International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-5)
Research Article | **May 2013**

An Approach of Authentication in Public Cloud using Two Step Verification Code

Namrata Thakur *
PG Student
MTECH (CSE),Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Mrs. Vimmi Pandey
Head of Department of Information Technology, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Abstract— With the advent of cloud computing the task of users have become far easy as cloud provides various benefits to its users. As by the definition given by NIST (National Institute of Standards and Technology) cloud provides convenient, on demand network access to shared pooled of resources. Although cloud provides so many benefits still security is one of the major challenge in front of cloud providers. Users move their confidential data and applications onto the cloud which needs to be secured to gain users trust. Gaining users trust needs providing security on cloud. Security is needed in cloud as it provides heterogeneity of services and multi domain access. Security can be enforced in cloud by only letting authentic users gain access to cloud. Authentication could be provided using static password but there are various security breaches in this, therefore this technique of authentication is no longer an adequate solution for authentication. This paper proposes a dynamic approach towards password generation and using it as user authentication measure on cloud. The dynamic password will be sent on registered e-mail id of users and user will input it as password to access cloud along with the static password chosen by user, in this sense two times checking of user authentication takes place one by static password and other by dynamic password and hence called two step verification.

Keywords- Authentication, static password, dynamic password,security, trust.

I. INTRODUCTION

Cloud security is a hot topic and two-factor authentication is one way to mitigate users' well founded concerns. As a result, development and adoption of two-factor authentication systems is proceeding at a rapid pace and should be available for most cloud applications within just a few short years. Though Cloud offers sophisticated storage and access environment, it is not hundred percent reliable; the challenge exists in ensuring the authorized access. Because third parties make the decision regarding our data, security is a big concern. So cloud must ensure that the data accessed is by the trusted users. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It is a way by which it is verified that someone is who they claim they are. In private and public networks (ie. internet) authentication is commonly done through the use of logon passwords. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a fingerprints, smart card, retina scan, voice recognition, or signature. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password.

II. RELATED WORK

Earlier Lamport used Hashing function for authentication of users but this approach needed password resetting which was a major drawback [7]. Afterwards, Shimizu [8] solved Lamport's problem by proposing CINON without password resetting, together with PERM protocol [9] in finding the solution for the random number memorizing problem of CINON protocol. But none of them has direct focus on the solution for the problematic web authentication, and still contained the complicated procedure which was difficult to be practically implemented. Lin, Shen, and Hwang [10] 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. [11] 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. Song Luo, Jianbin Hu and Zhong Chen [12] has proposed a one-time password scheme using the smart card based on the bilinear pairings. It was based on the Computational Diffie-Hellman Problem.

III. Authentication Tools

- **ATM Cards:** These are perhaps the most widely used two-factor authentication device. The user must both insert the card and enter a password in order to access the ATM.
- **Tokens:** The use of tokens has increased substantially in recent years. Most of these are time-based tokens that involve the use of a key sized plastic device with a screen that displays a security code that continually changes. The user must enter not only their password, but also the security code from the token. Tokens have been popular with sensitive applications such as on-line bank and brokerage sites.
- **Smart Cards:** These function similarly to ATM cards, but are used in a wider variety of applications. Unlike most ATM cards, smart cards have an embedded microprocessor for added security.

- **Smart Phones:** The proliferation of smart phones has provided the perfect impetus to expand two-factor authentication to widely used internet applications in the cloud. In these cases, users must enter not only a password, but also a security code from their phone or other mobile device. This code can be sent to a phone by the service provider as an SMS text message or generated on a smart phone using a mobile authenticator app. Both Google and Dropbox now use this method.

IV. Authentication Principals

The authentication is based on 3 factors or principals [3][4] on basis of which person's identity is verified prior to grant access to resources. These principals are as follows:

1. "Something the user knows" e.g., password, PIN
2. "Something the user has" e.g., ATM card, code generator
3. "Something the user is" e.g. fingerprint or iris scan.

V. Dynamic Password

Various security issues has been reported regarding static password based authentication method , due to which there was a significant financial loss caused to the enterprises .This factor was highlighting the fact that the traditional static password based authentication solutions are no longer an adequate protection mechanism. So there was increasing pressure from regulatory bodies on enterprises to use strong forms of authentication to mitigate the identity theft related problems. The main weakness with static passwords is the human interaction when choosing the secret password. If the password is to simple, it will be exposed to different kinds of threats where an attacker will try to crack it, such as social engineering, trojan attacks, password attacks, key loggers or by just trying to guess the password. On the other hand, if the user picks a very hard password, it will be very hard to remember, leading to writing the password down on a piece of paper and store it under the keyboard, which is a big security risk. It can also lead to more work for the IT administrators when users forget their passwords, forcing the administrator to take valued time to reset passwords. This necessitates enforces the enterprises to explore more robust, secure, multifactor, dynamic password based authentication technologies into their
IT infrastructure[1] .

The dynamic password is one of strong authentication technologies. It has the following features:

a) Dynamism: - The dynamic password generated by the token changes with the dynamic factor, so that the generated dynamic password varies from time to time.

b) One-time Usability: - A dynamic password can be used only once. It will not be valid then. Therefore, disclosure of the used dynamic passwords does not matter.

c) Randomization: - Each time a dynamic password is generated randomly. It is unpredictable.

d) Resistance of Exhaustive Attacks: - If the correct dynamic password is not hit in a minute, the attack must be restarted. Thus, the new dynamic password may have been attempted. In addition, the number of attempts to logon can be restricted in a minute by system settings.

e) Irreproducibility: - The dynamic password relates to the token. Each token generates a different set of dynamic passwords. In addition, the token is sealed physically. Once the token is powered off, the key data will be lost. Thus, only the user with a legitimate token can obtain a correct dynamic password.

f) Rapid Discovery of Risk: - Because users carry the token with them, once the token is lost, users can take an action timely to reduce their loss to the minimum.

g) Anti-theft Capability: - The dynamic password is anti-theft because of its randomization and one-time usability.

The dynamic password is also referred to as the One Time Password (OTP). Once a dynamic password has been consumed or used for authentication, it cannot be used for later authentication (a new dynamic password is required then). A one-time password (OTP) is a password that is valid for only one login session. OTPs have overcome a number of short comings that has been faced with traditional (static) password such as replay attack. This means that, if a potential intruder manages to record an OTP that was already used to log into a service or to conduct a transaction, he or she will not be able to abuse it since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology. A OTP can be generated using different methods [5],[1],[2] and is often used in conjunction with a device that is synchronized with an authentication server:

1) **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. With time-synchronized OTPs, the user typically must enter the password within a certain period of time before it's considered expired and another one must be generated.

2) **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). In this technique, it may happen that the seeds on client and server may drift (due to passwords generated by client but not submitted, passwords submitted by client but does not reaches to server due to network failure, etc.).So, synchronizing the client's seed value stored at client and server is a major challenge in this method. This also offers simple to use solution that can be easily integrated with most of the existing enterprise applications that are password aware.

VI. Proposed System

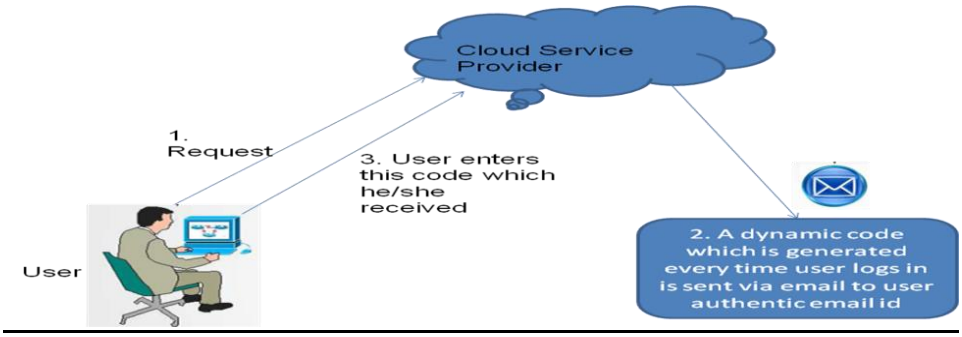
Due to the limitations in the static password approach of authentication, a new approach of dynamic authentication is proposed which has benefits like

- It is free of cost to attract more and more set of user.
- It is user friendly approach and easy to use as well.
- Adds an extra level of security.

This paper proposes a system with two step of authentication leading to an extra level of security. The whole task is divided into two steps:

1. User Registration- In this step user registers himself on the cloud environment giving his/her details like user name password and a valid email id which is must.
2. Authentication during log in- After the registration is successfully done the user tries to login in on the cloud environment as soon as he tries this system ask the user to input his user name and password, if user is a pre registered user and knows these details he enters those details, when user enters his/her details a dynamic code is generated by the system and is sent on the email account of the user given during registration. At the same time a copy of dynamic code is also kept at the cloud, next the user is asked to input the code and the user once does that, the code is sent to the cloud where it is matched with the existing copy of the code, if it matches the user authenticity is checked and is given permission to access the cloud otherwise not. This process happens every time user logins in into the cloud environment. The concept behind this scheme is that the email account of user is considered as being secure on which confidential information could be sent and no one else other than user has access to his account. This ensures confidentiality as well.

Two-factor authentication using email



Two-factor authentication involves not only the use of something the user knows such as a password, but also something that only the user has that is the dynamic code generated and sent to the user's email. An intruder can no longer gain access to the system simply by just obtaining your password.

In the proposed system, during the user registration, user information is carried through internet. So, to overcome from any security risk, SSL (Secure Sockets Layer) will be used between client and server. In contrast to the traditional Internet Protocol Security (IPSec). To maintain the integrity and non repudiation of data RSA algorithm will be used.

VII. Conclusion

Although there are extreme advantages of using cloud based system but still security is a major flaw in front of cloud. This paper focuses on various security issues related to static password and how dynamic password technique has overcome them.

References

[1] "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.

[2]. "Two-Factor Authentication: An essential guide in the fight against Internet fraud": WHITEPAPER GPayments Pty Ltd.

[3] "Authentication" http://en.wikipedia.org/wiki/Authentication

[4] "Access control system , verifying the authencity of an identity " http://www.informit.com/guides/content.aspx?g=security&seqNum=146 .
[5] "One time password" http://en.wikipedia.org/wiki/One-time_password .
[6] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
[7] L. Lamport. Password authentication with inse-cure communication. Communications of the ACM. 1981, 24 (1):770–772
[8] A. Shimizu. "A dynamic password authentication method by one-way function". IEICE Trans. Inform. Syst. 1990,73 (1): 630–636
[9] A. Shimizu, T. Horioka, and H. Inagaki. "A password authentication method for contents communication on the Internet". IEICE Transactions on Communications. 1998: 81 (2): 1666–1763.
[10] 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.
[11] W. C., Ku, "A hash-based strong-password authentication scheme without using smart card" ACM Operating Systems Review, vol. 38, no. 1, pp. 29-34, Jan. 2004.
[12] Song Luo, Jianbin Hu and Zhong Chen "An Identity-Based One-Time Password Scheme with Anonymous Authentication "International Conference on Networks Security, Wireless Communications and Trusted Computing 2009.