Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# One Time Password for Multi-Cloud Environment

**Richa Chowdhary**
Department of Computer Science Engineering
Amity School of Engineering and Technology
Noida-125

**Satyakshma Rawat**
Department of Computer Science Engineering
Amity School of Engineering and Technology
Noida-125

***Abstract- Cloud computing has changed the IT industry ever since it evolved. Cloud computing is basically cost effective and on demand service offered to the clients. The resources in the cloud are rented according to the needs and budget of the client. As the cloud has involvement of many parties and resources its security remains a major issue. Cloud Computing is still not able to reach its true potential due to limitations in security offered in the cloud. In the present scenario, there is dependency on more than one cloud i.e. organizations use services from multiple clouds. This leads to a multi-cloud or cloud-of-clouds environment. Security in such a multi cloud environment is an even more complex issue to deal with as authentication and authorization of more than one cloud are required at once. Cloud is synonymous with the Internet. So the first step in dealing with the cloud security is the use of usernames and passwords. Even passwords get hacked and can prove to be unsafe if used over a long time. One Time Passwords are better way of using user name-password based authentication.***

***In this paper we discuss the use the one time password implementation for authenticating services from multiple clouds at once. This paper elaborates what actually the cloud is. It then elaborates about the use of multi-clouds in organizations. It then investigates the security issues in cloud and finally the one time password concept. The implementation of this model is then discussed.***

***Keywords— computing; cloud security; cloud authentication; multi-clouds; one time password***

## I. Introduction

Cloud computing supports variety of service models like SaaS(Software as a Service), PaaS(Platform as a service), IaaS(Infrastructure as a service) to name a few. This section elaborates what actually the cloud is in section 2.1. It then elaborates about the use of multi-clouds in organizations in section 2.2. It then investigates the security issues in cloud in section 2.3 and finally the one time password concept is discussed in section 2.4

### 1.1 Cloud computing

The term ‘cloud computing’ is made up of two terms, cloud and computing. Cloud could be thought to be synonymous with the Internet where various resources are interlinked with the use of network. One can use the resource they want with the help of simple client-server architecture. The term ‘computing’ refers to processing. Cloud computing is computing on various resources over the network. In cloud computing Infrastructure, Platform and Application/Software are delivered as service over the network. The cloud concept has changed the IT market wherein organizations need not invest on resources; they rather rent the required resource on on-demand basis or take services from the cloud which has reduced the infrastructure costs in manifold. Cloud is basically used in three models namely, (Software as a Service), PaaS(Platform as a service), IaaS(Infrastructure as a service). Major of use of SaaS model of cloud computing lies with end users, where they store their critical, important and real time information. PaaS model of cloud computing is used mostly by Application developers, who use the platform from cloud as a service to develop, test, debug and deploy their applications. It is basically a middleware for developers. IaaS model is used by network analysts. Here services like storage, networking, and database management are also offered. In general pay per use payment model is followed here. The end user is generally interested only in SaaS. The data is consumed as well as produced by the cloud. This data is used by cloud computing systems and client computing systems as well. Cloud computing has no specific definition as such. However, one acceptable definition was given [1] which more or less defined cloud computing. It states cloud to be “*A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.*” Though cloud computing is an evolving technology; it has not yet been standardized. There is plenty of ongoing work in this regard.

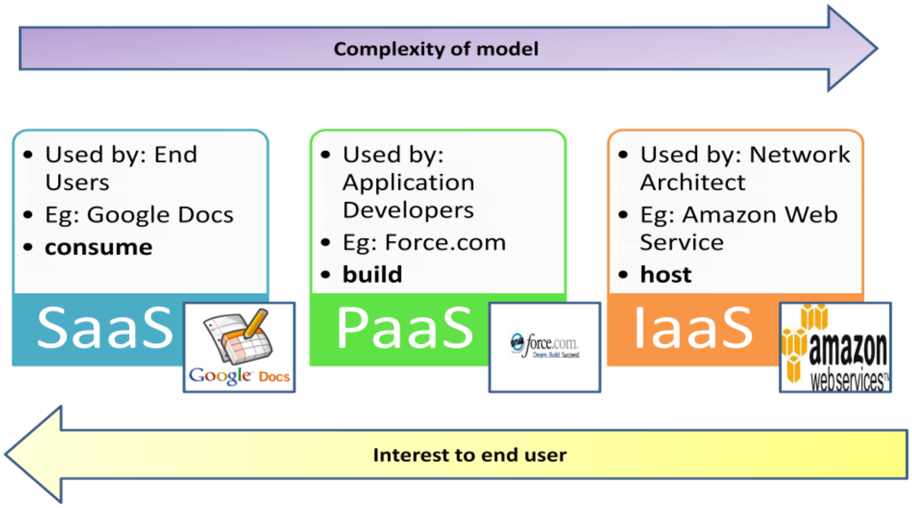

**Figure 1: Cloud computing models**

### 1.2 Multi-Cloud environment

These days, organizations tend to rely on more than one cloud for services. The clouds could be public clouds, private clouds as well as hybrid clouds. Organizations have started working in this multi cloud environment so that they never face lack of availability of a service or a resource at any point of time and could prevent from potential loss. Also trusting a single cloud is risky as there could be some malicious user or software who is spying on the data being exchanged. So, to deal with these issues multi cloud environments have gained importance. The term multi cloud as defined by Vukolic[2] is “cloud of clouds- which says that the term cloud computing should not end up as a single cloud”.

The most popular is the public cloud. Here, the provider of cloud services provides the user with applications, storage, resources etc. it is majorly the responsibility of the cloud provider to provide the features of security, availability, scalability etc. The infrastructure for provided such clouds are generally shared. Consumers are either charged on a pay-per-use basis or it may also be free like first 500MB of Google App Engine are free. Other popular clouds are the private cloud within an organization. It may be connected via Internet or Intranet. It is created solely for use by an organization and its users. Hence, security concerns are less here as it also has a dedicated infrastructure for its cloud hence multi tenancy issue is also avoided. However, managing the cloud, its data, users etc all remain the responsibility of the organization providing the cloud. Users are generally not required to pay for such cloud. There may also be a condition where both these clouds and their services may be required. Such a scenario leads to hybrid cloud. Rules and protocols are to be developed to use hybrid cloud as per the need and convenience[3].

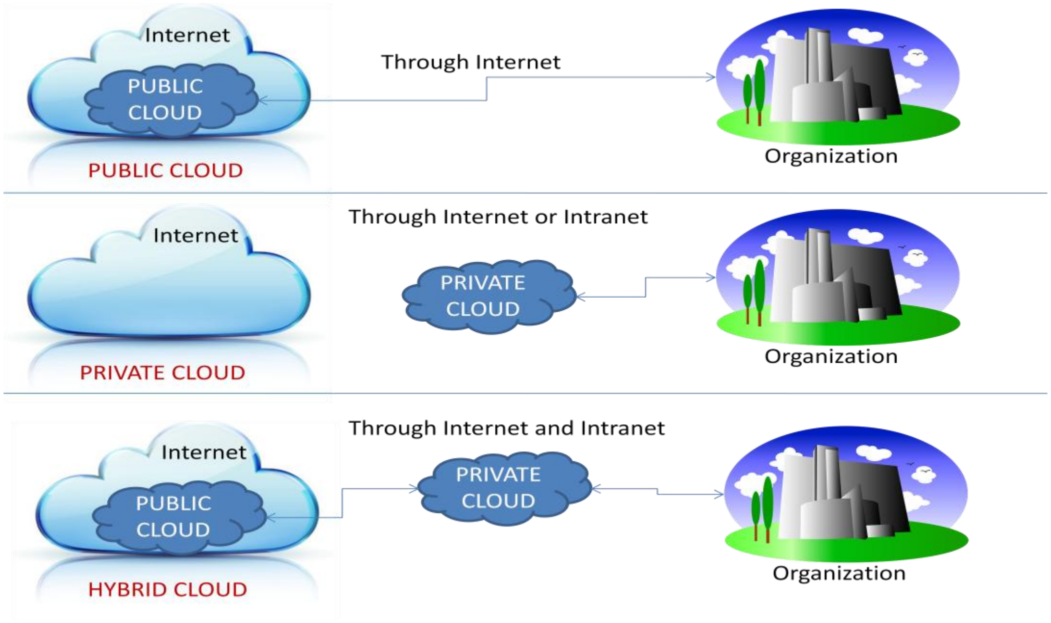

**Figure 2: Architecture of cloud data storage (CDSs)**

### 1.3 Security issues in cloud computing

The number or risks in cloud computing are various evolving from the fact that it includes use of various resources over the network. Primary issue of concern include authentication for which user names and passwords are used. Another issue is authorization for services for the authentic user by the cloud vendor. Another issue includes data confidentially, which should be maintained while data is transmitted over the cloud. For this various techniques like checksum, hash functions are used. Also Byzantine fault-tolerant replication protocol[] within the cloud is intended to be implemented to maintain confidentiality of data over the cloud. Another major issue includes protecting the cloud from malicious attackers or data intrusion. Various encryptions schemes are used for this purpose. Lastly, service availability is also a potential risk of failure to the cloud. For this data redundancy is introduced. Also data is replicated and stored over various locations or data centre. Moreover availability of data in real time is also a risk.

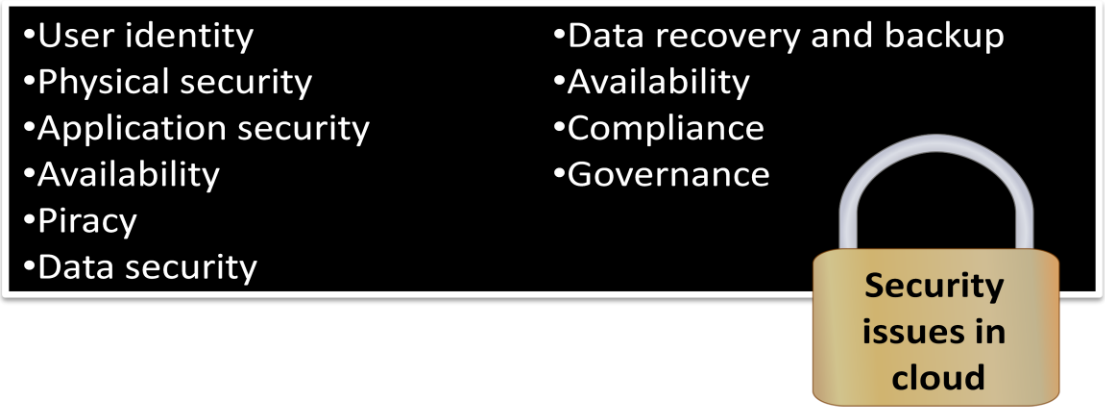

**Figure 3: Security Issues in cloud**

- ➢ User Identity: Accessing resources like infrastructure, software or hardware over internet by different individuals increase the security issues. Therefore User Identity is required to authorize the person accessing the resources.
- ➢ Physical Identity: Over internet sometimes the users doesn't want to reveal their physical location . For this purpose the Physical Identity is to be kept confidential. Therefore, physical identity is also some of the concerned security issues in cloud.
- ➢ Application security: As clouds provide the services and applications over internet, so there security is to be taken into consideration because user provide their information for accessing application. Hence, security of the applications is a necessity in cloud.
- ➢ Data Integrity: "Protection of data stored in the cloud during transmission is known as data integrity." defined by Alzain [3]. It is an important security issue.
- ➢ Availability: Availability basically defines [4] "data is continuously available in any situation either normal or disastrous". Availability is also a security issue in cloud because the data should be available to the user all the time and there should be no loss in data.
- ➢ Authentication: Authentication if defined is [5] "confirmation of any data, identity being processed and accessed". The whole concept of security came into existence for this purpose.
- ➢ Authorization: " The permission to access or process any data within the network", [6]. The Authorization is also one of the main and important security issues around which whole security concern lies.

### 1.4 One Time Password Schemes

Passwords are used by almost all business applications for authentication. However static passwords have lots of limitations e.g. passwords can get hacked; careless employee may write down passwords somewhere; system with saved passwords may be used by various users or a malicious user may reset all passwords just to create havoc. Hence it is advisable to move to a more dynamic password scheme like one time passwords or OTP. OTP [7] are way more secure than static passwords as there are no chances to forget or reuse passwords. Each time a new password is generated for each login session. Authentication by one time passwords are more reliable and user friendly as well. OTP generation can be done by various OTP generation algorithms for generating strings of passwords.

## II. Design Of Otp In Multi Cloud Enviornment

One time password for authenticating multiple clouds is really useful. There are various private clouds that organizations use. Also they tend to use one or more public clouds. This leads to authenticating them again and again over the period of time for each login session. To avoid the overhead we can use OTP for multi cloud environment. Also OTP ensures safety. For this we need to design authentication software that can generate OTP and can connect to all clouds. Authentication is the first step of ensuring privacy and security. It is done at the application layer of the OSI model. We can use a private cloud and a public cloud. Cloud can be created using Openstack and Ubuntu 12.10 for research purpose. We can implement the OTP by designing authentication software using the .NET framework. This application can further be deployed at the cloud for use over the entire organization.

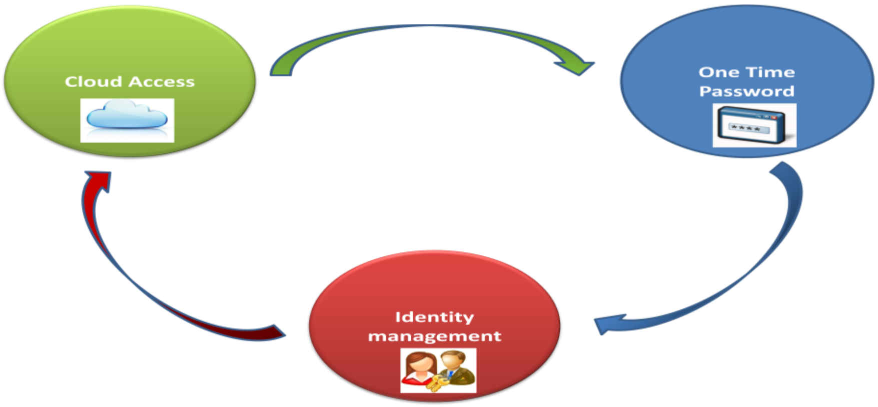

**Figure 4: Working of OTP mechanism in multi cloud**

## III. Conclusion

One Time Password implementation for multi-cloud environment enforces tight security on the clouds. Passwords can easily be exploited in general. However OTP reduces the chances of misuse of passwords. While at the same time it can save considerable amount of overhead in logging again and again to various clouds to take their services. OTP have been in use for quite some time but its implementation in muti cloud scenario is still not there.

## IV. Future Scope

OTP is a form of security offered. The security can further be enhanced with the use of firewalls and antivirus. Also a lot of work is been done on various other authentication and authorization techniques, integrity of data and confidentiality of data in cloud. Cloud is still a budding technology and needs various improvements and standardizations.

## ACKNOWLEDGEMENT

We would like to thank our mentor Dr. Abhay Bansal for motivating us to pursue the research work in this area. He has always been there to educate us, guide us, motivate us and enlighten us. This would have not been possible without him.

## Refrences

[1] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu:"Cloud Computing and Grid Computing 360-degree compared", IEEE conference 2008.

[2] M. Vukolic, "The Byzantine empire in the inter cloud", ACM SIGACT News, 41,2010, pp.105-111.

[3] M.A.Alzain, E.Pardede, B.Soh, J.A.Thom: "Cloud Computing Security: From Single To Multi Clouds", 45th Hawaii International Conference on System Sciences,2012.

[4] D. Linthicum, "Selecting the right cloud," book excerpt, InfoWorld Cloud Computing Deep Dive, InfoWorld, Sept 2009

[5] Rongxing et al, "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing", ASIACCS'10, Beijing, China.

[6] Soren Bleikertz et al, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", CCSW 2010, Chicago, USA.

[7] W.B.Hsieh, J.S.Leu: "Design of a time and location based one time password authentication scheme", 7th IEEE International Conference,2011.

[8] Jinpeng et al, "Managing Security of Virtual Machine Images in a Cloud Environment ", CCSW, 2009, Chicago, USA.

[9] Dan Lin & Anna Squicciarini, "Data Protection Models for Service Provisioning in the Cloud", SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA

[10] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security.

[11] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciences 2011.