Department of Computer Science & Engineering
[1,2]RMK College of Engineering and Technology, Chennai, India [3]Cognizant Technology Solutions, Chennai, India

Abstract— Cloud computing is the emerging phase in the Internet's evolution, where it provides means through which power of computing, infrastructure of computing, computer applications and other business services can be delivered to businesses and individual as a service wherever and whenever they need. Using cloud storage, users can store their data remotely and enjoy the required high-quality applications and services from a shared pool of Configurable computing resource without the burden of local data storage and maintenance. A directory server is created that allows its registered users to access server information with remote logins that are secured by Kerberos authentication protocol (Third party Auditing-TPA) for secure communication over insecure channels. The original password or user credential, does not travel in the network and thus the transaction is more secure. Unlike usual authentications which verify login credentials with stored credentials, Kerberos authentication works by using the concept of principal credentials that are temporary credentials and temporary keys that are time stamped. A key distribution center manages production of tokens. Verification is done by a two way authentication of the principal login credentials by combining the generated token and the principal login in an encryption decryption process along with the stored credentials.

Key words: Cloud Computing, Third Party Auditor, Kerberos Protocol, LDAP

I. INTRODUCTION

Cloud computing is a very competitive industry, where cloud providers are always pressured to provide higher computation and storage capabilities, while reducing costs. Cloud providers are therefore tempted to lower the computational and storage space allocated to their users, without their knowledge. A deceptive CSP may violate the SLA by moving some of its users data and services to a lower quality of service level, saving a great deal of money. Un-fortunately, a deceptive CSP may avoid TPA detection [3][4] by respecting SLAs only when auditors are monitoring that CSP. Avoiding detection is possible due to the fact that a CSP may provide auditors with preferential access to cloud users data and services, which prove to TPAs that the CSP is adhering the SLA. In reality, however, the services of a cloud user are not allocated with resources, specified by the SLA.Kerberos is a computer network authentication protocol which work on basis of 'tickets' to allow nodes communication over a non-secure network to prove their identity to one another in secured manner. Kerberos develops on symmetric key cryptography and requires trusted third party, and by chance, may use cryptography using public key during certain phases of authentication.To fully ensure the data integrity and save the cloud user's computation resources as well as to reduce online burden, it is of great importance to enforce public auditing service for cloud data storage, so that users may adapt to an independent TPA who has expertise and capable to audit the outsource data when needed.It is an attempt to show the security by applying various techniques and justify the performance of proposed schemes through concrete experiments and comparisons.It is our attempt to create a directory server that allows its registered users to access server information with remote logins that are secured by Kerberos authentication protocol [1] [2]for secure communication over insecure channels.

II. DIRECTORY SERVICES OVERVIEW

A directory service [1] called as naming service, maps the network resources names to their respective network addresses. The name service type of directory provides with the name that locates a resource so that the user does not have to remember the physical address of a network resource. Each resource on the network is considered to be an object on the directory server. Information about a each resource is stored as attributes of that object. Also Information within objects can be made secure so that only authenticated users are able to access it. More enhanced directories are designed with namespaces. Here the design process is similar to Identity management.

A. LDAP:

LDAP, Lightweight Directory Access Protocol [3], that is used to communicate with one another about the data in a directory and this provides a standard language that directory client applications and directory servers use. LDAP applications can add, search, delete and modify data in directory. LDAP preserves most features of DAP [3] at minimal cost. LDAP uses an access protocol with open directory running over TCP/IP and uses simplified encoding methods. LDAP directories differ from other relational databases. In LDAP, looking up of data in tables is not done. Instead, data is looked up in trees, if you portray the contents of a file system, you get a diagram identical to the tree. The data is not in rows and columns, but in entries. These entries are similar to entries in the phone book. Entries sometimes even contain phone numbers. An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The root directory (the starting place or the source of the tree)
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers).

1) Implementation of LDAP:

The given steps will take us to an operational LDAP server:

1) Install packages
2) Edit configuration files
3) Generate Dynamic Configuration Files
4) Create an LDIF data file
5) Start the LDAP database
6) Load the LDIF data file into the database
7) Test LDAP
8) Manage

III. PRIVATE CLOUD ARCHITECTURE

Private cloud is the implementation of cloud storage on resources dedicated to your organization, whether they exist inside the premises or outside the premises. With a private cloud, you acquire most of the advantages of public cloud computing such as self-service, scalability, and elasticity, combined with the additional control and customization available from dedicated resources. Two models for cloud services can be delivered in a private cloud: Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). With IaaS, you can use infrastructure resources (compute, network, and storage) as a service, while PaaS offers application platform as a service. A form of cloud storage where the enterprise data and cloud storage resources both reside within the enterprise's data center and behind the firewall. Internal storage clouds, also referred to as private cloud storage where the services are managed inside the data center. Eventually it carries higher capital and maintenance costs than public cloud storage services due to the enterprise needing to provide the space for data centre, connectivity for network, power and cooling. Private cloud storage does help resolve the potential for security and performance concerns while still offering many of the benefits of cloud storage such as reliability, faster deployment, scalability and the option of management by a provider of specialized cloud storage.

IV. SECURITY ISSUES IN CLOUD

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data. There is another chance where a malicious user can penetrate the cloud by impersonating an existing user, thereby getting the entire cloud infected. This affects a number of customers who share the infected cloud. There are four types of issues raise while discussing security of a cloud. They are Data issues, Privacy issues, Infected Application and Security issues.

A. Data-Issues:

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud system. Initially, if data is on cloud, anyone from any place, any time can access data from the cloud because data is common, private and sensitive in a cloud. Simultaneously, many cloud computing service consumers and providers access and modify data. Thus there is a need for some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and to the cloud service provider. So there is a greater chance for data to be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud service provider shuts down his services due to some financial or legal problem then there will be loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accessible to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

B. Privacy-Issues:

The cloud service provider must ensure that the customers' personal information is well secured from other providers, other customers and users. As most of the servers are external, the cloud service provider should also ensure of who is accessing the data and who is maintaining the server so that it enables the provider to protect the customers' personal information.

C. Infected-Application:

Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and server maintenance. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

D. Security-Issues:

Cloud computing security must be carried out in two levels. Firstly, on provider level and secondly on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may face. Even though the cloud service provider has provided with a good security layer for the customer and user, the user should ensure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is said to be good only when it has good security offered by the service provider to the user.

V. ARCHITECTURE OF THE MODEL

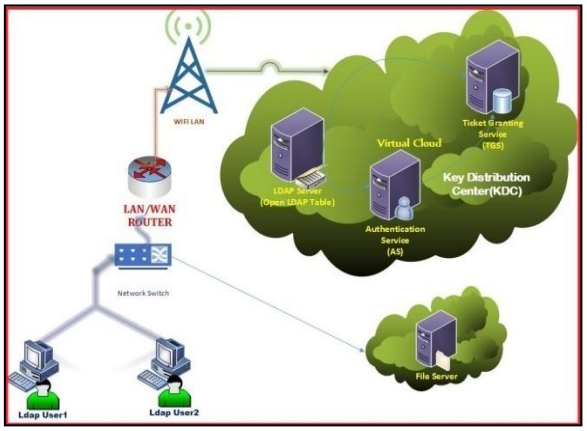

Fig. 1: Architecture of the Model

VI. THIRD PARTY AUDITOR-KERBEROS PROTOCOL

Kerberos is an authentication protocol where it achieves all the required security goals for the system like integrity,authentication,confidentiality etc.kerberos acts as a security system where it can help in stopping the stealing of information in the network when travelling from one place to another. It is based on secret key encryption technology, it uses RSA for encryption to extend the security for system

A. Terminologies:

1) Key:

Kerberos uses private key encryption. Each Kerberos principal is being assigned with a large number that is its private key which is known only to that principal and Kerberos alone. So the private key is applied to the user's password.

2) Key Distribution Centre:

KDC is the heart of the Kerberos. This center provides the Kerberos authentication services by issuing encrypted tickets that required secret keys to decode. On the whole KDC handles the distribution of keys and tickets.

3) Ticket Granting Server:

TGS does the work of issuing tickets to clients upon request.

4) Ticket Granting Ticket:

This is issued by the authentication server. This TGT is encrypted in the user's password which is known only to the user and KDC.

5) Session-Key:

Session keys are the temporary private keys generated by Kerberos .These keys are known to the client and it is used to encrypt the messages between the client and the server.

B. Working of Kerberos:

Kerberos is a mechanism that operates on a ticket granting technique using TGS. The client must first call the KDC and it should request for a TGT. The TGT consists of the following like the network address, client ID, validity period of the ticket. The secret key of TGT is used to encrypt session key. The client uses this TGT to get the ticket from the TGS. So now the client uses the ticket to access the server. The server decrypts the ticket using its own secret key and sends the message to the client. Now the client decrypts the message using the session key and checks the time stamp for the updates. If the time stamp is properly updated then the client can trust the authenticity of the server. So this process can avoid the usage of password mechanism that can be easily hacked.

The authentication process can be depicted as follows:

1) The client requests for a TGT from KDC.
2) The AS sends the TGT in encrypted form and the session key to the client.
3) From the TGS the client requests for the server access.
4) TGS sends the encrypted session key and the ticket to the client.
5) The client sends the ticket to the server.
6) server can send an encrypted time stamp to client if necessary.

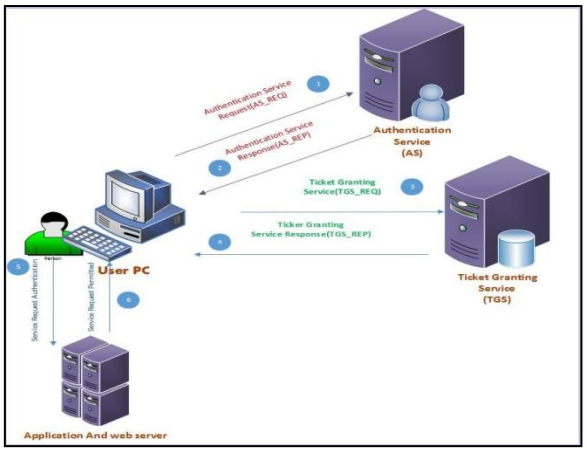

Fig. 2:

VII. ADVANTAGES AND LIMITATIONS:

The overall model discourages a cloud service provider(CSP) from deceiving its clients. This is true because any user who request to access client data and services that are originating from auditing volunteer, rather than just a user. This model makes the TPAs convince clients to subscribe for TPA services.

A. Limitations:

1) The first limitation is the participation of more volunteers in the CSP.
2) Secondly the dependability of those volunteers.
3) In Kerberos approach, the system entirely depends on passwords for the authentication of user. If the passwords are stolen, then the probability of system attack is unlimited.

VIII. CONCLUSION

Cloud computing is the solution that relieves businesses from the task of managing their IT. The client data and services are managed by the providers of CSP. But security in the present scenario has become a more rational issue. Adding kerberos to a network can increase the overall security to the users and administrators of that network. Here the Kerberos provides distributed authentication service that allows a process running on behalf of a principle to prove its identity to a verifiers without sending the data across the network that might allow an attacker to subsequently impersonate the principal.

REFERENCES

[1] M. Armbrust et. al (2010). A view of cloud computing. Communications of the ACM, 53(4): 50-58.
[2] P. Patel, A. Ranabahu and A. Sheth. Service level agreement in cloud computing. In Proc. of OOPSLA Cloud Computing workshop (2009).
[3] J. Xu. Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage. IACR Cryptology ePrint Archive (2011): 304.
[4] M. Hussain and H. Abdulsalam. Software Quality in the Clouds: A Cloud based Solution. Springer Journal of Cluster Computing, in press.
[5] Z. Qi, L. Cheng, and R. Boutaba (2010). Cloud computing: state-ofthe-art and research challenges.

Journal of Internet Services and Applications 1(1): 7-18.
[6] http://csrc.nist.gov/groups/SNS/cloud-computing/
[7] http://csrc.nist.gov/groups/SNS/cloudcomputing/cloud-def-v15.doc
[8] Virtualization – The ability to increase computing efficiency http://broadcast.rackspace.com/hosting_knowledge / hitepapers/Revolution_Not_EvolutionWhitepaper.
[9] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud ComputingV2.1,http://www.cloudsecurityalliance.org/,December2009
[10] https://incometaxindiaefiling.gov.in/portal/faq_signature.do
[11] Kalyani D. Kadam,Sonia K. Gajre,R. L. Paikrao, Security issues in Cloud Computing

