International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Review Article

An Authentication Mechanism to Enhance Security in the Cloud Environment

A. Cecil Donald[Á*], A. Jenis[B̀] and L. Arockiam[Ć]

[Á]Computer Science Department, St. Joseph's College (Autonomous), Tiruchirappalli, India

Accepted 10 Sept 2014, Available online 01 Oct 2014, **Vol.4, No.5 (Oct 2014)**

Abstract

Cloud is a term defined as a pool of configurable computing resources that can be accessed by users based on a pay-as-you-go principle. Cloud computing is otherwise termed as internet computing because of its availability and that will be feasible only with the internet connection. Therefore, security plays a major role in cloud computing. Some of the important security services including encryption, authentication, integrity and confidentiality. This paper analyses various existing authentication mechanism and their issues. An enhanced authentication mechanism for identifying user in cloud environment is also proposed. The mechanism authenticates the user to access the appropriate cloud services. There are three main components involved in this framework namely User, Trusted Authenticator (TA) and Cloud Service Providers (CSPs). The TA provides secure access to the user by generating the digital signature and credentials. In this paper, the steps for authenticating the users are also described.

Keywords: *Authentication, Cloud Computing, Digital Signatures, Security, Trusted Authenticator (TA).*

1. Introduction

Cloud computing is a hasty growth internet based technology. Using this technology, resources is shared on user's request. So, a cloud can be seen as virtual pool of resources that can be availed through internet in a unification of remote engineering. The services are tendered by the cloud service provider and the internet acts as a communication interface. The NIST defines cloud computing as *"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"* (NIST 2011).

NIST also defines three major service models for cloud computing: Software as a Service (SaaS) – The Cloud Service Provider (CSP) provides the capability of deploying an application into the cloud. Platform as a service (PaaS) – The provider supplies infrastructure, i.e. an integrated set of software with all the stuff that a developer needs for building applications i.e. both for developing and for execution progress. Infrastructure as a Service (IaaS) - The supply of hardware as a service, i.e. Servers, storage or computation, as well as basic characteristics such as Operating Systems and virtualization of hardware resources. NIST also defines four deployment models for cloud computing: public, private, hybrid and community clouds.

Even though cloud is gaining a potential profit, there are some issues that suppresses the usage. Security plays an important role in cloud, faced by the users as well as CSPs. The architecture of the cloud computing involves multiple cloud components interacting with each other. Thus, it helps the user to access the required services at a faster rate.

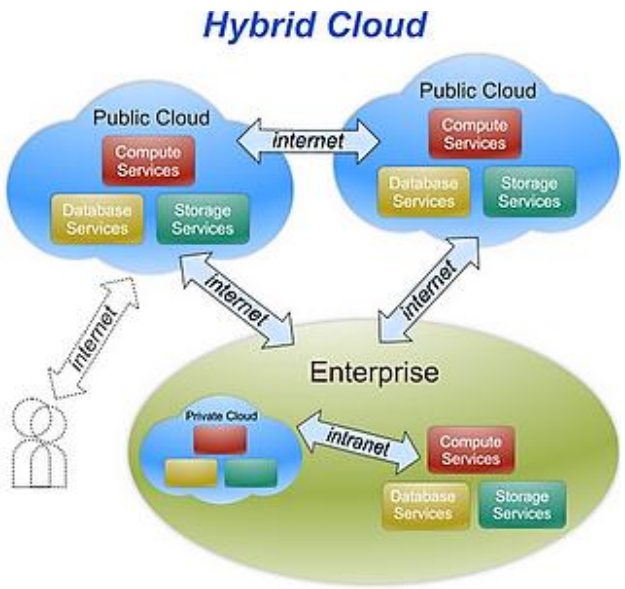

Fig.1 Cloud Deployment Models (Hameetha, *et al*, 2013)

The cloud computing is more centered upon the front end and the hinder end. Several research works are carried for securing the cloud environment. Due to the massive

*Corresponding author **A. Cecil Donald** is Research Scholar**; A. Jenis** is a M Phil Scholar and **Dr. L. Arockiam** is working as Associate Professor

complexity in the cloud environment, it will be difficult to provide an aggregate response for securing the cloud, at present. Thus, our goal is to make incremental enhancements for securing the cloud that will finally result in a secure cloud (Radha, *et al*, 2013).

Cloud computing security should address the cloud provider to incorporate with the customer's data security, privacy and compliance with necessary regulations. In order to develop a secure cloud environment, basic Security principles has to be taken into the account (Cloud, 2013).

Confidentiality: To ensure the guarantee of providing the information is not gathered by an unauthorized person. i.e. the information from both stored data as well as the data transferred via the internet.

Integrity: To ensure that the protected data cannot be modified by the third parties. Integrity is based on two principles, one is to prevent the modification of data from unauthorized users and another is to prevent the unauthorized modification of data by unauthorized user.

Authentication: Authentication is the process of identifying and verifying the user by a valid username, password and provides the rights for accessing the services or any resources of the cloud. Authentication usually means the proper verification of someone's identity.

This paper proposes an enhanced authentication mechanism for authenticating the users in cloud environment. In this framework, a concept of providing Digital Signature (DS) at the user level and also in the Trusted Authenticator (TA) for high security is introduced. Therefore, this model helps to solve main security issues like DOS Attack, DDoS Attack, Google hacking, eavesdropping, etc. in a cloud environment. This model allows the user to access the services from the cloud service provider side by authenticating the access. The organization of the paper is given as follows. Section 2 describes various related works carried out in the cloud environment. Section 3 elucidates the proposed framework for authenticating the cloud users. Section 4 explains the components involved in the proposed authentication mechanism and section 5 delivers the process work flow of the proposed mechanism and finally section 6 concludes the work and delivers the future research works.

2. Related Works

Nowadays, several number of researches on security issues in cloud computing are being carried out. Various security frameworks are proposed by different researchers. By analyzing those works, some security issues are identified and few works are taken into account for proposing a new framework to authenticate the user for accessing secure services from the cloud service provider.

Jivanadham *et al*. (Jivanadham, *et al*, 2013) explains the basic concepts of cloud computing, security issues and also proposed an integrated authentication mechanism called the Cloud Cognitive Authenticator (CCA). CCA is an API, integrating bio-signals, one round Zero Knowledge Protocol (ZKP) for authentication and Rijndael algorithm in Advance Encryption Standard (AES). To enhance security in cloud, CCA has proposed four procedures, providing two levels of authentication as well as encrypting/decrypting the user ID. The novelty of this paper is it provided two level authentication. The conflict of this concept arises the interoperability of the CCA and AES algorithm compatibility.

Sivasakthi *et al* (Sivasakthi, *et al*, 2014) proposed a user authentication model with digital signature. The proposed model addresses two key issues. One was the *key distribution* in order to secure the communication and another was the *digital signature* which verifies the message originated from the sender. The table of system server and database server are disjoint sets. The algorithms involved in authentication process are RSA, SHA, and AES. The major advantage of the proposed model is it prevents data hacking and unauthorized user accessing of services. The disadvantage of this model are it is only for single user multiple servers not for multiple users and multiple servers. Another major issue was; when the user forgets the password, he will not be able to access the services rather he need to create a new username and password.

Venkataramana *et al*. (Venkataramana, *et al*, 2012) proposed Agent Based approach for Authentication in the Cloud (ABAC) to authenticate the users for accessing the cloud services and also to reduce the internal and external attacks. In cloud environment, the VMware components involved are VMware ESX, VCenter Server, and Active Directory Server. The phases involved in the ABAC architecture are Registration Phase, Key Generation and Distribution Phase and Authentication and Verification phase. The advantage of the ABAC is; it provided an extra layer of security for the entire cloud. The major disadvantage is; it does not provide scalable authentication infrastructure.

Hada *et al*. (Hada, *et al*, 2012) proposed a trust model for cloud architecture. It uses the mobile agent which is used as a security agent and it monitors the integrity and authenticity. This system remotely monitors and attests the integrity of crucial system files, thus filling a gap in the Xen Cloud Platform. This was its major advantage. Also service provider can ensure fulfillment of security policies by avoiding attacks on VMs. The drawback of the proposed model is; it provides secure and reliable communication only through a mobile agent not through agents present in the cloud environment.

Donald *et al*. (Donald, *et al*, 2014) proposed a model for trusted computing and solve the identity theft in the cloud and it was simulated in the .Net environment. The evaluation of the proposed model occurs in three ways: security analyzing, simulating, and BLP confidential. The model involves six steps on the Open ID exchange of data flow. The strength of the proposed model is evaluated against phishing attacks and it results in an optimal solution. The limitation of the proposed model is it was evaluated only in federated environment and it was its drawback.

Shenbagam *et al*. (Shenbagam, *et al*, 2014) proposed a model combining persuasive cud click points, alphanumerical authentication, sound signature and draw-a-secret in order to overcome the usability and security. This system is the combination of graphical password, text, draw-a-secret method and phone message, which

increase the confidence and reliability. This was the advantage of the proposed system. The disadvantage was that there is instability occurs in data storage for cloud.

Ganesh V. Gujar *et al.* (Ganesh, *et al*, 2013) proposed the stronger password authentication generation technique by STEP-2 (double) authentication and session management in a cloud computing environment. This STEP-2 user authentication executes in different modules like user registration, user authentication, password change. In User Registration user wants to access cloud resources, user has to register first on to the cloud. By User Authentication user should login on to the cloud and Password Change phase is used to provide facility of changing the password.

3. Proposed Framework

The proposed framework for authenticating the user in cloud platform. In this model, a concept of providing a Digital Signature (DS) at the user story and a Trusted Authenticator (TA) for providing high security is presented.

This model allows the cloud user to access the services from the cloud service provider's by authenticating the access requests. The communication between the user and the CSPs are authenticated by the Trusted Authenticator (TA). The trusted authenticator authenticates the user and allows the user and CSP to communicate in accessing the services.

The TA has two phases, one was the *Registration phase* and another was the *verification phase*. The TA has a database server which checks for registered user and validates the user to access services from CSP. If the user is not a registered client, it sends a message to the invalid client. The TA also provides a digital signature, which provides higher security level of accessing services.

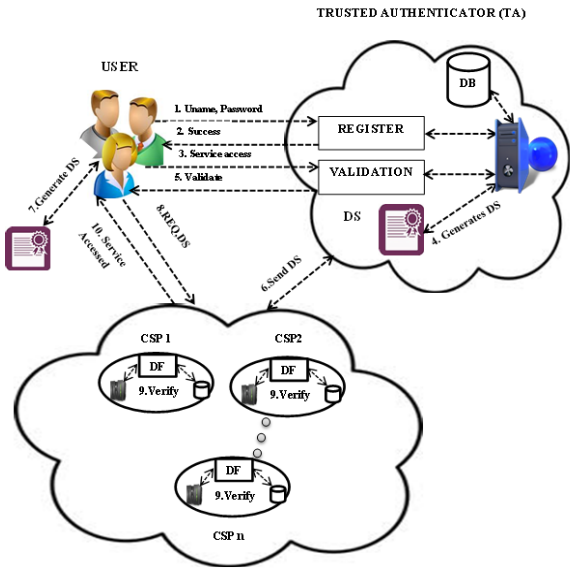

Fig.2 Proposed Authentication Mechanism

When the user gets validated, he is permitted to approach the CSP for demanding the services along with the Digital Signature. The browser on the user side has an add-on which generates the Digital Signature of the same credentials in which the TA generates, and the Digital Signature wraps the user request. The user requests for accessing services along with Digital Signature will be sent to the CSP.

The clouds of CSP have the request from the user side and the DS from the TA and allocate the respected CSP which has the requested services. The respected CSP has an agent who verifies the DS from both user and CSP. If they are equal, then the user is allowed to access the service successfully.

4. Components in proposed Mechanism

The components involved in the proposed mechanism are depicted one by one as follows:

4.1 User

User has limited access to the services from the cloud offered services. The user requests for cloud resources to the CSPs. The users may be students, organization, and other users.

4.2 Trusted Authenticator (TA)

TA establishes a trust connection with an authentication authority. The idea of insisting TA in cloud environment is to permit the user to access services through the service provider who never has an idea of the user.

4.3 Cloud Service Provider (CSP)

A cloud service can dynamically scale to meet the needs of its users, and because the service supplier has to supply the hardware and software necessary for the service.

4.4 Digital Signature (DS)

A digital signature is an electronic signature which authenticates the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

4.5 CSP's Agent

Agents are computer systems that are capable of making decisions when carrying out tasks on behalf of their users. The agents have the authority to interact with other agents through negotiation, cooperation, and coordination. In CSP, the agent works for service delivery, service negotiation, service cooperation and service coordination.

5. Algorithm work flow

Stairs in the authentication mechanism have ten steps. They are:

Step 1. The user sends his username and password for registration to the Trusted Authenticator.

Step 2. Trusted Authenticator (TA) registers the user credentials and reply success of registration.

Step 3. Again, after registration the user sends the request of a service to the Trusted Authenticator.

Step 4. TA validates the user and creates a digital signature for the request made along with user credentials.

Step 5. TA sends a message of success, or access denied, according to the establishment.

Step 6. TA sends the digital signature to the CSP's cloud.

Step 7. User gets validated and create the digital signature from the user side for the request he made along with his credentials.

Step 8. The user sends his request along with the digital signature to the CSP's cloud.

Step 9. Each CSP has an agent who breaks the digital signature of user and trusted authenticator, and if both accept the same digital signature, CSP provides the entry of the user request.

Step 10. User avails the service according to the request.

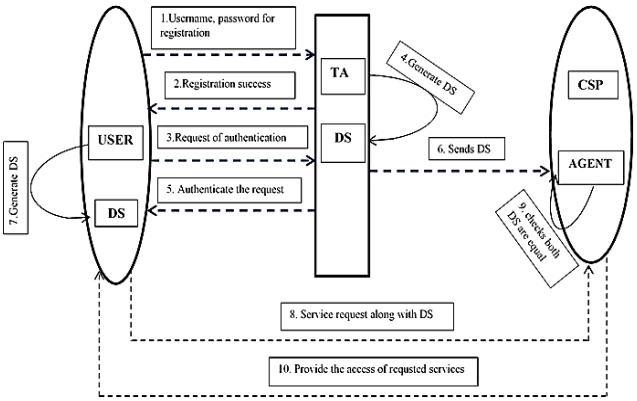

Fig 3 Workflow of Authentication mechanism

Conclusion

The proposed model is enhanced with secure, fault-tolerant, sustainable and scalable infrastructure for hosting internet based application services. The proposed mechanism illustrates the steps for accessing the services. Therefore, the user is responsible for authenticate himself with the TA and permitted to access the services according to his request. Digital Signatures brings the highest level of security. In order to prevent the intruder act during the transit Digital Signature from TA to user, the concept of creating the DS on the user side is applied. Therefore, the DS is newly created at the user side with the same credential created by TA. The Enhanced mechanism provides secure access to the cloud services. The future work might undertake more action on what type of Digital Signature should be used and also on the audit mechanism like the log maintenance, etc.

References

National Institute of Standards and Technology, (2011), *NIST Definition of Cloud Computing*.

S. Hameetha Begum, T. Sheeba, S. N. Nisha Rani, (2013), Security in Cloud based E-Learning, *IJARCSSE*, Volume 3, Issue 1, ISSN: 2277 128X, pp: 270-278.

Radha Krishna Reddy P, Pavan Kumar Reddy S, Sireesha G and Sechadri U, (2013), The Security Issues of Cloud Computing over normal & IT sector, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.2, Issue 3, pp. 356-361.

N Hemalatha, A Jenis, Cecil A Donald and L Arockiam (2014), A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing, *International Journal of Computer Applications*, 96(16):1-6.

L. B. Jivanadham, A.K.M. Muzahidul Islam, ShozoKomaki, S. Baharunand Yoshiaki Katayama (2013), Cloud Cognitive Authenticator (CCA): A Public Cloud Computing Authentication Mechanism, *IEEE, pp. 1182-1188.*

T. Sivasakthi and Dr. N. Prabakaran, (2014), Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, Issue 2, pp. 456-459.

K. Venkataramana and Dr. M. Padmavathamma, (2012), Agent Based approach for Authentication in Cloud, *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, ISSN: 2249-9555, Vol. 2, No.3, pp. 6-11.

Priyank Singh Hada, Ranjita Singh, and Mukul Manmohan, (2012), Security Agents: A Mobile Agent based Trust Model for Cloud Computing, *International Journal of Computer Applications* (0975 – 8887), Volume 36– No.12, pp. 1142-1147.

Cecil A Donald and L Arockiam (2014), Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues, *International Journal of Computer Applications* 94(1):25-29.

P.Shenbagam, C. Namasivayam (2014), 4 Level Authentication Security in the Cloud Computing, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.2, Issue 1, pp. 304-309.

Ganesh V.Gujar, Shubhangi Sapkal, Mahesh V.Korade (2013), STEP-2 User Authentication for Cloud Computing, *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(10), pp. 401-405.