World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:6, No:10, 2012

A Secure Mobile OTP Authentication Scheme for User Mobility Cloud VDI Environment

Jong-won Lee

Open Science Index, Computer and Information Engineering Vol:6, No:10, 2012 publications.waset.org/4820.pdf

***Abstract*—**Since Cloud environment has appeared as the most powerful keyword in the computing industry, the growth in VDI (Virtual Desktop Infrastructure) became remarkable in domestic market. In recent years, with the trend that mobile devices such as smartphones and pads spread so rapidly, the strengths of VDI that allows people to access and perform business on the move along with companies' office needs expedite more rapid spread of VDI.
In this paper, mobile OTP (One-Time Password) authentication method is proposed to secure mobile device portability through rapid and secure authentication using mobile devices such as mobile phones or pads, which does not require additional purchase or possession of OTP tokens of users. To facilitate diverse and wide use of Services in the future, service should be continuous and stable, and above all, security should be considered the most important to meet advanced portability and user accessibility, the strengths of VDI.

***Keywords*—**Cloud, VDI, OTP, Mobility

I. Introduction

As adaptation of cloud computing increases rapidly, there is a concern for more security-sensitive design to maintain continuous development of the relevant technology. Recently, the global corporations such as Google, Amazon, Microsoft, and IBM etc., have led the cloud computing technology, and also some domestic corporations such as Samsung, SK Telecom, KT, and LG also provide the service[1].

Therefore, as cloud environment emerged as the central keyword in the relevant business, the growth of the VDI (Virtual Desktop Infrastructure) has attracted most attentions. Particularly, in 2011, not only big conglomerates but also most security-concerned businesses such as banks began constructing VDI environment, which gives many businesses new challenge of VDI.

The main reason for many corporations to adopt VDI is its tangible effects in security and accessibility. Especially, the rapid growth in mobile devices such as smart phones or tablets and the growing demand for the work access in the outside by accessing clouds agree with the VDI's nature, and thereby further push its rapid adaptation.

However, although this enhanced accessibility and mobility can bring the enhanced productivity, it sometimes conflicts with the security, so there should be more detailed security solution, which is user authentication [2].

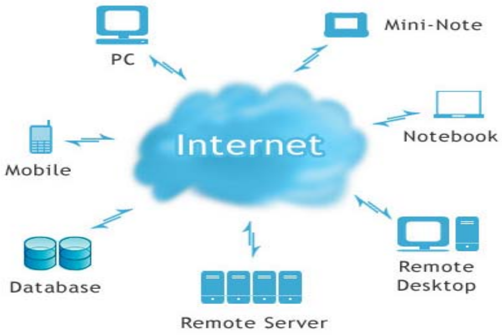

Fig. 1 Cloud Services

Thus, in this paper, mobile OTP (One-Time Password) authentication method is proposed to secure mobile device portability through rapid and secure authentication using mobile devices such as mobile phones or tablets, which does not require additional purchase or possession of OTP tokens of users. Also, this paper will provide explanation which defines the necessary components to realize this type of authentication, and its procedure in authentication and services.

This paper is designed in following way. Chapter II will examine the current examples of user authentications and cloud computing. Chapter III suggests the new solution for the user authentication guaranteeing the users' mobility under the could VDI environment. Chapter VI will conclude the entire analysis.

II. Previous Studies

A. Cloud Computing Service

Cloud computing can be defined as 'computing service that provides customers with IT resources by utilizing internet technology' [3]. 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 [4].

There are three categories that divide the service types of cloud services, as Table I shows.

Jong-Won Lee is with the Information Systems Management Team, National Research Foundation of Korea, Daejeon, 305-350, Korea (phone: 042-869-6712; fax: 042-869-6584; e Email: antonio@nrf.re.kr).

Open Science Index, Computer and Information Engineering Vol:6, No:10, 2012 publications.waset.org/4820.pdf

TABLE I
TYPES OF CLOUD SERVICES

Category	Contents	Example
Saas (service as a service)	Only provides services that users need	Salesforce.com's CRM service, U cloud service
Paas (Platform as a service)	Provides standardized flatform	App engines by Google
Iaas (Infrastructure as a Service)	Provides IT resources such as server, storage, DB etc. which are required for establishing a service or system.	Amazon's AWS services such as EC3 and S3

B. User Authentication in Cloud Computing

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

TABLE II
USER AUTHENTICATION TECHNOLOGIES

Types	Features
ID/Password	Most common personal authentication process. Can be used by only memorization
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
Multi-Factor authentication	Several methods are combined to enhance the security level
SSO(Single Sign On)	Only authenticate in one place and send the information to other place to exempt the procedure there

Therefore, it appears that ID/Password, Multi-Factor authentication etc., used by user input of the synchronized personal information on the web interface, and smart card-based authentication which is based on the system providing the standardized interface on the web browsers, and SSO types etc. will be mostly used among the diverse security technology above.

C. Threatening Elements in Cloud Computing

According to the data reported by RAD Lab in Berkeley University in 2009, the 10 elements of threats to cloud computing environment were reported, as in the Table III.

Therefore, this paper tries to come up with solutions for the authentication which is most urgent among 10 threats. For this matter, chapter III will suggest OTP authentication, which guarantees both user mobility and the cloud VDI environment.

TABLE III
THREATS TO THE CLOUD COMPUTING

Types
1. Availability of Service 2. Data Lock-in 3. Data Confidentiality and Auditability 4. Data Transfer Bottlenecks 5. Performance Unpredictability 6. Scalable Storage 7. Bugs in Large Distributed System 8. Scaling Quickly 9. Reputation Fate Sharing 10.Software Licensing

III. MAIN ANALYSIS

A. Conventional OTP-token Authentication

The conventional password system is a static authentication type, and can be exposed to dangers of illegal reuse when tapped through the network. Thus OTP is introduced to eliminate dangers from using the static type of passwords and strengthen the security of authentication.

1. Types of OTP-token Authentication

Since OTP does the authentication process by the OTP generating device (hereafter token) that users have and the password generated by this, it provides double authentication process and stronger security than the static type that provides a single process. OTP is divided into Asynchronous type and Synchronous type depending on whether there is a synchronization process, as shown in Table IV[6].

TABLE IV
ASYNCHRONOUS TYPE & SYNCHRONOUS TYPE

Asynchronous type	Pros	Users actively input the set of values sent by OTP authentication server -clear responsibility when there is an accident -mutual authentication process
	Cons	Users should always input the set of values -inconvenient to use -when values are repeated, it can be exposed to danger
Synchronous type	Pros	OTP token always generate different password every few minutes -convenient to use
	Cons	When there is time difference between the token and the authentication server, users should manually set the time again

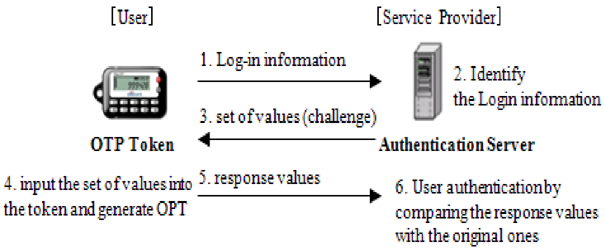
[User]
[Service Provider]
1. Log-in information
2. Identify the Login information
3. set of values (challenge)
OTP Token
Authentication Server
4. input the set of values into the token and generate OPT
5. response values
6. User authentication by comparing the response values with the original ones

Fig. 2 OTP's mutual communication

Open Science Index, Computer and Information Engineering Vol:6, No:10, 2012 publications.waset.org/4820.pdf

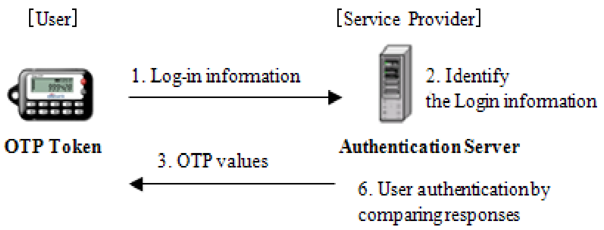

Fig. 3 Synchronization process of OTP

2. *Trend of Standardization of OTP*

OATH (Open AuTHentication) was an organization founded by the suggestion of VeriSign in America, in February 2004. Currently, based on its open standard, the organization leads standardization process related to OTP, to found strong authentication system and expand the technology to public. HOTP (HMAC based One-Time Password) uses event-synchronization authentication process with the OTP algorithm suggested by OATH as a standard.

Also, it is used in the OTP devices supporting OATH by using HMAC-SHA1 algorithm. This is documented as IETF RFC 4226 in December 2005, and reported in the IETF meeting in March 2006.

B. The Authentication Suggested in this Paper

This paper suggests a solution that enables to use cloud services quickly in the cloud VDI environment while users are in motion, without always carrying OTP tokens or cards that are conventionally used.

1. User Authentication Process

To provide users appropriate services in cloud, it is necessary to collect data to identify users. Thus when users come into the cloud environment, they go under the user identification process and the authentication process. Figure 4 & 5 shows the procedure of authentication for users to initiate their service and to reuse the service later.

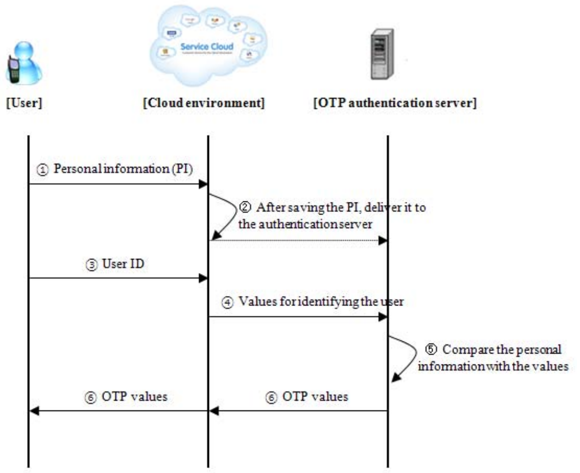
[User]
Service Cloud
[Cloud environment]
[OTP authentication server]
① Personal information (PI)
② After saving the PI, deliver it to the authentication server
③ User ID
④ Values for identifying the user
⑤ Compare the personal information with the values
⑥ OTP values
⑥ OTP values

Fig. 4 User authentication procedure for the initial use

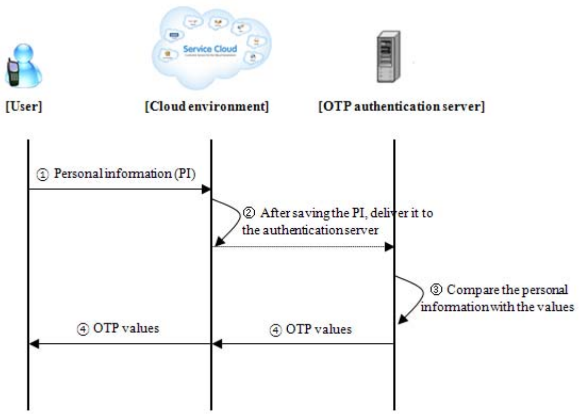
[User]
Service Cloud
[Cloud environment]
[OTP authentication server]
① Personal information (PI)
② After saving the PI, deliver it to the authentication server
③ Compare the personal information with the values
④ OTP values
④ OTP values

Fig. 5 User authentication procedure for the revisiting users

1) When users come into the cloud environment, personal information (PI) is delivered to the cloud server for using the service. However, PI should be delivered only once for the initial login.

2) In the cloud server, after identifying the user information, it saves the PI in the server and deliver it to the OTP authentication server.

3) User will send his or her own ID to the cloud server for using the service.

4) The cloud server identifies the user and sends OTP authentication server the user identification values (PI_ID).

5) OTP authentication server identifies and compares PI_ID with the PI that it had before.

6) If the user information is congruent with each other, it sends the OTP values to the user. The user will finish authentication process by using the delivered OTP values, and begin using cloud service.

2. Comparative analysis with OTP-token types

OTP-token type authentication is that users follow the authentication process by using OTP tokens, and no additional devices are required other than the OTP-generating device, which is convenient and widely used. However, users should purchase the separate device and always carry the device with oneself, which creates some inconveniences. Also, the information is saved in the independent device, and the process takes about 60 seconds of synchronization process, which is relatively short.

The authentication process suggested here does not require the purchase of separate OTP token or carrying the device always with oneself, but its OTP-generating algorithm is integrated into the mobile devices such as cell phones or tablets as a software module, which gives secure and fast authentication processes to users who use mobile OTP and get access to the cloud VDI environment.

However, to utilize various services adapted in mobile devices in the cloud VDI environment, the mobile devices with OTP generating functions attached should be widely used in the first place, and the service providers should support the stable services by providing more differentiated strategies in their services provided through the mobile devices. Table V compares the conventional OTP token authentication with the process suggested in this paper.

TABLE V
COMPARATIVE ANALYSIS BETWEEN OTP-TOKEN AUTHENTICATION AND THE SUGGESTED MODEL

	OTP token-authentication	Suggested model
Security	-Danger against the hacking by MITM (man in the middle)	-Danger against the hacking by MITM (man in the middle)
Authenticating components	-Multi-factor authentication	-Multi-factor authentication
Purchase & control	-Costs arise from purchase & replacement -The device needs to be in control	-No cost for purchase & replacement -easy to update the software version
Portability and Receptivity	-Users should always carry the device and some possibility to be lost	-No need to carry everywhere & always -no danger to be lost
Accessibility	-Easy	-Easy

IV. CONCLUSION

This paper suggests an authentication method that can provide quick and secure access to cloud service under the cloud VDI environment even when users are in motion. Compared to the conventional OTP token type, this authentication process does not require to carry the device always and there is no cost for purchasing or replacing the device, and can provide easy access to the cloud service with convenient authentication process. However, as I mentioned above, the service should be consistent and stable for users to use cloud services broadly and in various ways, and most of all, the security issue should be always concerned importantly as other characteristics of cloud VDI such as portability and accessibility.

REFERENCES

[1] Seung-Ah Lee, Gi-Hwan Cho, “A Secure User Authentication Scheme for Public Cloud Environment,” Korea Information Processing Society (Published Conference Proceedings style) vol. 18, no. 1, pp. 909-912, May. 2011

[2] Mun-Hwan Park, “The need for enhanced user authentication in the cloud VDI environment,” IDG Tech Focus, pp. 10-11, Jan. 2012.

[3] Myung-Jun Kim, “Korea's Cloud Computing Strategy," IT21 Global Conference, 2009

[4] Hyun-Seong Kim, Choon-Sik Park, “Cloud computing and the personal authentication service,”Journal of the Information Security, vol. 20, no. 2, Apr. 2010.

[5] Jeong-Kyung Moon, Jin-Mook Kim and Hwang-Rae Kim, “An Efficient user authentication protocol for cloud computing environments,” Journal of the Korea Academia-Industrial cooperation Society, vol. 12, no. 5, pp. 2353~2359, May. 2011.

[6] Ki-Young Kim, “The Study on the authentication system based on One-time password,” Journal of the Information Security, vol. 17 no. 3, Jun. 2007.

[7] Financial Security Agency, “Financial information security week,”2006.

Open Science Index, Computer and Information Engineering Vol:6, No:10, 2012 publications.waset.org/4820.pdf