International Journal of Scientific Research in Computer Science and Engineering

Review Paper Vol-1, Issue-4 ISSN: 2320-7639

Securing the Cloud Environment Using OTP

Vimmi Pandey

Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Available online at www.isroset.org

Received: 18 April2013 Revised: 25 April 2013 Accepted: 06 May 2013 Published: 30 June 2013

Abstract- In today’s scenario, websites have been converted from just a display of information into an online transaction in the form of goods, services, or money. Along with development, the security of the website is also need to be tightened, not just rely on usernames and passwords but also to the dynamic code of the mobile token which is difficult to be cracked. Dynamic mobile token is an application which is planted in the mobile phone to generate a code that was formed by the method of one time password and can only be used for one login session or transaction. Each mobile token has a value in the "secret" variable that makes it unique or different from the others, to separate one user access transactions or personal page

Keywords- One Time Password, MD5 Algorithm, Website Security, Authentication, Mobile Token

1. INTRODUCTION

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures.

Security is one of the major issues which is hampering the growth of cloud computing. It is difficult, from a user perspective, to over-protect a service. If you make the login process too hard for a user, the user might grow tired of that service. It is also important for the cloud providers to have good security standards in order for the common users to trust the cloud, for future growth of the cloud technology. In a cloud system, company susceptible data and information will be stored on third-party servers, and user will possibly have very inadequate understanding or control regarding this information. So, there was a great demand for strong authentication system, which will not going to allow, the unauthorized user to access the cloud.

There are also four different cloud deployment models namely

(i) Private cloud,

(ii) Public cloud,

(iii) Hybrid cloud

(iv) Community cloud.

(i) Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user’s access and the networks used are restricted.

Corresponding Author: *Vimmi Pandey*

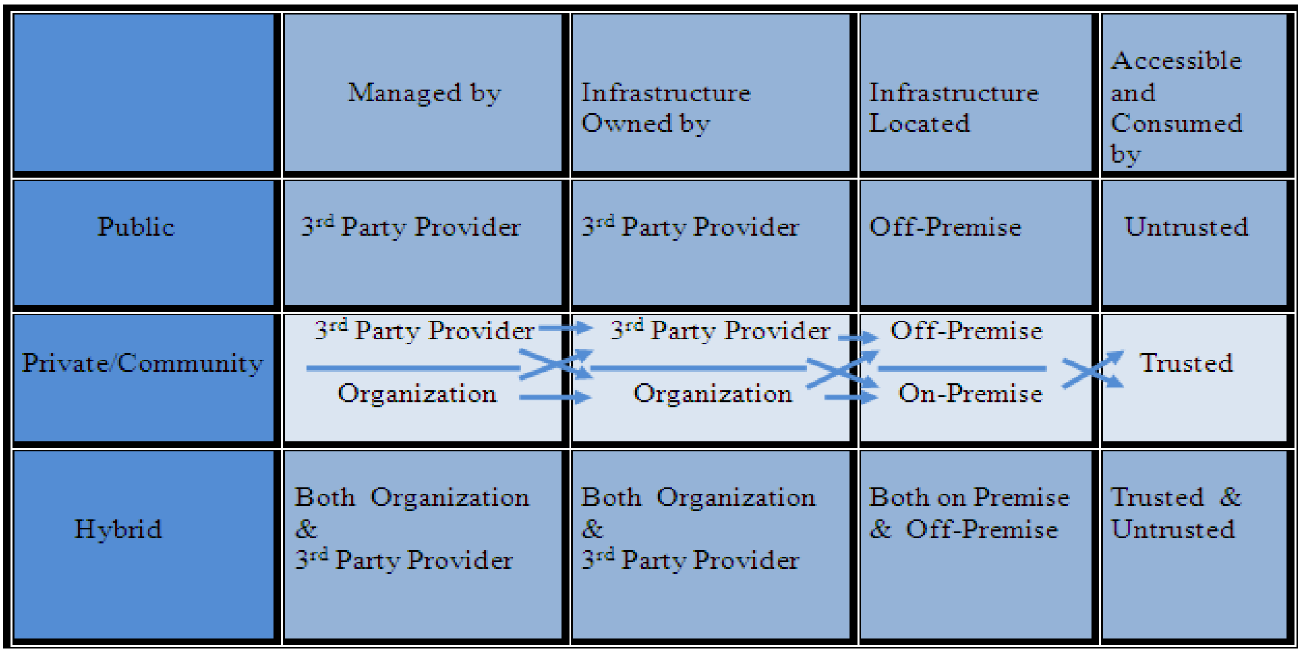
(ii) Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. Examples of a public cloud include Microsoft Azure, Google App Engine.

(iii) Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing.

(iv) Community Cloud: Infrastructure shared by several organizations for a shared cause and maybe managed by them or a third party service provider and rarely offered cloud model.

In cloud computing, the available service models are:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service(SaaS



	Managed by	Infrastructure Owned by	Infrastructure Located	Accessible and Consumed by
Public	3rd Party Provider	3rd Party Provider	Off-Premise	Untrusted
Private/Community	3rd Party Provider Organization	3rd Party Provider Organization	Off-Premise On-Premise	Trusted
Hybrid	Both Organization & 3rd Party Provider	Both Organization & 3rd Party Provider	Both on Premise & Off-Premise	Trusted & Untrusted

Cloud Deployment Models (Bardin et al. 2009)

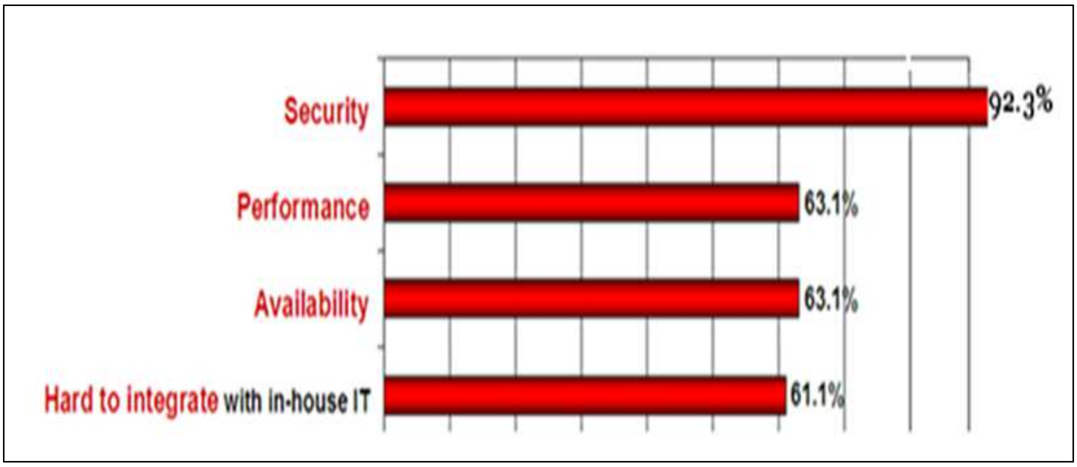
In cloud computing, the available service models are:

◦ *Infrastructure as a Service (IaaS):* Provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allow the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

◦ *Platform as a Service (PaaS) :* Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

◦ *Software as a Service(SaaS):* Provides the consumer with the capability to use the provider's applications running on a cloud infrastructure.

The concept of One time password (OTP) is that it is only valid for a single login session or transaction [1]. It is widely used as a password that is not static in the database, but only as a single use password. The use of encrypted static passwords are also not immune from the attack by using a key logger [2] or sort of it, because if an attacker managed to get the main password and OTP password still login and transactions will not be processed because the password is no longer valid. Code generation as encryption is using Message-Digest Algorithm 5 (MD5) which are widely used with 128-bit hash value, this algorithm has been widely used for security applications, password encryption, and integrity test of a file [3].



Source : IDC Enterprise Panel , Jan 2012

The application of Dynamic Mobile Token uses three codes consisting of epoch time as the key of one time password, the value of the "secret" variable in which each user has a different value so that when it degenerate at the same time, it will result in different value, and 4 digit random value between 1000 and 9999 resulting from the website. These three values are then combined and encrypted with md5 algorithm to generate the output of the value of 128 bits or 32 hexadecimal numbers. Only first 6 digits of the hexadecimal number are used from the result of the output.

2. PREVIOUS STUDIES

A. Cloud Computing Service

Cloud computing can be defined as 'computing service that provides customers with IT resources by utilizing internet technology' [4]. Cloud computing not only enables the scattered services on internet to be more convenient, but also allows easier access to the personal data that are also scattered. These convenience and dispersion the access to information is the central characteristics of its virtualized service that cloud computing provides for its customers [5, 6].

B. User Authentication in Cloud Computing

The representative authentication security technologies that are often used in cloud computing are as Table I shows.

i) ID/Password- Most common personal authentication process and it can be used by only memorization.
ii) Open key authentication certificate - Using the open key passwords .The level of security is determined by the location of the personal key or authentication certificate and the pass coding or decoding.
iii) Multi-Factor authentication- Several methods are combined to enhance the security level
iv) SSO (Single Sign On) - Only authenticate in one place and send the information to other place to exempt the procedure there.

3. MATERIALS AND METHODS

3.1 Findings For Otp

The previous password system was a static authentication which posed a great threat as it can be easily hacked by multiple use .To overcome this danger the concept of OTP was introduced to strengthen the security.

The aim of authentication is to prove that the accessing user is the real user. There are many methods that can prove it, but for authentication methods can be seen in the three categories of methods:

i]. Something You Know

It is the most common authentication method. This method is relying on the confidentiality of information, such as passwords and PIN. This method assumes that no one knows the secret unless the user itself.

ii]. Something You Have

This is usually an additional factor to create a more secure authentication. This method relies on items which usually are unique, for examples, the magnetic card/smartcard, hardware tokens, USB tokens, and else. This method assumes that no one has the hardware unless the user itself.

iii]. Something You Are

This is the most rarely used method because of technology and the human factor as well. This method relies on the uniqueness of the body parts that is not exist in others such as fingerprint, voice, retina or fingerprint. This method assumes that the parts of the body such as fingerprints and retina are different with others.

3.2 Methodology

There are various methods to implement one time password (OTP) technique, which are as follows [7]

a) Time Synchronization - In this technique, both the client and server will have synchronous time clocks and it use an algorithm that generates one-time password from that synchronous time and any other inputs (PIN). In this time is used as the changing factor, which changes every 60 seconds. The token time must be synchronized with the authentication server time. That is, if the authentication server and the user token don't keep the same time, then the expected OTP value won't be produced and the user authentication will fail.

b) Event Synchronization – In this method, both the client and server will typically have an identical initial seed i.e. counter value. Whenever client wants to login, it generates a one-time password from the initial seed and any other input (PIN) and updates the seed (increment/ decrement the counter). User submits this one-time password generated to server. Server also generates the password for that instance using the seed (counter) and other inputs. If both passwords match, the server authenticates the user and updates the seed (increment/ decrement the counter).

c) Asynchronous Challenge-Response Technique –In this technique, every time the application presents a dynamically generated unique challenge to the user when it tries to login to server. User enters this challenge into the client software. Then the client software use some crypto primitive technique to generate a unique password by the combination of challenge and any other information (PIN) provided. Each time server generates a new challenge for user when it wants to login. This offers good security because This offers good security because the intruder has to start the brute-force search from scratch every time a new one-time password is generated.

3.3. Password Mode

Dynamic Mobile Token there are two mode used [8,9] :

1. Challenge/Response Mode (C/R) [10]
This mode is most often used when doing transaction. In this mode the server provides a challenge in the form of a series of numbers. That number must be entered into the Mobile Token to get an answer (response). Then the user enters the number that appears on its own Mobile Token into text box on the website. Mobile Token will issue a different code though with the same code challenge. Periodically depending on the time when we answer the challenge in a token.

2. Self Generated Mode (Response Only)

In this mode the server does not give any kind of value (challenge). Mobile Token users can directly issue a series of combination of numbers and letters without having to enter the challenge. As the mode C/R, Mobile Token also issued different codes periodically depending on the time when the token is ordered to produce self-generated code.

3.4 Related Work

i) Lin, Shen, and Hwang [11] has proposed a strong password authentication scheme by making use of smart cards, and claimed their scheme can resist guess attack, replay attack, impersonation attack and stolen attack. Later on, W. C.Ku. has proposed a hash-based strong-password authentication scheme to enhance the security without using smart card. However, it still has the intrinsic weakness and suffers some attacks.

ii) A. Saxena [12] has proposed a technique in which he suggested to use one time password (OTP) for authentication. The generated OTP was based on event synchronization technique. For that, he has used a counter value, that must be synchronized between client and server. But many times it happens that client counter has been incremented but due to some network problem request doesn't reach to server and counter value between client and server become different.

iii) M. Viju Prakash, P. Alwin Infant and S. Jeya Shobana [13] in their paper they has proposed a system which was based on challenge response technique to generate one time password and was fully based on SMS service. But SMS services have its drawback, such that many times it does not delivers the SMS on time due to the network or coverage problem. As, in OTP technique it is very important that SMS should reach on time.

4. PROPOPOSED SYSTEM

The Figure below shows that how authentication will be carried out. Steps which will going to involve during authentication is listed below

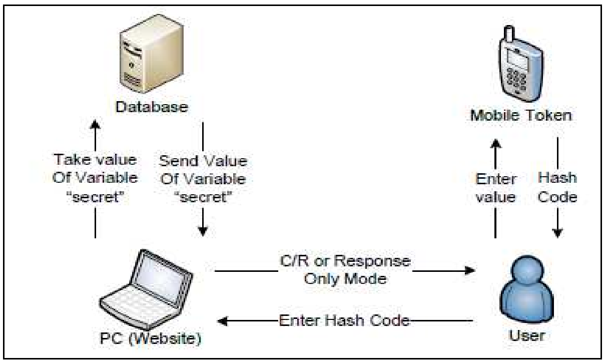
i) A client wishes to log in will surfs to the login page.

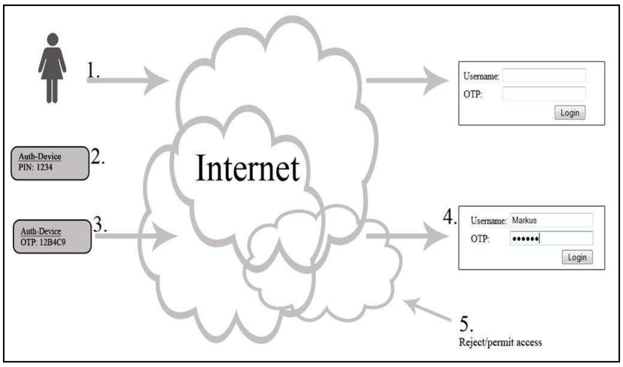
ii) The client then starts an application on a mobile phone, and enters a PIN code.

iii) After entering the PIN code, OTP is generated and displayed on the phone.

iv) The client enters his username and the OTP at the login page, and sends the information to the authentication server.

v) The server either permits or denies the client to access the cloud.





i) Registration phase.

ii) Login phase.

Each new user has to first register itself to the cloud for accessing the services of the cloud. After the registration process user can login into the cloud by using the credentials which it has supplied during the registration process.

i) Registration phase

In this phase client will register itself to the cloud. For registration process client will has to provide some information to the cloud such as user name, pin code and init secret. User name that will be chosen by client must be unique, means no other user with the same user name will be allowed, pin code can be any 4 digit number and init secret is the hexadecimal code which is used to initialize the mobile phone as an authentication device. For generating the init secret user will run MID let on its mobile phone, it will prompt the user to enter the pin code for initializing the mobile phone first time user will enter '0000' in place of pin code, after that it will ask the user to enter 25 random number on basis of that init secret will be generated, which will use by client during registration Process . After the user registration its information is added to server side database, containing the user name, pin code and its init secret as shown in figure 2. Only registered users can login to cloud, as its init secret is stored in client mobile and is only known to server during registration process. On basis of that init secret, pin code and time as a dynamic factor, one time passwords are generated, so no unauthorized user can login to cloud.

ii) Login phase

For login-in to the cloud, user will enter his user name and one time password (OTP) which has been generated on its mobile phone, on to login page. This user name and one time password will then send to server for authentication. At server side, it will also generate one time password and will match with the received one time password. If received OTP and server generated OTP are same, then only user will allowed to login to the cloud otherwise its access will be denied. One time passwords (OTP) are generated based on three parameters-

1) The current time.

2) The 4-digit PIN code

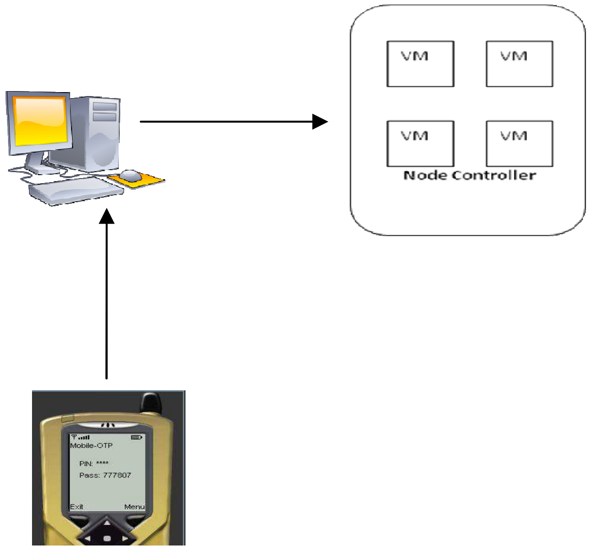
3) Init-secret

These three parameters are then hashed together with MD-5 and will generate an OTP, which will then used by user to login. At the server side, server knows 4-digit PIN code and Init-secret, for proving authentication it will also calculate OTP by using current time of the server. As, it is based on time synchronization technique so mobile time and server time must be properly synchronized If calculated OTP and received OTP are same, then user will allowed to access the cloud. Since time is part of the hash, so OTP is valid only for three minutes. During the registration process and at the time of login and even when user accesses the services from the cloud lots of important information is transmitted through the network. For securely transmitting all the information between the client and server secure socket layer has been used. HTTPS protocol has been used for that purpose. It is responsible for transmitting all the information in secure manner. The main concept of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection against eavesdroppers attack and man in the middle attack, provided that adequate cipher for data is used. For securely transferring all the information AES-256 encryption technique has been used. It will encrypt all the information by using this encryption technique so that sensitive information doesn't disclosed to anyone.

4. PROPOSED WORKING MODEL

The model which I propose in the present scenario works like this:
i) The user logs in to the system using Mobile OTP.
ii) Server I is the cloud controller which is used to access various installed applications on srever II.

The proposed model can be built using a VM ware with ubuntu installed on it, Mobile phone is used to authenticate server and access the private cloud. Now server comprise of node controller.The proposed system calls upon authenticating the server.



5. Benefits of OTP in Cloud Computing

i) OTP offers strong two-factor authentication.
ii) The OTP is unique to this session and cannot be used again
iii) OTP offers strong security because they cannot be guessed or hacked
iv) Provides protection from unauthorized access Easier to use for the employee than complex frequently changing passwords
v) Easy to deploy for the administrator Good first step to strong authentication in an organization
vi) Low cost way to deploy strong authentication

6. Conclusion

Certainly cloud computing will be a boon in enhancing information systems as its benefits outnumber its shortcomings. Cloud computing offers deployment architecture, with the ability to address vulnerabilities recognized in traditional IS but its dynamic characteristics are able to prevent the effectiveness of traditional counter measures. In this paper we have identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats So, in this paper we have proposed to make use of Dynamic one time password with two factor authentication as a strong authentication technique which requires mobile phone as an authentication device. In this technique mobile phones are responsible to produce OTP which is valid only for 3 minutes. A combination of Mobile OTP and SSO can address most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained.

REFERENCES

[1] Dr. Mark D. Bedworth PhD BSc FSS. February 2008. A Theory of Probabilistic One-Time Password. Computer Science Computer Engineering and Applied Computing, Security and Management.

[2] Kiddo. 2010. Hacking Website: Menemukan Celah Keamanan & Melindungi Website dari Serangan Hacker. Mediakita

[3] Rivest, Ronald L. 1992.The MD5 Message Digest Algorithm.

[4] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, " Security Enhancement in Cloud Computing (CC)", IJSRCSE, Volume-01 , Issue-01, Page No : 31-37 3013

[5] Rajesh Piplode, Pradeep Sharma and Umesh Kumar Singh , "Study of Threats, Risk and Challenges in Cloud Computing", IJSRCSE, Volume-01 , Issue-01, Page No : 26- 30, 2013

[6] Vishal Paranjape and Vimmi Pandey' " An Improved Authentication Technique with OTP in Cloud Computing" IJSRCSE, Volume-01 , Issue-03, Page No : 22-26, 2013

[7] "Privacy and consumer risks in cloud computing", Dan Svantesson, Roger Clarke, computer law & security review 26 (2010) 391e97, @ 2010 Svantesson & Clarke. Published by Elsevier Ltd. doi:10.1016/j.clsr.2010.05.005.

[8] N. Haller, Bellcore, and C. Metz. 1996. A One-Time Password System. Kaman Sciences Corporation.

[9] Fadi Aloul, Syed Zahidi, Wassim El-Hajj. 2009. Two Factor Authentication Using Mobile Phones. Digital Library Telkom Institute of Technology (IEEE).

[10] Arya Sapoetra Y. June 2010. Rancang Bangun Arsitektur Library Sistem Autentikasi One Time Password Menggunakan Prosedur Challenge-Response. Informatics Engineering, Pembangunan Nasional "Veteran" University, East Java.

[11] C.W. Lin, J. J. Shen, and M. S. Hwang, "Security enhancement for optimal strong password authentication protocol," ACM Operating Systems Review, vol. 37, no. 2, pp. 7-12, April 2003.

[12] "Dynamic Authentication: Need than a Choice", A. Saxena, Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference, 10 (1) (2008), 214, IEEE conference.

[13] "Eliminating Vulnerable Attacks Using One-Time Password and PassText – Analytical Study of Blended Schema" M. Viju Prakash, P. Alwin Infant and S. Jeya Shobana, IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI) (2):35–41, 2011. Published by Foundation of Computer Science.