International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 4, Issue 4, April 2015)

Ensuring Secure Cloud Premises : An Approach Towards Enhancing Security

Nirmla Sen[1], Prof. Monali Sahu[2]
[1]M.Tech Scholar, [2]Prof. Dept. of CS, Takshshila Institute of Engg. & Tech. Jabalpur

***Abstract*-- The concept of Cloud Computing comprises of many computers which are connected through a real time network like that of internet. Cloud computing is a dynamic delivery of information technology resources and capabilities as a service over the internet. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet. Cloud provides facility to share distributed resources and services that belong to different organizations or sites. In this paper we have proposed an innovative technique for generating a dynamic password which is applied to authenticate the cloud computing platform. The Proposed technique is based on the one time password generated through a device.**

***Keywords*-- Cryptography, Public Key, Encrypted one time password.**

I. INTRODUCTION

Cloud computing is based on the concept of distributed computing over a network, where a program or application may run simultaneously on many connected computers. This concept basically refers to a computing hardware machine commonly referred to as a server connected through a communication network such as the network, a local area network (LAN) or wide area network (WAN) or an intranet. Only an authorized person who has access rights to access the server can use the processing power of the server to run an application, store data, or perform any other computing task. It has benefitted a person for using a personal computer every-time to run the application from anywhere in the world.

There are four types of cloud models , they are:

1. Public
2. Private
3. Hybrid
4. Community

1.1 Public Cloud

It is one in which the cloud infrastructure and computing resources are made available to the general public over a public network.

1.2 Private Cloud

A private cloud gives a single cloud consumer's organization the exclusive access to and usage of the infrastructure and computational resources.

1.3 Hybrid Cloud

It is a composition of two or more clouds.

1.4 Community Cloud

It serves a group of cloud consumers which have shared concerns such as mission objectives, security, privacy and compliance policy rather than serving a single organization as does a private cloud.

II. CLOUD SERVICES

These services are categorized into these prominent sections which are as follows:

2.1 Infrastructure as a Service (IaaS): It is a model based on the concept that the entire infrastructure is deployed in an on-demand model. It almost always takes the form of a virtualized infrastructure and infrastructure services that helps the customer to deploy virtual machines as components that are managed through the console.

2.2 Software as a Service (SaaS): It is a model in which the prebuilt applications such as CRM, word processing, spreadsheets, and HRM are offered to customers via a web browser or other local interface such as mobile device application.

2.3 Platform as a Service (PaaS): It is a model in which specific development and deployment platform for example Java, EE, IBM Web Sphere etc is the basis for deployment.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 4, Issue 4, April 2015)

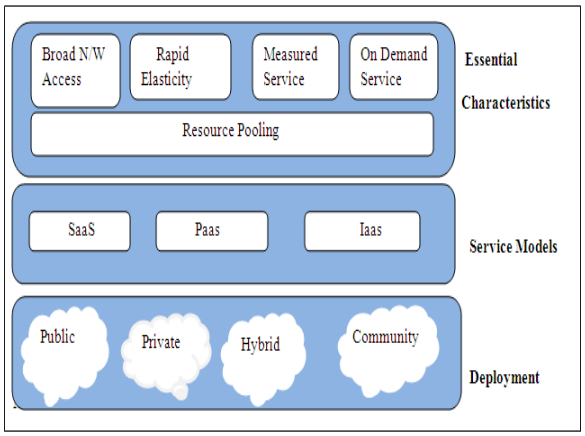

Fig1: NIST working model of cloud computing [1]

III. Security Issues In Cloud Computing

It is a major concern for companies who have already adopted cloud services . However an association of cloud vendors and users believe that it provides security services for our information on the cloud .There are a number of security issues pertaining to the used of cloud services.In todays scenario the primary issue of concern is the authentication for which static user names and passwords are used. Next comes the issue of authorization which means verification of users and yet another issue is of confidentiality of data.which is quite importanat while transmitting data across the network.Various encryptions schemes are used for this purpose. Lastly, service availability which means providing of services on demand 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.

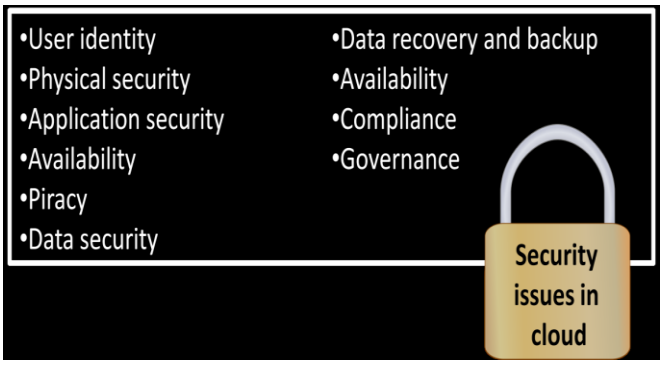

Fig 2: Security issue in cloud Computing [1]

3.1 User Identity:

Security issues are increasing as accessing of resources like infrastructure, software or hardware over internet by different individuals. Therefore User Identity is required to authorize the person accessing the resources.

a) Physical Identity: When user needs to hide his physical identity for certain confidentiality issues this is known as physical identity.

b) Application security: Since applications and services in cloud are provided over the internet so it is mandatory to enhance the application security in cloud.

c) Data Integrity: protecting data during transmission in the cloud environment refers to as data integrity. Defined by Alzain [1]. It is an important security issue.

d) Availability: Availability basically defines [2] "making the data continuously available in any situation either normal or disastrous". The theme of availability is to make data available to the cloud user without any loss.

e) Authentication: It means verification of data identity [3]. The whole concept of security came into existence for this purpose.

f) Authorization: The access rights provided for accessing data in a network. [4]. The It is also one of the main and important security issues around which whole security concern lies.

3.2 Some well known security challenges in cloud computing are:

a) *Increased attack surface:* with the advent of new technologies vulnerabilities are also increasing. The virtual access layer adds a new dimension for threat vectors.

b) *Shared Environments:* In cloud environments subscribers typically share infrastructure, applications and other resources. Threats to the network and computing resources can be amplified when sharing with unknown outside co-subscribers.

c) *Privacy issue:* These issues include lack of user control, unauthorized secondary usage, transformer data flow and data proliferation etc.

3.2 One-time password (OTP):

It refers to an authentication technique where user is valid with a password only for a single login. OTP concepts are based on the concept of time synchronization which overcomes the flaws which were present in the static password schemes.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 4, Issue 4, April 2015)

This two factor authentication is based on the concept that the unique password can only be generated accornding to the two factor scheme which shows that something a person have and something a person knows. [1]

Various approaches for the generation of OTPs are listed below:

- **OTP based on synchronization** between the the client and authentication server providing the password which is valid only for short period of time.
- OTP can also be generated by using a mathematical **algorithm** to generate a new password based on the previous password these are also called seed chain technique.
- It can also be generated based on a mathematical **algorithm** where the new password is based on a challenge.
- Our present proposed solution works on the concept of Time Synchronization. In this method, a device with an internal clock generates passwords that are dependent on the current time. For example, at every time pulse a the device generates a new password, and at the same time the password is generated on the server which matches with the password generated on the client device if both are same user is allowed to login and access the cloud.

IV. Proposed Solution

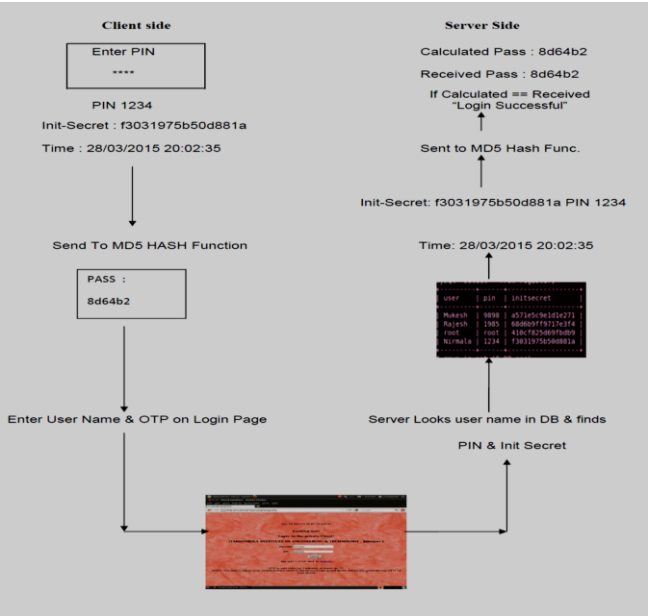

Fig 3: Process diagram

4.1 The Working methodology of the proposed solution is as follows:

1. To get Init secret User feeds PIN as 0000 on to the device.
2. Then 25 random numbers are pressed to get a 16 digit secret field called Init-Secret.
3. User enters the Init Secret which is feed into the Registration Page.
4. On the basis of PIN chosen we generate a password on our device.
5. Now we put the Init Secret in the Registration page .
6. Now the user successfully joins and is redirected to the login.
7. Now User types his User name and OTP being generated on the device.
8. The server checks for the authenticity and if the password being generated by device is same as that of password generated on server, user is authenticated.

V. Conclusion

In this paper we have shown how static passwords are less secure and can be prone to security threats moreover this paper proposes the concept of dynamic password using the concept of time synchronization which ensures a unique one time password being generated which certains that only authentic user who have access rights can access the cloud services moreover it can save considerable amount of overhead in logging again and again to various clouds to take their services.

REFERENCES

[1] 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.

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

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

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

[5] http://en.wikipedia.org/wiki/Cloud_computing.

[6] Atul Kahate, Cryptography and Network Security , Tata McGraw-Hill Publishing Company Limited.

[7] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi.

[8] http://en.wikipedia.org/wiki/One-time_password

[9] H:B Kekre,V.A Bharadi , International Journal of Intelligent