ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

Analysis of Novel Authentication Methods

S.Thangavelu[1], T.Purusothaman [2]

Senior Lecturer, IRT Polytechnic College, Chennai, India[1]

Associate Professor, Government College of Technology, Coimbatore, India[2]

ABSTRACT: Cloud computing is one of the most powerful and emerging technology for everyone in the Internet field. Cloud computing refers to an on demand, pay per usage service through Internet infrastructure that enable users to access computing resources from anywhere at any time. Cloud services and all other online activities require some type of authentication to access the resources and data stored on the cloud. Authentication means to check the identity of the user, with the credentials provided by them at the time of registration. Authentication prevents unauthorized users from gaining access to the protected resources. Secured authentication systems must ensure the identity of the users who claim to be. This paper analyzes the various types of conventional authentication methods available at present and the novel methods proposed for the improvement of cloud security.

KEYWORDS: Authentication, Password, Image, PIN, Cloud computing.

I. INTRODUCTION

Authentication is a process of identifying a person normally based on username and password. In all web based applications, authentication is the process, which grant access to the individual to the system objects and resources based on their identity. Authentication merely ensures that the individual is who he or she claims to be. Various types of authentication methods are employed in various types of web based security methods. The ways in which someone may be authenticated mainly falls into the following three categories [11],

Something you know (password, PIN, passphrase, challenge response etc)
Something you have (smart cards, security token, cell phone etc)
Something you are (fingerprint, retinal pattern, DNA, signature, face etc)

II. CONVENTIONAL AUTHENTICATION METHODS

The popular Conventional Authentication methods used in different cloud based applications are classified as under.

- Password or PIN based authentication
- SMS based authentication
- Symmetric key authentication
- Public key authentication
- Biometric authentication

Password or PIN based authentication

Using password or Personal Identification Number (PIN) to login, is the most common knowledge based (something you know) authentication method. The longer the password, the stronger is the protection. As a best practice for security, strong passwords that contain the Combinations of numbers, symbols, and mixed cases should be enabled as far as possible in an authentication system. Graphical passwords using colors, images, 3D passwords are also used to identify the identity of the users.

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

SMS based authentication

SMS is used as a delivery channel for a one time password (OTP) generated by an information system. The OTP is sent as an SMS message to the user cell phone, and the user enters the password to complete the authentication. Internet banking system is an example for SMS based authentication

Symmetric-key authentication

In symmetric key authentication method the users shares a unique, secret key with the authentication server. The user need to send a randomly generated message known as challenge encrypted by the secret key to the authentication server. The server will match the received encrypted message (response) using its shared secret key, then the user is authenticated. OTP token is based on this approach with few modifications, which generate the OTP on user side for matching with that generated on server side

Public key authentication

Public key cryptography is another popular method provides an authentication that uses a private and public key pair. The private key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others.

Biometric authentication

Biometrics is a method by which the user authentication information is generated by digitizing the measurements of a physiological or behavioural characteristic. Biometric authentication verifies the user's claimed identity by comparing an encoded value with the data stored in the system database. If match occurs then authentication will be granted.

III. NOVEL AUTHENTICATION METHODS

IMAGES FOR AUTHENTICATION

Images are more secured than text. Dhamija and Perrig [1] proposed an approach to improve the security of the web systems which relies on recognition based methods instead of recall based authentication. They proposed Deja Vu, which authenticates a user through their ability to recognize previously seen images. Deja Vu is more reliable and easier to use than traditional recall based schemes, which require the user to exactly recall passwords or PINs. It is based on the Hash visualization technique. In this system the user is asked to select a certain number of images from a set of random images by the system as shown in figure 1. At the time of Login the user have to identify the preselected images in order to get authenticated.

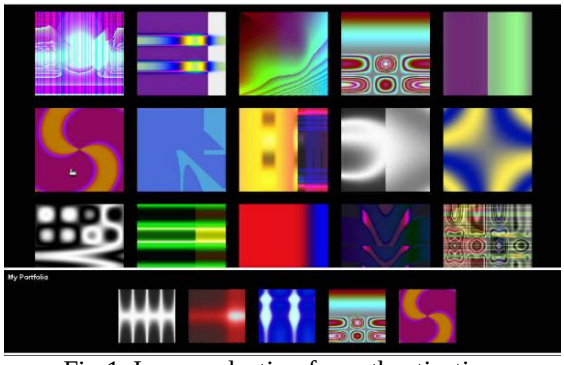

Fig.1. Image selection for authentication

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

IMAGE BASED REGISTRATION &AUTHENTICATION

Akula [2] proposed a similar image based registration and authentication system shortly known as IBRAS. The system displays an image or set of images to the user, who would then select one to identify them. Image registration enables users to have their favorite image. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1 algorithm produces a 20 byte output which is very secure and requires less memory.

GRAPHICAL PASSWORD

Sobrado and Birget [3] suggested the Graphical password technique. In this method the system will display a number of pass objects preselected by the user along with many other objects. To get authenticated the user needs to recognize pass objects and click inside the convex hull formed by objects as shown in figure 2.

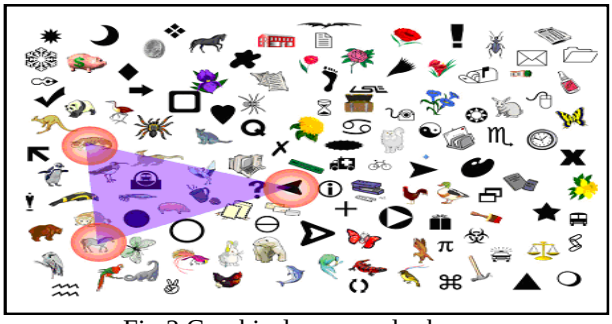

Fig.2.Graphical password scheme

DRAW A SECRET METHOD

Jermyn et al [4] proposed a technique, called 'Draw a secret' which allows the user to draw a simple unique picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication the user is asked to redraw the picture. If the drawing touches the same grid in same sequence, then the user will be authenticated. The concept of 'draw a secret' authentication method is shown in figure.3.

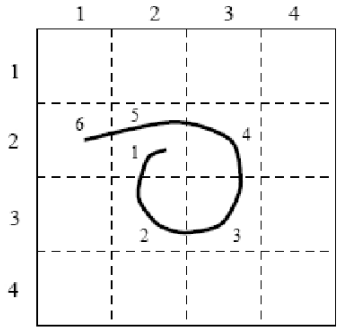

Fig.3.Draw a Secret Method

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

GRAPHICAL PASSWORD SCHEME

Mathuri Pandi [5] proposed that a series of connected questions will be generated by the system at the time of registration. The answers to the questions are stored in the form of pictures. While Login, a Globe picture will be displayed for the question 'which is your favorite place' if Delhi is the chosen answer then the user has to click 'India' in the globe. After expanding to India from the Globe he has to click 'Delhi', as shown in figure 4.

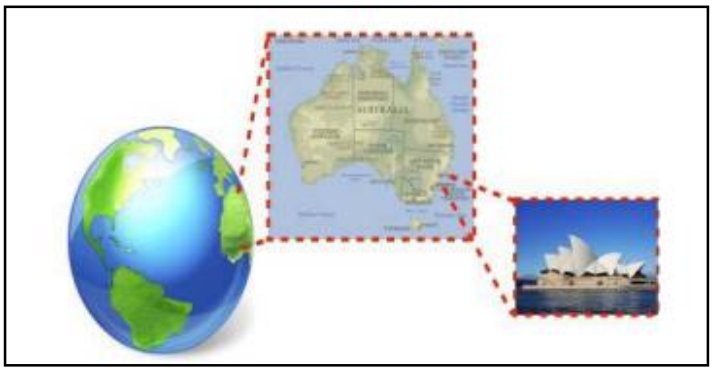

Fig.4. Secured Graphical password scheme

PICTURE PASSWORD METHOD

Jensen et al [6] proposed another graphical password scheme based on picture password, especially for mobile devices. During the password creation, the user has to select the theme first (e.g. sea and shore, cat and dog etc) which consists of thumbnail photos. The user then selects and registers a sequence of the selected thumbnail photos to form a password. The user needs to recognize and identify of the previously seen photos and touch it in the correct sequence using a stylus in order to be authenticated. In order to create a complex password the user can select one or two thumbnail photos as one single action in order to create the size of the password space. The picture password by cat and dog is shown in figure.5.

Fig.5. Pass code using Cat and Dog

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

PASSFACES METHOD

Brostoff et al [7] proposed pass face method for authentication. At the time of registration the user need to choose their pass face set either male or female. They have to select four face images. Humans are more capable of remembering the face images and during login they need to click the pass face images in order to get authentication. The concept of pass face authentication method is shown in figure.6.

Fig.6. Pass face Method

PASS POINT METHOD

Wiedenbeck et al [8] proposed a Pass Point scheme in which user has to select a background image. User can click arbitrarily anywhere on the image to register sequence of click points to be registered as password. When logging in, the user has to click on points as done during registration time. The click points are acceptable if they are within the predefined level of tolerance as shown in figure.7.

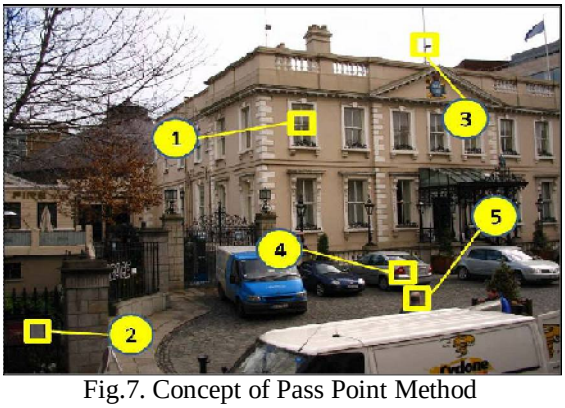

Fig.7. Concept of Pass Point Method

PASS DOODLE METHOD

Varenhorst [9] proposed the Pass doodle scheme for authentication. It is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen. It shows that the users were able to recognize a complete doodle password as accurately as text based passwords. The Pass doodle scheme has many

ISSN(Online) : 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

drawbacks. The Pass doodle scheme is vulnerable to several attacks such as guessing, spyware, key logger, and shoulder surfing. The pass doodle authentication is shown in figure.8

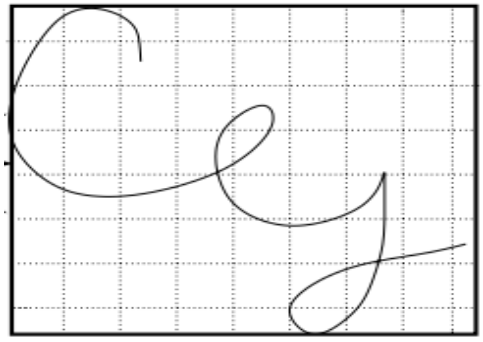

Fig.8.Pass doodle

FINGERPRINT METHOD

Vajna[10] proposes an effective fingerprint verification system . Fingerprint recognition is the technology that verifies the identity of a person based on fingerprints. It works on the fact that everyone has unique fingerprints. This method identifies the fingerprint image and validates the identity of a person by extraction of essential information from the reference image and matching with the captured image. The information is obtained from the reference image by filtering and careful minutiae extraction procedures. His fingerprint identification is based on triangular matching to cope with the strong deformation of fingerprint images due to static friction or finger rolling. The matching is finally validated by dynamic time warping techniques.

IV. CONCLUSION

Authentication is the first and most important process, which verifies the user credentials and grant access to log into the network, cloud services and web applications. The conventional authentication methods are normally performed by a username and password or PIN etc. In order to provide high security and to protect the resources from unwanted intruders on the network, novel authentication methods are introduced. Multiple numbers of Cognitive activities ensures more security and becomes a challenge to the intruders in different forms. Thus Cognition based novel authentication methods become the best alternate and employed in most of the web based applications. Thus the overall security of the cloud services and web applications are improved.

REFERENCES

[1] Rachna Dhamija and Adrian Perrig, " Deja Vu: A User Study Using Images for Authentication", SIMS/CS, University of California Berkeley.
[2] Srinath Akula and Veerabhadram Devisetty "Image Based Registration and Authentication System ",St cloud State University, St. Cloud, MN 56301
[3] Leonardo Sobrado and Jean Camille Birget "Graphical passwords ",The Rutgers Scholar, Electronic journal, Rutgers University, Camden New Jersey, 2002.
[4] IanJermyn , AlainMayer, FabianMonrose and MichaelK.Reiter, "Design and Analysis of Graphical Passwords" , Proceedings of the 8th USENIX security symposium, August 23-26 ,1999
[5] M. Mathuri Pandi and Valarmathi "A Secured Graphical Password Authentication System ", International Journal of Engineering Research &Technology, Vol 2,issue 5, May 2013.
[6] Wayne Jansen et al, "Picture Password: A Visual Login Technique for Mobile Devices", NIST, July 2003.
[7] Sacha Brostoff and M. Angela Sasse , "Are Passfaces More Usable Than Passwords? A Field Trial Investigation", Department of Computer Science, University College London, 2000.
[8] Susan Wiedenbeck et al, " Authentication Using Graphical Passwords: Basic Results" , Drexel University, Philadelphia, PA, USA.
[9] Varenhorst .C, "Passdoodles: A lightweight authentication method", Research Science Institute, 2004
[10] Vajna et al, "A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping" , IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol.22,No.11, November 2000.
[11] Jae-Jung Kim and Seng Phil Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems, Vol.7, No.1, March 2011.