International Journal of Modern Engineering Research (IJMER)
www.ijmer.com *Pp-42-46* *ISSN: 2249-6645*

Secure Substantiation in Cloud Computing Environment

Raja Shree S.
Jerusalem College of Engineering, Anna Univeristy Narayanapuram, Chennai 600 117 India

ABSTRACT: *Cloud computing is an emerging style of IT delivery that intends to make the Internet the ultimate home of all computing resources- storage, computations, and accessibility. It holds the promise of helping organizations because of its performance, high availability, least cost and many others. But the promise of the cloud cannot be fulfilled until IT professionals have more confidence in the security and safety of the cloud.. However cloud computing has the security issues such as service availability, massive traffic handling, application security and authentication. In this user authentication requires high guaranteed security. To ensure secure authentication of client in the cloud environment, an effective method is being proposed. This paper mainly focused on authentication issues in the cloud computing environment, where an enhancement is made to the intrusion login by Kerberos authentication service having fingerprint as its base.*

KEYWORDS: *cloud computing, Kerberos, authentication*

I. INTRODUCTION

The study of 1,300 U.S. and U.K. executives, conducted by Rackspace Hosting finds cloud engagements are delivering positive impacts, from cost savings to more innovation. Interestingly, it also reveals that most of these executives see cloud as laying the groundwork for the next entrepreneurial boom. Sixty-two percent of respondents either agreed totally or somewhat with the statement that "cloud computing is a key factor in the recent boom of entrepreneurs and start-ups," the survey finds. Twenty-five percent agreed strongly with this idea. Cloud computing may be a shot in the arm our economy needs. Because it enables entrepreneurs and innovators to start up new ventures with minimal capital requirements — most of what they need is now available as online services, sometimes at no cost. As we ponder unemployment and underemployment in our economy, the availability of cheap cloud computing may be laying the groundwork for a startup boom, the likes we have never seen before. Cloud provides a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. This applies to departments of larger organizations as well — designing new products, without the need to go through corporate finance and IT approvals definitely is a great way to instill entrepreneurial spirit. Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. Clouds are of particular commercial interest not only with the growing tendency to outsource IT so as to reduce management overhead and to extend existing, limited IT infrastructures, but even more importantly, they reduce the entrance barrier for new service providers to offer their respective capabilities to a wide market with a minimum of entry costs and infrastructure requirements – in fact, the special capabilities of cloud infrastructures allow providers to experiment with novel service types at the same time reducing the risk of wasting resources. Cloud is not only simple collecting the computer resource, but also provides a management mechanism and can provide services for millions of users simultaneously. The composition of the paper is as follows: chapter 2 Related works looks at the back ground of cloud computing. Chapter 3 describes user authentication services in cloud computing and problems of them. Chapter 4 describes the proposed work for user authentication in cloud computing. Chapter 5 draws the conclusion.

II. BACKGROUND OF CLOUD COMPUTING

2.1. What is cloud computing?

The official definition from the National Institute of Standards and Technology reads:"Cloud computing is a model for enabling 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." Cloud computing differs from the classic client-server model by providing applications from a server that are executed and managed by a client's web browser, with no installed client version of an application required. As further defined, Cloud Computing refers to the use and access of multiple server-based computational resources via a digital network to access the World Wide Web. Cloud users may access the server resources using a computer, net book, pad computer, smart phone, or other device. In cloud computing, applications are provided and managed by the cloud server and data is also stored remotely in the cloud configuration. Users do not download and install applications on their own device or computer; all processing and storage is maintained by the cloud server. The on-line services may be offered from a cloud provider or by a private organization.

2.2. Services provided by cloud

Cloud Computing is a general term that provides hosted services over internet. Broadly speaking, these services are divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS refers to the sharing of hardware resources. The resources are all virtual machines, which has to be managed. E.g. Amazon Ec2,Right Scale. PaaS aims to protect the data, which is especially important in case of storage as a service. E.g. Amazon SSS, Microsoft Azure. SaaS provides different type of application and web services to the end users. E.g. google , Sales-force. In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the

remote server at some other place.

2.3. Types of Cloud

The types of Cloud computing can be classified according to deployment. This deployment can increase or decrease the major cloud computer problems, the security and privacy can be increase or decrease upon the choice of cloud. These classifications are also based on different parameters like, the customer requirement, location of cloud and by their architecture. There are basically four types of clouds, which are described below-

Public cloud: This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per usage model.

Private Cloud: This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

Community Cloud: This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

Hybrid Cloud: This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

III. ISSUES IN USER AUTHENTICATION

Authentication is the verification of the identity of a party who generated some data, and of the integrity of the data. A principal is the party whose identity is verified. The verifier is the party who demands assurance of the principal's identity. Data integrity is the assurance that the data received is the same as generated. Authentication mechanisms differ in the assurances they provide: some indicate that data was generated by the principal at some point in the past, a few indicate that the principal was present when the data was sent, and others indicate that the data received was freshly generated by the principal. Mechanisms also differ in the number of verifiers: some support a single verifier per message, while others support multiple verifiers. A third difference is whether the mechanism supports non-repudiation, the ability of the verifier to prove to a third party that the message originated with the principal.

Because these differences affect performance, it is important to understand the requirements of an application when choosing a method. For example, authentication for electronic mail may require support for multiple recipients and non-repudiation, but can tolerate greater latency. In contrast, poor performance would cause problems for authentication to a server responding to frequent queries.

Other security services include confidentiality and authorization. Confidentiality is the protection of information from disclosure to those not intended to receive it. Most strong authentication methods optionally provide confidentiality. Authorization is the process by which one determines whether a principal is allowed to perform an operation. Authorization is usually performed after the principal has been authenticated, and may be based on information local to the verifier, or based on authenticated statements by others.

A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure. In which if a user (either employee or anonymous) want to access the data if it belongs to protection then user have to register itself. Now suppose the user registered itself for accessing data, Organization will provide username and password for authentication. At the same time organization sends the username to cloud provider .Now when user sends request along with username to access the data to cloud provider, the cloud provider first check in which ring requested data belong. If authentication is required, it first checks the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches it redirect the request to company for authentication. Now the user sends password for authentication, and after authentication it redirect the request to cloud provider to access resource .If user-name and password doesn't match then user is not allow to access their account.

3.1 Kerberos Authentication Service

3.1.1 What is Kerberos?

Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. Kerberos was developed in the mid-'80s as part of MIT's Project Athena.

As use of Kerberos spread to other environments, changes were needed to support new policies and patterns of use. To address these needs, design of Version 5 of Kerberos (V5) began in 1989 . Though V4 still runs at many sites, V5 is considered to be standard Kerberos.

3.1.2 Kerberos –an Overview

The Kerberos Authentication System uses a series of encrypted messages to prove to a verifier that a client is running on behalf of a particular user. The Kerberos protocol is based in part on the Needham and Schroeder authentication protocol, but with changes to support the needs of the environment for which it was developed. Among these changes are the

use of timestamps to reduce the number of messages needed for basic authentication [6], the addition of a ``ticket-granting" service to support subsequent authentication without re-entry of a principal's password, and different approach to cross-realm authentication (authentication of a principal registered with a different authentication server than the verifier).

The remainder of this section describes the Kerberos protocol. The description is simplified for clarity; additional fields are present in the actual protocol. Readers should consult RFC 1510 for a more thorough description of the Kerberos protocol.

Though conceptually, Kerberos authentication proves that a client is running on behalf of a particular user, a more precise statement is that the client has knowledge of an encryption key that is known by only the user and the authentication server. In Kerberos, the user's encryption key is derived from and should be thought of as a password; we will refer to it as such in this article. Similarly, each application server shares an encryption key with the authentication server; we will call this key the server key.

Encryption in the present implementation of Kerberos uses the data encryption standard (DES). It is a property of DES that if cipher text (encrypted data) is decrypted with the same key used to encrypt it, the plaintext (original data) appears. If different encryption keys are used for encryption and decryption, or if the ciphertext is modified, the result will be unintelligible, and the checksum in the Kerberos message will not match the data. This combination of encryption and the checksum provides integrity and confidentiality for encrypted Kerberos messages The client and server do not initially share an encryption key. Whenever a client authenticates itself to a new verifier it relies on the authentication server to generate a new encryption key and distribute it securely to both parties. This new encryption key is called a *session key* and the Kerberos ticket is used to to distribute it to the verifier.

The Kerberos ticket is a certificate issued by an authentication server, encrypted using the server key. Among other information, the ticket contains the random session key that will be used for authentication of the principal to the verifier, the name of the principal to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is not sent directly to the verifier, but is instead sent to the client who forwards it to the verifier as part of the application request. Because the ticket is encrypted in the server key, known only by the authentication server and intended verifier, it is not possible for the client to modify the ticket without detection.

Limitations of Kerberos

Limitations of Kerberos have been described in the literature. Though most are a matter of preference or apply to V4 and early drafts of V5, a few are fundamental and are discussed here. In particular, Kerberos is not effective against password guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user. Similarly, Kerberos requires a trusted path through which passwords are entered. If the user enters a password to a program that has already been modified by an attacker (a Trojan horse), or if the path between the user and the initial authentication program can be monitored, then an attacker may obtain sufficient information to impersonate the user. Kerberos can be combined with other techniques, as described later, to address these limitations.

To be useful, Kerberos must be integrated with other parts of the system. It does not protect all messages sent between two computers; it only protects the messages from software that has been written or modified to use it. While it may be used to exchange encryption keys when establishing link encryption and network level security services, this would require changes to the network software of the hosts involved.

Kerberos does not itself provide authorization, but V5 Kerberos passes authorization information generated by other services. In this manner, Kerberos can be used as a base for building separate distributed authorization services.

Kerberos uses strong encryption and a complex ticket-granting algorithm to authenticate users on a network. Also of interest to many of users, Kerberos has the ability to distribute "session keys" to allow encrypted data streams over an IP network each user for connecting to the cloud at the first shoud make the profile and user ID. After that it must get the password and also the information of all participating user such as User ID, hashed password will save in the large Data Base for more secure. All user are register with the Kerberos server. In this method each user want connect to the cloud server at the first time he or she logs on to workstation. Kerberos issues ticket to the client as one ticket per session. Whenever the Client(C) request the ticket to the Authentication Server (AS) with its own identifier (IDc) and with the identifier of the ticket granting server(ID tgs),the AS responds with a ticket (i.e) encrypted with a key(Kc) that is derived from users password. When this response arrives, the user decrypts it by using his own password. If the correct password is supplied, the ticket is successfully recovered.

C->AS : IDc || IDtgs
AS->C : EKc[Ticket tgs]

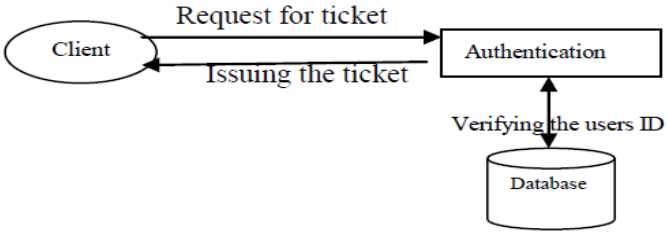

Figure 1 Ticket per session

Now this hash value gets registered with the users hash value in AS database. Whenever the user sends request to

the AS, the AS verifies the user identity in its data base and then it issues the ticket to the user.

IV. PROPOSED WORK

In Kerberos authentication service the AS stores the hash value of all the users' password. Therefore the hacker may hack the database and retrieves the password. The work being proposed here is, instead of storing the hash value of users password, here we can store the hash value of the particular users finger print along with his password hash value. The ticket gets encrypted with the hash value of the finger print and password. So that the user can decrypt the data only by giving his own finger print and password. Even if the hacker hacks the hash value then there is no use of that hash value. The session ticket gets decrypted only with the particular persons finger print and password.

4.1 Computation of Hash Value and storing

Here a fingerprint scanner scans the finger print of the user and converts it into binary form using any modern technique.Take this binary form as input and compute the hash value by using SHA-1 algorithm.

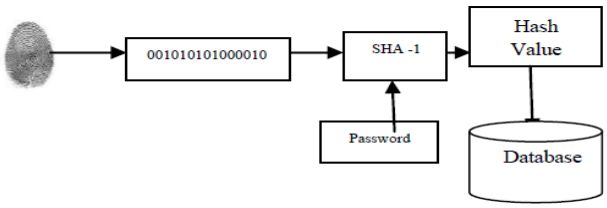

Figure 2 Hash value computations

4.2 Authentication Process

If the user wants to acess the cloud service ,the user first request a session ticket to the AS by giving his ID(IDc) and the ticket granting server ID(IDtgs).The AS checks the user ID in its database and issues the ticket to the user which is get encrypted with the hash value of the user.The user can able to use the ticket only by decrypting it using his finger print and password.If both matches the ticket gets decrypted .By using this ticket the user can enjoy the services of cloud.

IDc || IDtgs

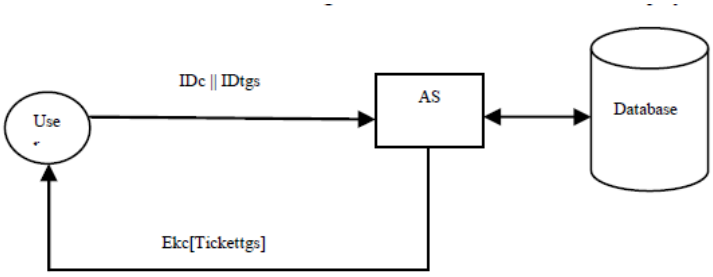

Figure 3 Requisition Process

Here the AS stores all its user passwords hash value in a database. The hacker may hack the database and able to retrieve the password from the hash value . Then the hacker may enjoy the service of the ticket.

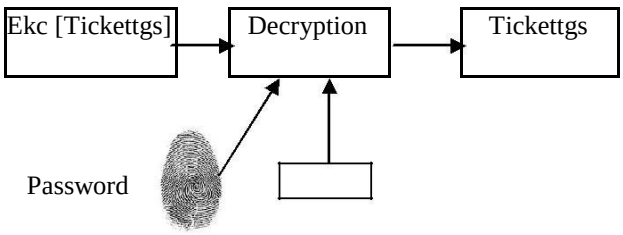

Figure 4 Decryption Process

V. Conclusion

Cloud Computing is a fast growing technology in the modern world but it needs some more security features to enhance it in the business world. Security depends upon the way Cloud service provider allows its client to come and get registered with his cloud network.This paper investigates about the problem of authentication in cloud computing envoirnment.A method is being proposed to ensure the secure authentication in the cloud by Kerberos authentication service with finger print as its base.. The future work is to research every component of the secure architecture in detail.

References

[1] John E. Canavan "Fundamentals of Network Security", Library of Congress Cataloging-in-Publication Data ISBN 1-58053-176-8 (alk. paper)

[2] Gawali M. B., R. B. Wagh, S. P. Patil "Enhancement for data security in cloud computing environment", international journal of internet computing.

[3] Torry Haris "cloud computing an overview", http://www.whitepapersdb.com/white- paper/9201/cloud-computing-an-overview

[4] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham Mirza Aamir Mehmood "Implementation of Eap with RSA for Enhancing The Security of Cloud Computing" International Journal of Basic and Applied Sciences ,1 (3) (2012)177-183

[5] Joshi Ashay Mukundrao "Enhancing Security in Cloud Computing Information and Knowledge Management", ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011

[6] Kai Hwang ,Deyi Li "Trusted Cloud Computing with Secure Resources and Data Coloring" ,Published by the IEEE Computer Society 1089-7801/10/$26.00 © 2010

[7] Mandeep Kaur, Manish Mahajan " Using encryption Algorithms to enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013

[8] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,http://www.cloudsecurityalliance.org/, December 2009

[9] B. Clifford Neumann,Theodore Ts'o "Kerberos: An Authentication Service for Computer Networks",IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994.