CCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATION
(ISSN 2455-5061) *Vol. - 3, Page-07-10, Year-2018*

# Mutual Authentication in Cloud System using Two Level Security with One Time Password

**Sitendra Tamrakar,[*] Kapil Dev Raghuwanshi,[**]**

[*]*Associate Prof, Department of Computer Science & Engineering, CCET Bhilai, C.G, India*
***drsitendra@gmail.com***,
[**] *Assistant Prof, Department of Computer Science & Engineering, BIST Bhopal, M.P, India*
***dev_2988@yahoo.co.in***

**Abstract**

*Today, cloud computing is the most popular term in enterprise, news and research area of computer science engineering. It is a model to provide on demand service to the user as per their requirements and on Pay per Use basis. The cloud computing provide flexibility to user, user can access, process and store their data on cloud server using existing internet standard without self built infrastructure .The infrastructure of cloud computing is built on Internet. It brings out all the issue of security that will encounter in Internet, such as identity management, application security, access control and authentication. A Mutual Authentication in Cloud System Using Two level Security with One Time Password should be proposed in this paper for improving authentication mechanism and let the user to access cloud service securely.*

***Index Terms:*** *Cloud System, User authentication, Identity Management, Graphical password OTP*

## I.Introduction

Cloud Computing is one of the new technologies on which a lot of research work is going on currently. It provides a distributed, flexible and heterogeneous platform where a number of Users can access the Cloud and get the services as per their needs.

An important characteristic of Cloud Systems is that it provides the Services to its Customers on "PAY PER USE" basis, i. e., the customer will have to pay for what he / she is using. It provides a way for sharing the data and resources between a numbers of Users through Internet, hence, it is also referred to as Internet Based Computing [13].

A Cloud is normally referred to as "XAAS" where X is a type of Service that a particular Cloud is providing to its Users and AAS means "As A Service".

## II.Cloud Models

The Cloud Models are classified into two broad categories, as Cloud Service Models and the Cloud Deployment Models.

### A. Cloud Service Models

It is also referred as the Cloud SPI Model. Here, the Cloud is classified on the basis of the Services that it provides. It has three broad categories, as Software (SaaS), Platform (PaaS) and Infrastructure (IaaS).

*i)* *SaaS:* "Software as a Service" or the SaaS Model deals with providing various Software / Applications to the Users of the Cloud Systems by deploying them over the Cloud and made them available to the Users for use.

*ii)* *PaaS:* "Platform as a Service" or the PaaS Model provides the facility to the Cloud Users to use the available Hardware Resources like Operating Systems on rent so that the Users can access the Applications or

they can deploy their own applications on them.

*iii)* *IaaS:* "Infrastructure as a Service" or the IaaS Model allows the Users to use the Cloud System Resources like Servers, Hardware, Storage and Networks to carry out the desired operation. The Cloud Infrastructure is accessible to the User and the User can use it to store its Data / Information.

### B. Cloud Deployment Models

The Cloud Deployment Models are classified on the basis of the Users that are using the Cloud Services[11].

*i)* *Private Cloud:* The Cloud Infrastructure and Services can be accessed by a limited number of Users.

*ii)* *Community Cloud:* The Cloud Infrastructure and Services can be used by a number of communities together.

*iii)* *Public Cloud:* The Cloud Infrastructure and Services can be accessed by a large audience.

*iv)* *Hybrid Cloud:* It is a mixture of Public and Private Clouds as some Resources are accessed only by specific Users like Private Cloud and others can be used by a large audience like Public Cloud.

## III. Security Issues For Cloud Systems

*A. Physical Security*

Managing the Security of Data Centers against Physical Damages like Crashing of Work Stations due to abnormal situations[5].

*B. Network Security*

Keeping the Data safe from various types of Attacks and Intrusions.

*C. Data Security*

Keeping the Confidential Information of the Users private / secret from others.

*D. Access Control*

Maintaining the System in such a way that only the Authorized User can access the System and its Resources and Unauthorized User cannot get a single point in the System from where he / she can perform Intrusion.

*E. Identity Management*

The Identity of the User that is accessing the System must be identified and verified by the Server before allowing his to access the System and it must also be verified that the Services it is using are authorized for him[7].

*F. Trust*

Mutual Authentication between the Client and the Server must be made so that both are verified to and by each other. It is also necessary that none of the Parties can share the Secret Information of each other with any outsider who can misuse that Information and create serious problems for the System and its Users.

## IV. Security Parameters

*A. Authentication*

Basically, to check whether the User is correct or some fake User is pretending to be an Authorized User[6].

*B. Authorization*

The User is accessing the Service for which it has proper privileges.

*C. Secrecy / Privacy*

User Data has been kept Secure and hidden from others.

*D. Confidentiality*

The Communication between the two parties cannot be penetrated by any third party.

*E. Integrity*

The correctness of the Data should remain intact.

## V. Literature Review

1. A. J. Choudhary, P. Kumar, M. Sain, H. Lim and H. J. Lee in 2011 proposed a Strong User Authentication Framework for Cloud Computing. They suggested an approach for Mutual Authentication based on Out Of Bound Technique using the Smart Cards. During access, the Smart Card is provided in the Terminal along with the Password. If both are valid, then the Server generates an OTP and sends it to the Client. The Client then provides this OTP back to the Server. In this way, Mutual Authentication has been achieved between the Client and the Server.

2. M. H. Guo, H. T. Liaw, L. L. Hsiao, C. Y. Huang and C. T. Yenp proposed an Authentication Scheme for Cloud Systems using Graphical Passwords. They proposed an Authentication technique in which the Client first provides his / her ID and Password to the System. If they are validated then the User has to select a combination of Pictures that he / she have already selected during the Registration Process. If the combination of Pictures is correct then the User get access over the System. They defined the Recognition based Graphical Passwords for Cloud Security.

3. H. A. Dinesha and V. K. Agarwal suggested Multi Level Authentication Technique for accessing Cloud Services. Their scheme is actually divided into various levels based on the flow of information. The first level is an Organizational Level Authentication in which the Authentication of the User can be made by the Cloud Service Provider or Vendor. The second level is a Team

Level in which the Authentication can be made for accessing a particular cloud service by a specific team. The third level is a User Level Authentication in which the Cloud Server verifies the User and provides the access to Services if the User is valid. Similarly, we can have one or more levels for adding more security in the System.

4. S. Kolhe and S. Dhage in 2012 suggested a Trusted Platform for support Services in Cloud Computing Environment. They proposed a Dynamic Password Scheme in which each time the User accesses the System, he / she has to provide a new Password that can't be used before and after this Log In. The User first provides his ID and Password to access the System. The System verifies them and if both are correct, then the System generates an OTP (dynamic Password) and sends it to the User. The user then provides this Password to the System again. In this way, Mutual Authentication between the two ends has been achieved.

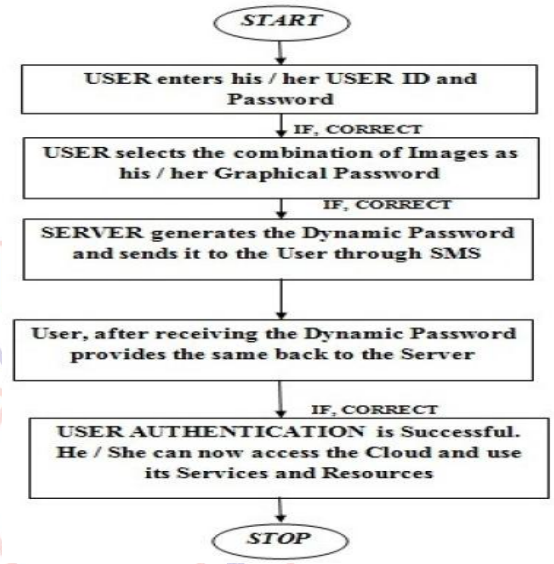
## VI. Proposed Algorithm

Security is the most important feature that must be considered in any Distributed Environment where a number of Users are sharing common Resources. It is necessary that the Data and Identity of all these Users must be kept secret from others, so that these Data can't be misused. The Users also need to make sure that they do not disclose their secret information with others.

Cloud computing also requires Security at various levels of usage. So, we are proposing a Framework for implementing Authentication and Security in Cloud Systems. Cloud computing is a version of client server architecture where thousands of client use the same infrastructure at a large scale. Before proposing the Technique, we had gone through a number of Authentication Techniques that are already being used for providing Security in Cloud Systems.

Our proposed System consists of four main Phases, which are Registration Phase, LOG IN Phase, Change Password Phase and Authentication Phase.
The Authentication Phase is the main part of our approach that acts as the Base / Heart of the proposed System.

1. *Registration Phase:* The Cloud User provides his Credentials along with User ID and Password that he / she will use to access the System. In this Phase, the User also selects the combination of Images that are used later for second level of Authentication.
2. *LOG IN Phase:* The Cloud User access the Cloud System through this Module. The User provides his / her User ID and Password for first stage of Authentication. In second stage, the User selects the combination of Images that he / she had finalized during Registration Phase. Then the User provides the received OTP to the System.




**Flow chart of the proposed algorithm**

3. *Authentication Phase:* In this Phase, the User ID and Password provided by the User is validated and if they are true, then the User completes the first level of Authentication. The User then selects the combination of Images as Graphical Recognition Based Passwords. If the combination is correct, then the User successfully completes the second level of Authentication.
   The System then generates a Dynamic Key and sends it to the User. The User then provides the same Key to the Server. If it is correct then the third level of Authentication is successful. Now, the User can access the System and utilize its Resources and Services as per his / her needs.
4. *Change Password Phase:* In this Phase, the User can change his / her Password as well as Graphical Password, as and when needed.

## VII. Conclusion

The proposed Manual Authentication Scheme for Cloud using Two Level Security with One Time Password (OTP) will enhance the security mechanism in Cloud Computing with many Security features such as Mutual Authentication, Identity Management, Sharing of Session Keys between the Users and the Cloud Server. The Dynamic Password is one of the Strong Authentication Technique.
Once the Dynamic Password has been consumed or used for Authentication, it can't be used later for

Authentication, i. e., it is valid for only one Log In Session. By this, a number of short comings that are faced by us earlier are reduced, such as Replay Attacks, Social Engineering, Sniffing, etc.

The proposed technique can resist many popular attacks like Password Stolen Attacks, as a Password used once, if hacked by Intruder, cannot be used again, as each time a new Dynamic Password is used to access the System. It also provides the features like Trust Maintenance between the Client and the Server, Identity Management of the User and Access Control to the Services that a particular User is going to access.

## VIII. References

[1] A. J. Choudhary, P. Kumar, M. Sain, H. Lim & H. J. Lee, "A Strong User Authentication Framework for Cloud Computing", IEEE Asia – Pacific Services Computing Conference, 2011, 110 – 115

[2] M. H. Guo, H. T. Liaw, L. L. Hsiao, C. Y. Huang & C. T. Yen, "Authentication using Graphical Password in Cloud"

[3] H. A. Dinesha & V. K. Agarwal, "Multi Level Authentication Technique for accessing Cloud Services"

[4] S. Kolhe & S. Dhage, "Trusted Platform for support Services in Cloud Computing Environment", International Conference on System Engineering & Technology, 11 – 12 September 2012, Indonesia

[5] S. Jain "Security Challenges and Resolutions in Cloud Computing", UACEE International Journal of Advances in Computer Networks and its Security, Vol. 2, Issue 1

[6] R. L. Krutz & R. D. Vines, "Cloud Security – A Comprehensive Guide to Secure Cloud Computing", Wiley India Publications.

[7] Cong Wang, Qian WangKui Ren, Ning Cao, and Wenjing Lou ―Toward Secure and Dependable Storage Services in Cloud Computing‖ IEEE transactions on services computing, vol. 5, no. 2, april-june 2012

[8] Qian Wang,Cong Wang, Kui Ren, Wenjing Lou Jin Li ―Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing‖ IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011.

[9] Norshakila Muhamad Rawai 1,a, Mohamad Syazli Fathi 2,b, Mohammad Abedi 1,c, , Shuib Rambat 3,d,‖ Cloud Computing for Green Construction Management‖,2013

[10]Haibo Mi, Student Member, IEEE, Huaimin Wang, Member, IEEE, Yangfan Zhou, Member, IEEE,

[11] R. Agarwal, H. Lucas, The information systems identity crisis: focusing on highvisibility and high-impact research, MIS Quarterly 29 (3) (2005) 381–398.

[12] T. Alford, G. Morton, The Economics of cloud computing, Booz Allen Hamilton,2009.

[13] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A.Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the Clouds: A Berkeley View of cloud computing, University of California at Berkeley, 2009.

[14] P. Bhoj, S. Singhal, S. Chutani, SLA management in federated environments,Computer Networks 35 (1) (2001) 5–24.