Article can be accessed online at http://www.publishingindia.com

# Security Enhanced Multi Level Authentication for Cloud

**Vishal Vijay Saswade*, S. M. Bansode****

**Abstract**

Cloud Computing provide a delivery of scalable IT resources over the Internet as opposed to hosting and operating those resources locally such as on a college or university network. Resources like applications and services, as well as the infrastructure on which they operate. Cloud providers specialize in particular applications and services, and this expertise allows them to efficiently manage resources like applications and services, expertise allows them to efficiently manage, upgrades and maintenance, backups, disaster recovery and Failure functions upgrasources locally, such as on a college or uscalable IT rdes and maintenance, backups, disaster recovery, and failover functions. Cloud computing [1] encourages IT organizations and providers to increase standardization of protocols and processes so that the many pieces of the cloud computing [1] model can interoperate properly and efficiently. Concern about identity theft, data breaches and fraud is increasing but at the same time organizations are feeling pressure to enable employees, partners and customers to access more sensitive information from anywhere and any device. These market dynamics make multi-factor authentication [4] and fraud prevention critical parts of any organization's security[2] strategy Cloud computing has been around for over some years in different forms. However the third generation trend in IT industry is now ruled over by cloud computing. Cloud services require Attestation and different models of Attestation have been proposed over the years. Two Factor Attestation[6] technique contains a two layer Attestation system, where the first layer contains user name and password and second layer contains tokens and pins.

"Cloud" is a virtualized pool of computing resources. Two of them are : Multifactor Attestation (MFA) [6] contains more than one form of Attestation that is implemented to verify the legitimacy of a user.

In this paper, we will be discussing our proposed model for multi level Attestation and compare the existing models with the proposed one.

**Keywords:** Cloud Computing, SEMAM, User Authentication, PAAS

## 1. INTRODUCTION

Cloud computing is an Internet based resource sharing methodology wherein data and resources are shared and integrity of data, resources have become prime concern.

Access to intruders can be restricted by providing username and password as first level Attestation.

In our proposed work we have attempted to minimize the loop holes related to the security[2] and the Attestation of the user in an organization by providing multi level Attestation (User ID , Password and MAC Address) encrypted in digital certificate.

Various Service modules of Cloud Computing[1] are:

1. **SaaS(Software as a Service)**: Software is deployed over Internet. This is pay per use model.
2. **PaaS( Platform as a Service)**:Uses the middle man's equipment to develop your own program and deliver it to the users through Internet and various servers.
3. **IaaS( Infrastructure as a Service)**: Rather than purchasing servers, softwares or network equipments, client instead, use those resources as a fully outsourced services.
4. **HaaS( Hardware as a Service)** : Allows to use hardware on pay per basis.

* Assistant Professor, CSE Department, Government Engineering College, Aurangabad, Maharshtra, India.
E-mail: vishalsaswade@gmail.com
** Assistant Professor, CSE Department, Government Engineering College, Aurangabad, Maharshtra, India.
E-mail: sskandhare11@gmail.com

In this paper we have proposed new security architecture model for cloud computing platform. In this model multi level Attestation technique is used for giving secured access to a cloud user. Here credentials are encrypted into a digital certificate with AES algorithm[6] in which keys are generated randomly by the system. In our proposed model multi factor Attestation[6] is used, thus ensuring higher security[2]. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing platform. The RSA algorithm[5] is used for secured communication [8] between the users and the servers.

This paper is formatted in the following way: - section 2 describes related work of this paper work, section 3 describes proposed architecture and its working steps.

## 2. RELATED WORK

Current Attestation model (Consolidated Architecture Model) enables smart devices to perform user Attestation by using user certificate stored in the devices. It requires web browser such as Internet Explorer, Opera, Safari, Firefox, Chrome etc. Furthermore, this model is designed not to reveal the sensitive data such as digital signature information to Auth Server through end-to-end encryption which ensures its secure delivery between service provider and smart device. [8]

However this model does not store Machine Address Code of the device.

By adding the MAC to the certificate, we can ensure that user is bonded to use the exact same machine which is assigned to him/her by the administrator.

Existing Multi level Attestation Technique For Accessing Cloud Services[7] This technique has two separate entities:

i. Cloud service provider, who provides the cloud services and ii) Authenticated client organizations that access the cloud services.

This architecture helps in checking the Attestation against the services and privileges. This is evaluated by multiple levels Attestations. First level of Attestation is organization level password Attestation/generation. It is for ensuring the cloud access Attestation from cloud vendor.

**Second level of Attestation**[6] is a team level password Attestation/ generation. It is to authenticate the team for particular cloud service.

However this architecture does not implement any encryption technique, also it does not bind a user physically to his/her device.

## 3. PROPOSED ARCHITECTURE

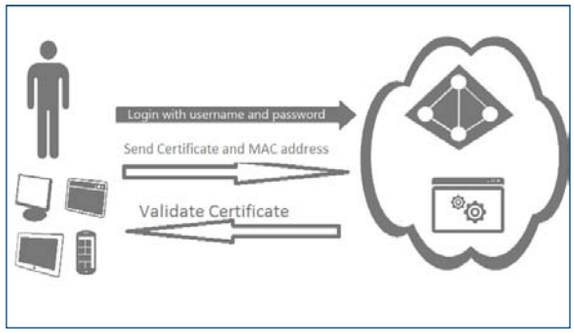
Security Enhanced Multilevel Attestation Model (SEMAM) The SEMAM consists of username and password encrypted along with MAC address in a digital certificate.

Encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

PKCS#12 is used to exchange public and private objects within a single file.

**Figure (a). Architectural Diagram for SEMAM**




### 3.1. Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA)[4]. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public

key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

### 3.2. Public Key

The receiver of the certificate uses the public key to decipher encrypted text sent by the certificate owner to verify its identity. A public key has a corresponding private key that encrypts the text.

### 3.3. Private Key

A private or secret key is an encryption/ decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.

Public key encryption[8] requires that a public key and a private key be generated for an application. Data encrypted with the public key can only be decrypted using the corresponding private key. Data encrypted with the private key can only be decrypted using the corresponding public key. The private key is stored in a key database file that is password-protected. Only the owner of the private key can access the private key to decrypt messages that are encrypted using the corresponding public key.

The issuer of the certificate signs it with a digital signature to verify its authenticity. This signature is compared to the signature on the corresponding CA certificate[4] to verify that the certificate originated from a trusted certificate authority.

**Definition and Basic Scheme**

In our proposed model multi factor Attestation is used, thus ensuring higher security. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing[1] platform. we have proposed new security architecture model for cloud computing platform. In this model multi level Attestation technique is used for giving secured access to a cloud user. Here credentials are encrypted into a digital certificate with AES algorithm[6] in which keys are generated randomly by the system. The RSA algorithm is used for secured communication between the users and the servers.

Algorithm and Psuedo Code:

Step 1:

User will enter User Name and Password (provided by organization)

If Attestation Successful then

Request Digital Certificate from User's machine onto server

End If

Step 2:

If certificate provided then Check and compare the certificate key with server key

Else

Go to Step 7

End If

Step 3:

If Key matches then

Go to Step 4:

Else

Go to Step 7

End if

Step 4:

Read contents of Digital Certificate and extract user name password along with MAC Address of the ethernet adapter.

Step 5:

Compare the extracted Credentials with the already stored credentials in the Database.

Step 6:

If Credentials and MAC Address Matches then

Allow services to be accessed.

else

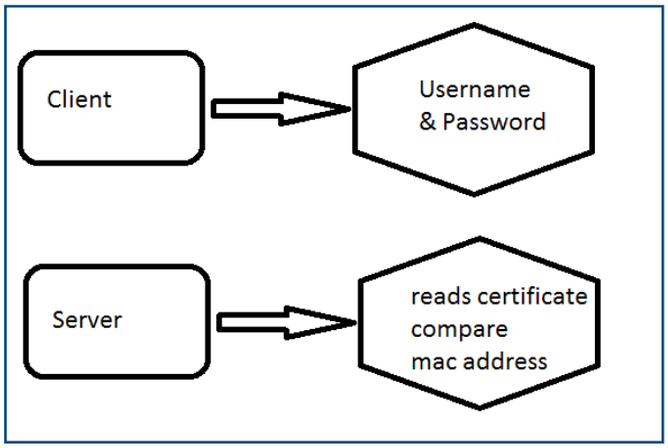
Revoke certificate and restrict the client system and user.

End if

Step 7:

Exit

**Basic Data Flow Diagram**




SEMAM will consists of following steps in Authenticating the user:

1. User information account (User ID and passsword)
2. Add MAC address and ecrypt in a digital certificate
3. Store Digital certificate on server and install the same on users machine
4. When user tries to establish a connection with organizations cloud server then installed certificate will be checked with certificate stored on server
5. User will be prompted to provide user name and password on the server
6. MAC address will be verified

If successful

7. Gain access to organization server
8. prompt user to input another set of credentials that is user name and password for service access else
9. FAIL

Display appropriate message.

## REFERENCES


1. Mykletun, E., Narasimha, M. & Tsudik, G. (2006). Attestation and integrity in outsourced databases. *ACM Transactions on Storage*, 2(2), 107-138.
2. Wang, B. & Xing, H. Y. (2011). *IEEE-The Application of Cloud Computing in Education Informatization*. In International Conference on Computer Science and Service System (pp. 2673 - 2676). North China: Modern Educational Technology Centre.
3. NIST Definition. Retrieved from http://www.au.af.mil/au/awc/awcgate/nist/cloud-defv15.doc
4. CA Technologies Cloud Attestation System. Retrieved from http://www.ca.com/us/Attestation-system.aspx
5. Suo, X., Zhu, Y. & Owen, G. S. (2005). *Graphical passwords: A survey*. In Proceedings of 21st Annual Computer Security Application Conference (pp. 463-472).
6. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005). *Attestation using graphical passwords: Basic results*. In Proceedings Human-Computer Interaction International, (pp. 25-27). Las Vegas, NV.
7. Alsulaiman, F. A. & Saddik, A. E. (2008). *Three-dimensional password for more secure attestation*. IEEE Transactions on Instrumentation and Measurements, 57(9), 1929-1838. Retrieved from http://ieeexplore.ieee.org.
8. Cloud Computing Services & Comparisons. Retrieved from http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%
9. 20services.pdf
10. Eludiora, S., Abiona, S., Oluwatope, A., Oluwaranti, A., Onime, C. & Kehinde, L. (2011). A User Identity Management Protocol for Cloud Computing Paradigm. *International Journal of Communications, Network and System Sciences*, 4(3), 152-163.
11. Trusted Computing Group. Retrieved from https://www.trustedcomputinggroup.org/
12. Stallings, W. (2003). *Cryptography and Network Security-Principles and Practices* (3rd Ed). India: Prentice Hall.
13. Madhavi, K. V., Tamilkodi, R. & Dinakar, R. B. (2012). Data storage security in cloud computing for ensuring effective and flexible distributed system. *International Journal of Electronics Communication and Computer Engineering*, 3(1), 133-137.
14. Patidar, S., Rane, D. & Jain, P. (2008). *A Survey Paper on Cloud Computing*. 2012 Second International Conference on Advanced Computing & Communication Technologies (pp.394-398)
15. Patidar, K., Gupta, R., Singh, G., Jain, M. & Shrivastava, P. (2012). Integrating the trusted computing platform into the security of cloud computing system. *International Journal of Advanced Research in Computer Science and Software Engineering*, February, 2(2).