International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-1 Issue-14 March-2014

A Secure Authenticate Framework for Cloud Computing Environment

Nitin Nagar[1], Pradeep k. Jatav[2]

Abstract

Cloud computing has an important aspect for the companies to build and deploy their infrastructure and application. Data Storage service in the cloud computing is easy as compare to the other data storage services. At the same time, cloud security in the cloud environment is challenging task. Security issues ranging from missing system configuration, lack of proper updates, or unwise user actions from remote data storage. It can expose user's private data and information to unwanted access. it consider to be biggest problem in a cloud computing. The focus of this study based on the secure cloud framework and to define a methodology for cloud that will protect user's data and highly important information from malicious insider as well as outsider attacks. It also protects their data from service hijacking with LDAP authentication.

Keywords

Cloud computing, Security, Authentication, LDAP.

1. Introduction

Cloud computing is one of the important research aspects of distributed computing. Companies such as Google, IBM, saleforce.com, and Microsoft are the biggest player of cloud computing environment. Cloud computing contains to services, applications, and data storage delivered online through powerful file servers. Deployment of cloud computing depends on whether the cloud is a private, community, public, or hybrid one. Private clouds are operated for a particular organization, whereas community clouds are mutual by a number of organizations.

Public clouds are available to the common public or large groups of Industries, while hybrid clouds combine public and private elements in the same data center. There are three types of models for providing the services of cloud. These three models are often referred as the SPI (Software, Platform and Infrastructure) model. These services are known as SaaS, PaaS and IaaS. These services are used to make IT Infrastructure scalable, reliable and cost effective.
Sometimes conventional data center best fit for the organization, but for business agility and economical reason cloud is imported reason for the companies [1]. In this paper, security concern of cloud computing will be analyzed and propose a secure framework for cloud computing. The rest of the paper is organized as follows. The section 2 presents literature survey on various cloud computing challenges. The section 3 states problem in security challenges and issues in adoption of cloud computing. In section 4, we proposed work with architectural view. The section 5 presents methodology of proposed work with various aspects. The section 6 presents related work with various aspects. The section 7 states conclusion and future work and finally we incorporate references.

Manuscript received February 06, 2014.
Nitin Nagar- International Institute of Professional Studies, Devi Ahiliya University, Indore, India.
Pradeep k. Jatav - International Institute of Professional Studies, Devi Ahiliya University, Indore, India.

2. Literature Review

Recently cloud computing security received significant attention from IT industries and research communities as there are still several unresolved issues which needed to be addressed before important development take place. There is a file system that provides a secure file storage service. Currently, each web application stores its own user data, which is not only burdens the applications with storing, managing, and securing user data but also dispossess users from controlling their own data [2].

For improvement in security, analyst have their different view as privacy is an important issues in Cloud computing in terms of user trust and need to be considered at every phase of design [3]. Sometime it happens that without awareness of company's detail user record their data; companies may send user's sensitive information to other companies for economical reason, from transformation of data cyber criminal may steal the user email and bank's detail etc. The awareness is also increases for the need for design for privacy from both companies and government organization [4]. Authentication may the required user name or password or any of the authentication techniques include hardware token,

software token, digital certificates on smart cards and USB Tokens, out-of-band authentication and biometric [5]. It is observed that everyday new security advisors are published [6] [7].

In this paper, security concern of cloud computing will be analyzed and propose a secure framework for cloud computing.

3. Problem-Security challenges and issues of cloud computing.

The cloud computing security has to be part of company's overall security strategy. Security risks break and threats can come in so many forms. It comes from so numerous places that many companies take a comprehensive approach to security management across IT and the business function. For example, many companies tracks someone's identity by latest technology whether this person enters a company's building or access corporate information, either from company's perimeter or from any other external location[8]. A company planning to secure cloud environment will generally focus on the broad range of potential vulnerabilities to its data center. It is also necessary that safeguard sensitive corporate, customer, and partners highly information whenever it is located. A company's software application may include lots of built in application and data level protection, but there are many situations where these protections aren't enough.

Currently, IT industries face a perimeter security problem because 70 percent of security breaches are caused by the malicious insider. Whenever, companies are going to plan to deploy cloud services. They must have to deal with insider attacks as well as outside attacks (threats).

The most important threads of cloud computing are abuse and nefarious use of cloud computing, insecure interface and API, malicious insider, shared technological issues, data loss or leakage, account on service hijacking, unknown risk profile etc [9]. Thus, we suggest a secure architecture to avoid abuse and nefarious use of cloud computing, design a framework to secure insecure interfaces and API, account on service hijacking and malicious insider with following consideration.

- Authenticate all people to access network.
- Frame all access permissions so users can have access only to application and data that they have been granted.
- Authenticate all the software of the company.
- It monitors network activities.
- Log all user activity and program activity and analyzed it for unexpected behavior.
- Encrypt data, when there is need of some extra protection.
- Regularly check all networks for vulnerabilities in all software.

4. Proposed Idea

The basic idea of cloud computing is that it describes a new enhancement, utilization and delivery model for IT services based on Internet protocols. The best feature of cloud computing is that it has made access to computing resources a lot effortless way, but with that convenience has come a whole new universe of threats and vulnerabilities. Our work focus is to provide a solution for the threats that are the major issue for anyone when they want to adopt cloud model and services for their work. For this purpose, a framework should be designed for execution of data and information securely in cloud computing environment. It will protect user's data, information from various attacks. In this paper, we explore the security issues and challenges for the cloud computing and suggested a cloud computing framework to secure user's private data, messages and highly important information.

5. Methodology

In a cloud computing environment, any user can apply for any server to access the services of other users. This called as impersonation. An opponent can pretend to be another user and obtain unauthorized privileges on cloud machines. To counter this risk, servers must be able to confirm the authentication proof of user who request service. Fig.1 represents the functioning of authentication mechanism.

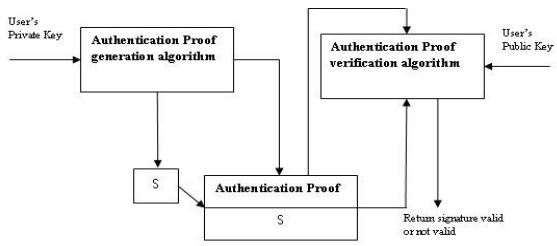

Figure 1: Represent the generation and verification of authentication proof

Each cloud server can be required to undertake this task for each client/server interaction, but in an open environment, this places a substantial burden on each cloud. There are the step are required to access the data from our secure cloud framework which include Invoke APIs with Web-Services, Register access gate and pass credential to AM (Access Management) provider, Validate credential, Validated, Pass Security token to access gate, Issued Security token to user group, Server responsible for generating encrypted key, Verified Encrypted key and forward key to encryption key provider. A substitute is to use an authentication server (AS) that knows the passwords of all users. It also stores in a cloud database or lightweight directory access protocol (LDAP). LDAP provides a standard format to access the certificate directories. They are stored on network LDAP servers and provide public keys. LDAP is based on the X.500 standard, but significantly simpler and more readily adapted to meet user's need.

6. Related Work

Kerberos is model for securing authentication service in a network. In the Kerberos authentication model, AS shares a unique secret key with each server. These keys have been distributed physically or in some other secure manner such as ticket [8]. Consider the following hypothetical dialogue: The portion to the left side indicates the sender and receiver. The portion to the right side indicates the message, the symbol || indicates concatenation.

(1) U ⟶ AS: $ID_U \| P_U \| ID_{CDS}$
(2) AS ⟶ U: *Ticket*
(3) U ⟶ CDS: $ID_U \|$ *Ticket*

Ticket = E (K_{CDS}, [$ID_U \| AD_U \| ID_{CDS}$])

Where,

U = User, ID_{CDS} = Identifier of Cloud server
AS= Authentication server, P_U = Password of user
CDS = Cloud Data Server, AD_U = Network address of user
ID_U = Identifier of user, K_{CDS} = Secret encryption key shared by AS and CDS

6.1 A More Secure Authentication channel of communication

Although the foregoing scenario solves some of the problems of authentication in an open cloud computing environment, problems remain. If user U logs on to a web service in the morning and wishes to check his or her data on a cloud data server, U must supply a password to get a ticket for the data server. If U needs to verify the data several times during the day, each attempt requires re-entering the password. We can improve matter that saying tickets are reusable. For a single login session, the web service can store the data server ticket after it is received. It uses it on behalf of the user for multiple accesses to the data server. However, under this scheme it remains the case that a user would need a new ticket for every different service. If a user wished to access a print server, a mail server, a file server, etc. The first instance of each access would require a new ticket and hence require the user to enter the password. The second problem is that the earlier scenario involved a plaintext communication. An eavesdropper could capture the password and use any service of the user. To solve these additional problems, we introduce a scheme for avoiding plaintext passwords and encrypt this password. Also introduce a new server, known as the ticket-giving-server (TGS). The scenario is as follows:

User login session:
(1) U ⟶ AS: $ID_U \| ID_{tgs}$
(2) AS ⟶ U: E (K_U, $Ticket_{tgs}$)
User services:
(3) U ⟶ TGS: $ID_U \| ID_{CDS} \| Ticket_{tgs}$
(4) TGS ⟶ U: $Ticket_{CDS}$
Once per service session:
(5) U ⟶ CDS: $ID_U \| Ticket_{CDS}$

$Ticket_{tgs}$ = E(K_{tgs},[$ID_U \| AD_U \| ID_{tgs} \| TS_1 \| Lifetime_1$])
$Ticket_{CDS}$=E(K_{CDS},[$ID_U \| AD_U \| ID_{CDS} \| TS_2$ | $Lifetime_2$])

The new service, TGS, issues tickets to users who have been authenticated to AS. Thus, the user first requests a ticket-giving ticket ($Ticket_{tgs}$) from the AS. Each time the user requires access to a new services, the user applies to the TGS, using the ticket to authenticate itself. TGS grants a ticket for the particular service. Here, only the correct user knows the password and the correct user can recover the ticket. Ticket consists of the ID and network address of the user and the ID of the TGS. These correspond to the first scenario. The idea is that the user can use this ticket to request multiple service-giving tickets. So the ticket-giving ticket is to be reusable.

Consider the following scenario, an opponent captures the login ticket and waits until the user has logged off his or her cloud services. Then the opponent either gains access to that web services. The opponent would be able to reuse the ticket to send-up the TGS. To counter this, the ticket includes a timestamp, indicating the date and time at which

the ticket was granted, and a lifetime, indicating the total time for which the ticket is valid. Thus, the user now has a reusable ticket and need not bother the user for a password for each new service request.

6.2 Kerberos AS problem

Kerberos model is having no provision of host security. Each network service requires a different host name that will need its own set of Kerberos keys. It creates complication in virtual hosting and clusters. Kerberos model is running with a strict time requirements, which means the clocks of the involved in hosts must be synchronized within configured limits. A ticket has a time availability period and depends on host clock synchronization. If the host clock is not synchronized with the Kerberos server clock, the authentication will fail.

In our research we found that Kerberos and LDAP together make for a great combination in cloud computing environment. Kerberos is used to manage credential securely (authentication) while LDAP is used for hold authoritative information about the account such as what they're allowed to access (authorization). Fig. 2 represents the working of AS. In this scenario, the user logs on to a web services and requests access to cloud data server (CDS). The client module U in the user's workstation requests the user's password and then sends a message to the AS that includes the user's ID, the server's ID, and the user's password. The AS checks it's from LDAP server with simple authentication mechanism to see if the user has supplied the proper password. LDAP checks given authentication for a Kerberos principal and contacts appropriate KDC (Kerberos Data Center). User ID and ticket must be check whether this user is permitted access to server CDS(Cloud Data Server). After passing the tests, the AS accepts the user as authentication. AS creates a ticket that contains the user's ID, network address and the cloud server's ID. The ticket is encrypted using the secret key shared by the AS and cloud servers. This ticket is then sent back to U. Because the ticket is encrypted, it cannot be altered by U or by an opponent. With this ticket, user can now apply to CDS for service. U sends a message to CDS containing U's ID and the ticket. CDS decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message. If these are two matches, the server considers the user authentication and grants the requested service.

User Interact Through Web Services (WS):

Step1: User login to access through WS.
(If pre-authentication is not there)
Step2: WS ask for Authentication.
Step3: User request for authentication.
Step5: WS Issued Authentication Proof.
Cloud1: Cloud Authentication Provider
Step4: Authentication provided through AS and LDAP.
Step6: Encryption key generator generate encryption key and verifier verified the encryption key.
Step7: Now, user can access through encryption key and authentication proof.
Cloud2: Cloud Data Provider
Step 8: Access controller confirm the authentication.
Step9: Now, use can access the services for the data access.

The ticket is encrypted to prevent variation or fake. The server's ID (ID_{CDS}) is included in the ticket so that the server can verify that it has decrypted the ticket properly. ID_U is included in the ticket to indicate that ticket has been issued on behalf of U. Finally, AD_U serves to counter the following threat. An opponent could capture the ticket transmitted in message (2), and then use the name ID_U and transmit a message of form (3) from another workstation.

Authentication server would receive a valid ticket that matches the user ID and grant access to the user on the other cloud services. To prevent attacks, the AS includes in the ticket the network address from which the original request came. Now, ticket is valid only if it is transmitted from the same cloud service. It is initially requested the ticket. The ticket-giving ticket is encrypted with a secret key known only to the AS and the TGS. It prevents modification of the ticket. The ticket is re-encrypted with a key based on the user's password. It is the assurance that the ticket can be recovered only by the correct user, providing the authentication. Here encryption generated by two addition server which are responsible for generate and verified the encryption key.

7. Conclusion and future work

Security and authentication from the malicious insider or outsider threat is the major concerns for companies to adopt cloud computing environment. In this paper, we discuss about some of the top threat of cloud security concerns and also provide a simple and efficient secure framework for the authentication. The work will more enhanced with some more

powerful encryption keys. The encryption key will more needed when user have to prove its identity to the TGS by revealing the secret information in secure manner. It is also require when the ticket presenter is not same as the user for whom the ticket was issued and the threat is that an opponent will steal the ticket and use it before expire. The future work will focus on the analyzing unlike encryption algorithm used by different cloud computing tools.

References

[1] Janssen, M. and A. Johan, "Motives for Establishing Shared Service Centers in Public Administrations", International Journal of Information Management, 2006, pp.102-116.
[2] Francis Hsu, and Hao Chen, "Secure File System Services for Web 2.0 Application", CCSW'09, November 13 2009, Chicago, Illinois, USA, pp11-17.
[3] Harold C. Lim et al, "Automated Control in Cloud Computing: Challenges and Opportunities", ACDC'09, June 19, 2009, Barcelona, Spain, pp 13-18.
[4] Siani Pearson, "Taking Account of privacy when designing Cloud Computing" Cloud 09, may 23, 2009, pp.44-52.
[5] Entire Deniz Sarier, "A new approach for Biometric Templates storage and Remote Authentication", ICB'09: Proceeding of the 3rd International workshop on Advances in Biometrics, Volume 5558/2009, June 2009, pp 909-918.
[6] D. kesavaroja, R.Balasubramaniam et. al, "Implementation of Cloud Data Server (CDS) for providing secure services in E-Business", IJDMS, 2005, pp 18-21.
[7] Wenchao Zhou et al, "Toward-a Data Centric View of Security", CloudDB 2010, October 30, 2010, Toronto, Ontario, Canada, pp 25-32.
[8] B. Clifford Neuman and Theodore Ts'o (September 1994). "Kerberos: An Authentication Service for Computer Networks". IEEE Communications.
[9] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).

Mr. Nitin Nagar has received Master Degree in Computer Applications (MCA) from Devi Ahilya University, Indore and perusing Ph.D. Degree from Devi Ahilya University Indore, India. Presently he is lecturer at International Institute of Professional Studies, Devi Ahilya University Indore, India. He is having more than 5 years of teaching and 3 years of research experience. His areas of research are Cloud Computing, Advanced Database Management System, and Distributed Computing.

Mr. Pradeep kumar Jatav has received Master Degree in Computer Applications from Devi Ahilya University, Indore India. Presently he is the Lecturer at International Institute of Professional Studies, Devi Ahilya University Indore, India. He is having more than 4 years of teaching and 2 years of research experience. His areas of research are Cloud Computing, and Networking.

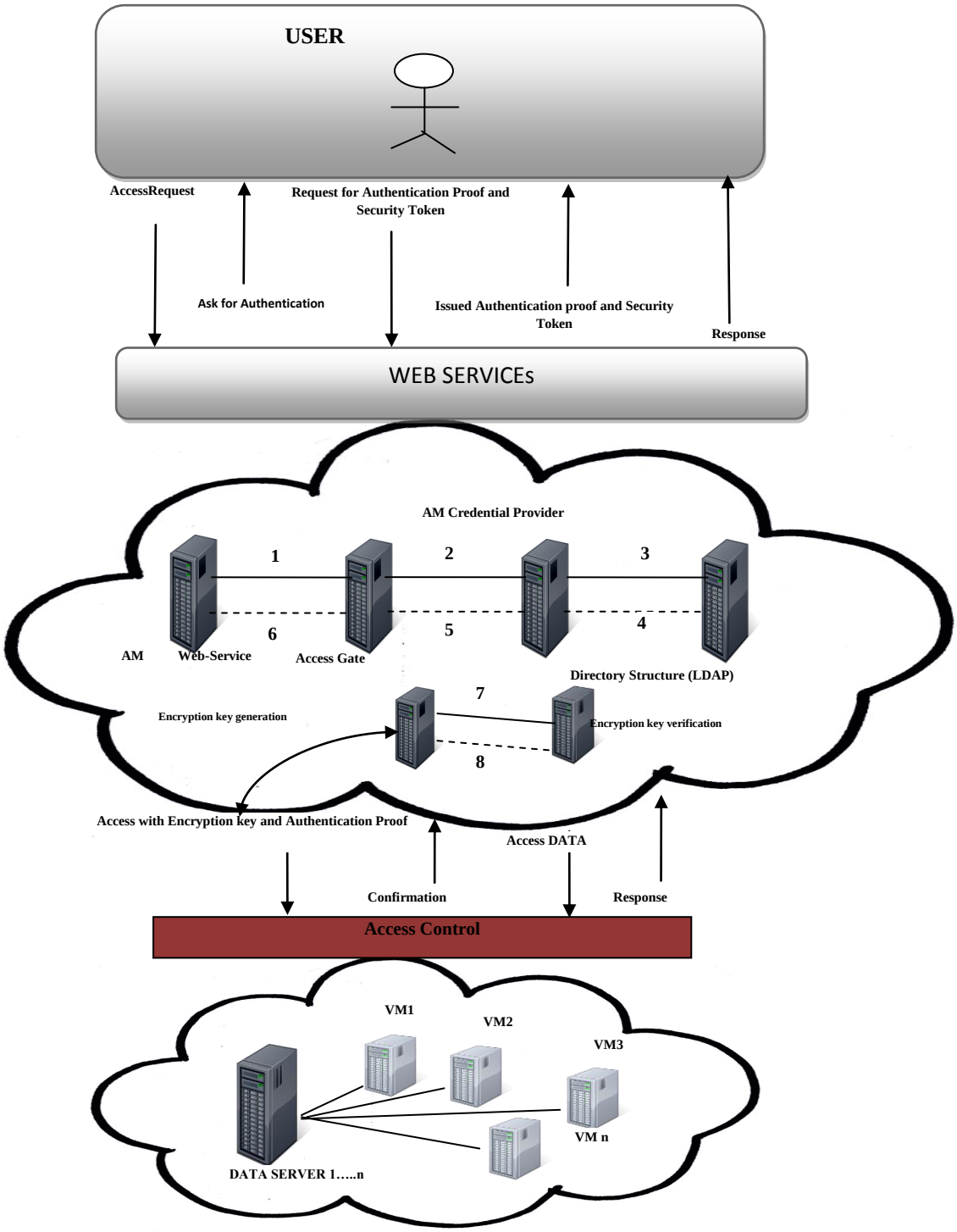

Figure 2: Represent the structure of user logging and access data server.