GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION

Himika Parmar[1], Nancy Nainan[2] and Sumaiya Thaseen[3]

[1]School of Information Technology and Engineering,
VIT University, Vellore, India
himika.parmar@gmail.com
[2]School of Information Technology and Engineering,
VIT University, Vellore, India
nanzyn18@gmail.com
[3]School of Computing Science and Engineering,
VIT University, Chennai, India
sumaiyathaseen@gmail.com

ABSTRACT

Phishing, a serious security threat to Internet users is an e-mail fraud in which the perpetrator sends out an email which looks like legitimate, in an order to gather personal and financial information of the receiver. It is important to prevent such phishing attacks. One of the ways to prevent the password theft is to avoid using passwords and to authenticate a user without a text password. In this paper, we are proposing an authentication service that is image based and which eliminates the need for text passwords. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after image authentication. This OTP then can be used by user to access their personal accounts. The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. This paper integrates Image based authentication and HMAC based one time password to achieve high level of security in authenticating the user over the internet. These algorithms are very economical to implement provided they are time synchronized with the user.

KEYWORDS

IBA (Image Based Authentication), OTP (One Time Password), SHA-1(Secure Hash Algorithm)

1. INTRODUCTION

Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures. There are mainly two types of password

Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,
pp. 195–206, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2417

- Static password
- Dynamic Password

Static password is the traditional password which is usually changed only when it is necessary: it is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. Static passwords are highly susceptible to cracking, because passwords used will get cached on the hard drives.

To solve this we developed One Time Password Token. Unlike a static password, dynamic password is a password which changes every time the user logs in. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker. This reduces the vulnerability of the hacker sniffing network traffic, retrieving a password, and to successfully authenticate as an authorized user. This password is used only for that session and when the user logins next time, another password is generated dynamically.

Image based authentication is included to provide additional security integrated with OTP. With IBA, when the user performs first time registration on a website, he makes a choice of several secret categories of images that are easy to remember, such as pictures of natural scenery, automobiles. Every time the user logs in, a grid of randomly generated images is presented to the user. The user identifies images that were previously selected. One-time access code is generated by the selected images, making the authentication process more secure than using only a static text password. It's significantly easier and advantageous for the user because he has to remember only a few categories to recognize the selected images.

The proposed work consists of the following steps: -The user will be asked to enter his user name, previously selected images (for authentication) and his email. An OTP will be generated following the submission and will be sent to the email id. The user has to enter the particular OTP communicated through mail. If OTP get verified then he will be directed to the home page.

1.1. Different Techniques Involved in Authentication

Current authentication methods can be classified as follows:
• Token based authentication
• Biometric based authentication
• Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan and facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further sub divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user is authenticated by recognizing and identifying the images he or she selected during the registration stage. Using

recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

1.2. Different Techniques Involved in Generation of One Time Password

One time password can be generated in any of the two ways:

- Time-synchronized OTP: In time-synchronized OTPs the user should enter the password within a certain period of time else it gets expired and another OTP must be generated.
- A counter-synchronized OTP: With counter-synchronized OTPs, a counter is synchronized between the client device and the server. The device counter is advanced each time an OTP is requested.

For example, consider hash-based OTPs wherein we use hash algorithms such as SHA-1 and MD5 that can be used to compute the OTP. A cryptographic hash function also called one-way function maps message of arbitrary length to a fixed-length digest. Thus, a hash-based OTP starts with the input parameters (synchronization value, username, password), runs them through the cryptographic hash function, and produces the fixed-length password, i.e., OTP.

1.3. Modes of OTP Delivery

- Text messaging: It is the common method used for the delivery of OTP.
- Instant Message Services and Email: These services are almost common and the cost of using them is negligible.

2. RELATED WORK

2.1. Recognition Based Techniques

Dhamija and Perrig [12] proposed a graphical authentication scheme based on the Hash Visualization technique [13].In this technique, the user is asked to select a certain number of images from a set of random pictures generated by a program. Then the user will be authenticated by means of identifying the preselected images. This technique fails to impress because the server has to store the seeds of the portfolio images of each user in plain text.

Akula and Devisetty's algorithm [14] is similar to the technique proposed by Dhamija and Perrig [12]. The difference is that by using hash algorithm SHA-1, which produces a 20 byte output, the authentication is more secure and requires less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDAs.

Weinshall and Kirkpatrick [15] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. This study revealed that pictures are the most effective among the three schemes discussed. Pseudo codes can also be used as an alternative but require proper setting and training.

Jansen et al. [16-18] proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is less. Each thumbnail image is

assigned a numerical value, and the sequence of selection will generate a numerical password. The result depicted that the image sequence length is generally shorter than the textual password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication [19]. The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program authorizes a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their password images. This technique is a secure authentication method in comparison with text-based passwords. Allowing users to use their own pictures would make the password even more predictable, especially if the attacker is familiar with the user.

2.2. Products Using One-Time Password Technology

Table 1. Name of Products

Product	*Description*
ActivIdentity Strong Authentication Solutions	Multifactor Authentication via smartcards, USB Tokens, One-Time password tokens, soft tokens, and Biometrics
MXI Security Stealth MXP	A line of portable devices designed to provide multiple levels of authentication and data protection
RSA Security Secure ID	A Well known-and widely used technology that uses time based OTP to generate unique passwords
VeriSign Unified Authentication Tokens	A variety of tokens that provides both OTP functionality and storage of digital certificates

3. PROPOSED SOLUTION

The proposed solution involves two methods: image based authentication and an OTP generation method.

- Image Based Password Authentication
- HMAC-Based One-Time Password

3.1. Image Based Authentication

The Image-based authentication is based on Recognition Techniques. When the user registers for first time in a web site they select set of images that are easy to remember, such as natural scenery, automobiles etc. Every time the user logs into the site, they are provided with a grid of images that is randomly generated. The user can identify the images that were previously selected

by him. It is significantly easier for the user because they need to remember a few simple images only.

IBA is based on a user's successful identification of his set of images. When the user logins for the first time, the website displays a grid of images, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images. Performing brute force attacks or other attacks on such systems is very difficult. A set of different images are selected to authenticate the user. The Image Identification Set (IIS), for each user is then stored at the Authentication System. When a user logins, the IIS for that user is retrieved and used to authenticate that particular user. The system does not store the images but the category of the images are stored in IIS as images are large files. This technique is also more secure and requires less memory. If this step is successful, next OTP is generated and send to the user email-id.

3.2. HMAC-Based One-Time Password Algorithm

This paper describes an algorithm which is used to generate Time-synchronized OTP values, based on SHA-1 based Hash Message Authentication Code (HMAC). This is called as the HMAC-Based One-Time Password because here OTP is generated based on HMAC. One-Time Password is obviously one of the easiest and most popular forms of two-factor authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as a secure and stronger forms of authentication, and allowing them to installed across multiple machines including home computers, mobile phones etc.

When the user selects the pre-selected images to login an OTP is generated and sent to the user's e-mail id. The user is then directed to next page where the user is asked to enter the OTP. The user gets the OTP using the e-mail account and enters it. If the OTP is verified the user succeeds in logging in the system.

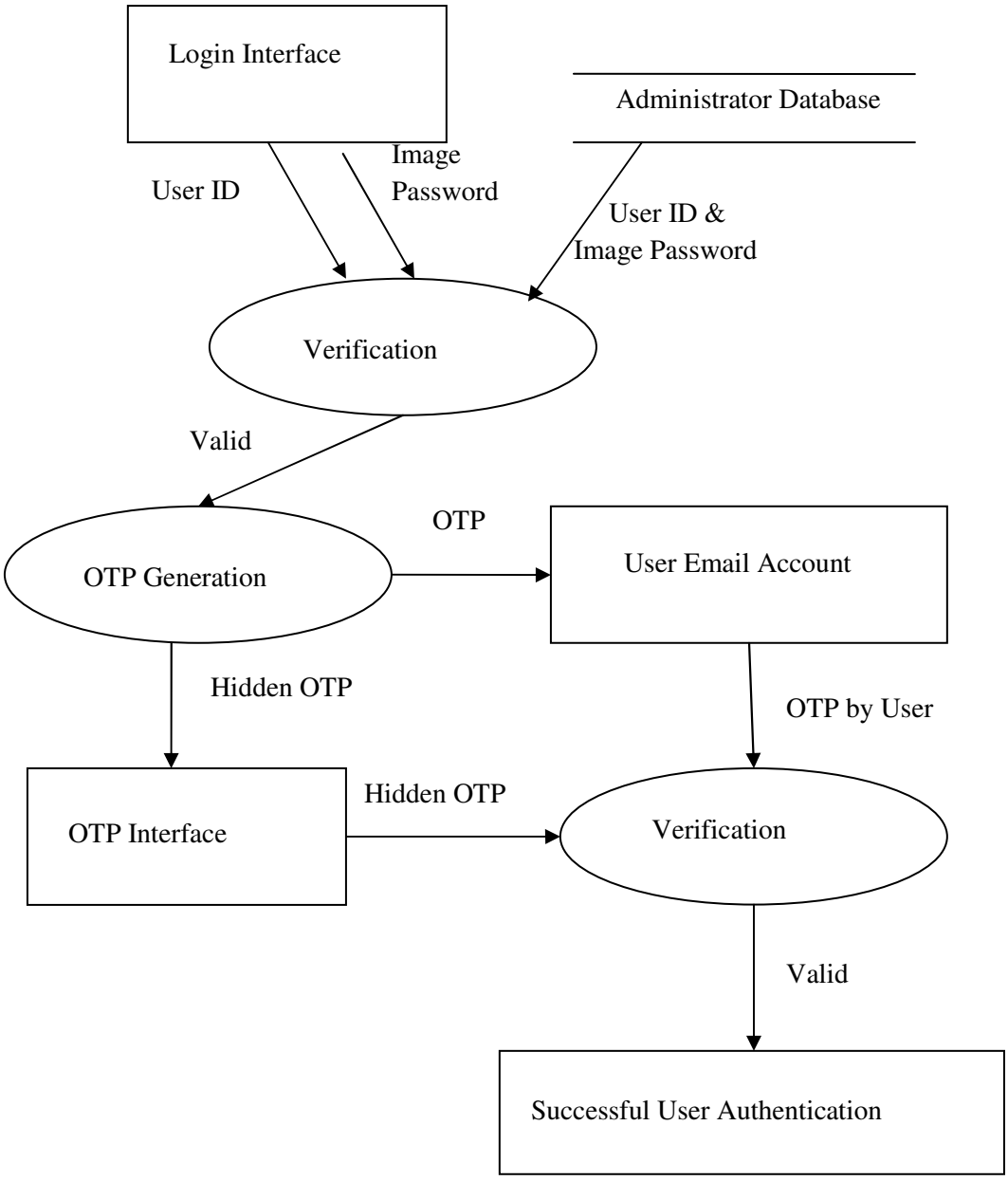

Figure 1. Data Flow Diagram

3.3 Algorithm Requirements

A - The algorithm MUST be time synchronized.
B - The algorithm SHOULD be economical to implement by reducing the amount of hardware required.
C - The algorithm MUST work with any sort of code generating tokens.

D - The value displayed on the token or any mail message should be easy to read and entered by the user. For this the OTP value should be of reasonable length such as a 8-digit value. It is desirable for the OTP value to be a numeric digit so that it can be easily entered.
E - User-friendly mechanisms should be available to resynchronize the time.

3.3.1.Algorithm

The notations used in OTP algorithm

Symbol	Represents
T	It is the Time value, the changing Factor.
Key	Shared secret between client and server, i.e. Username and Image Based Password.
Digit	Number of digits in an HOTP value.

3.3.1.1Description

The OTP algorithms are based on an increasing time value function and a static symmetric key known only to client and server. In order to create the OTP value, a HMAC- SHA-1 algorithm is used. Since the output of the HMAC-SHA-1 calculation is 160 bits, we have to truncate this value to a smaller digit so that it can be easily entered.

OTP (Key,T) = Truncate(ToHex(HMAC-SHA-1(Key,T)))
Where –Truncate converts the value generated through HMAC-SHA-1to an OTP value.

3.4. Generation of OTP Value

The algorithm can be described in 3 steps:

Step 1: Generate the HMAC-SHA-1 value Let HMK = HMAC-SHA-1(Key, T) // HMK is a 20-byte string
Step 2: Generate a hex code of the HMK.
HexHMK=ToHex (HMK)
Step 3: Extract the 8-digit OTP value from the string
OTP = Truncate (HexHMK)
The Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

3.5 Operation

```
MessageDigest md = MessageDigest("SHA1")
md.update(Key,T)
output = md.digest()
buf = hexDigit((output >> 4) & 0x0f)
otp=buf.toString()
otp=otp.substring(0,7)
```

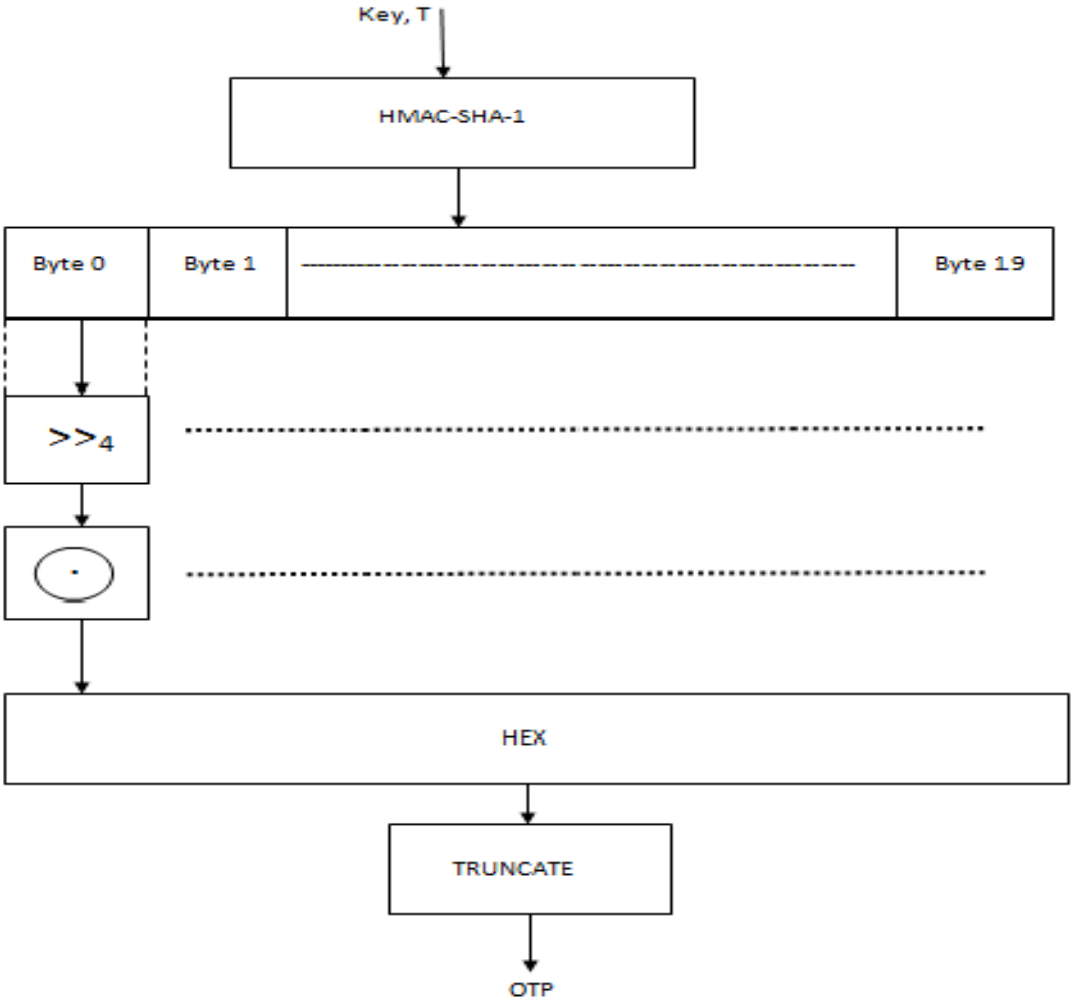

Figure 2. Operation of HMAC-SHA-1

3.6 APPLICATIONS

Google is currently using one time password. Hotmail is also using one time password to provide high security to users. RBI made OTP compulsory for transaction made with credit card. All banking systems are using OTP. E.g.:- ICICI Bank, HDFC, Citi Bank, Axis, SBI etc.

4. SCREENSHOTS

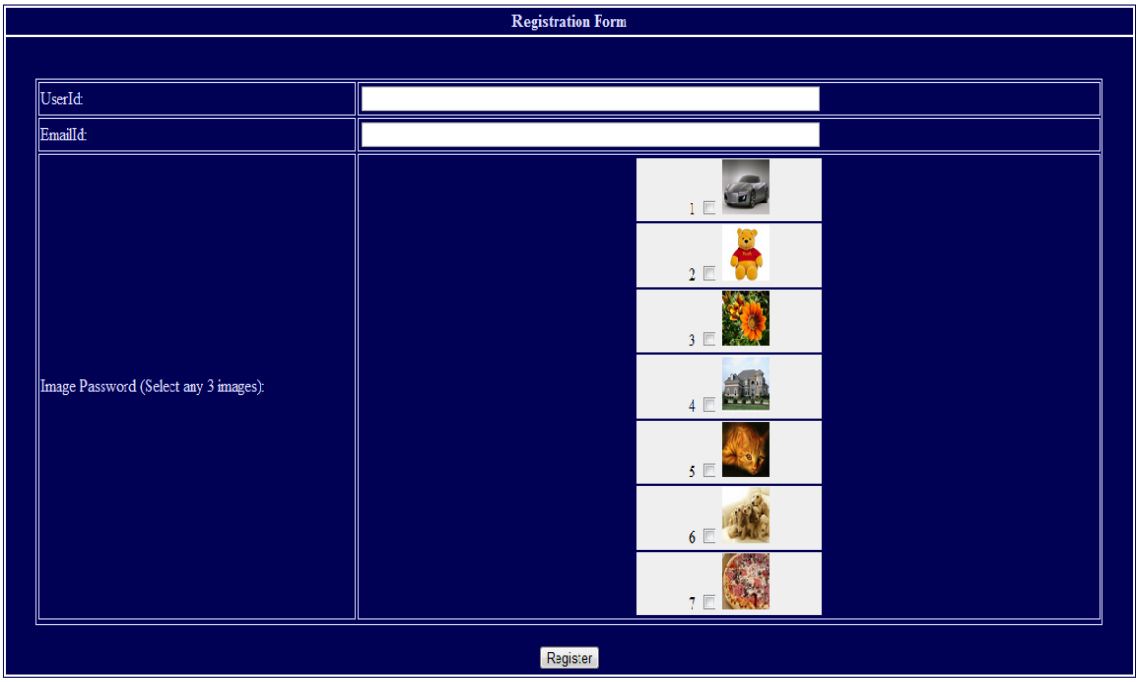

Figure 3 : Registration Form

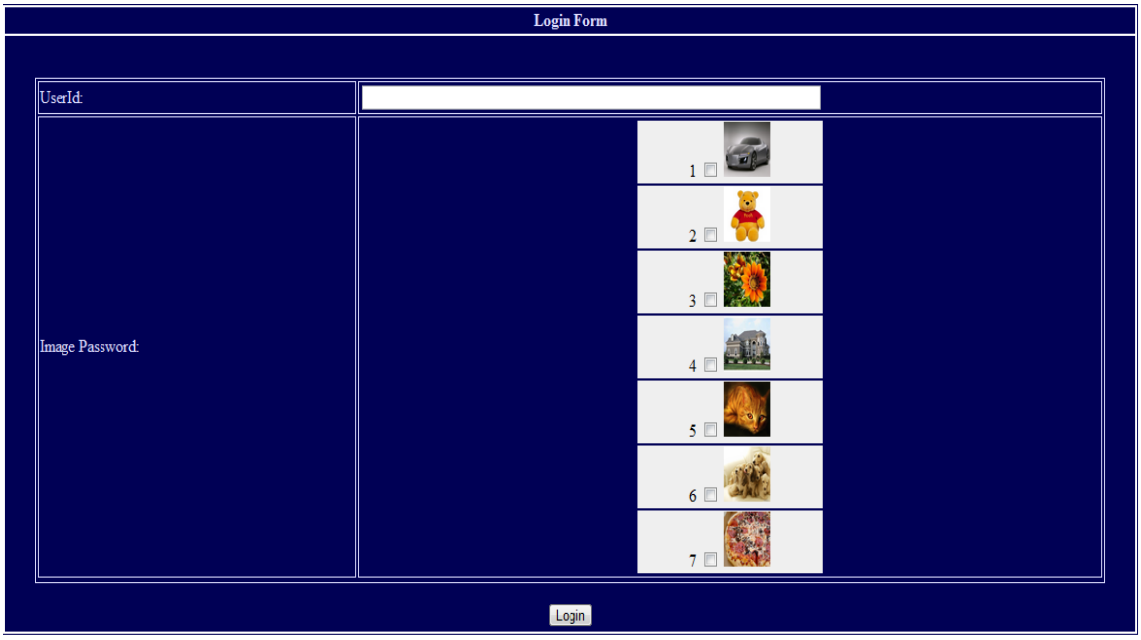

Figure 4. Login Form

Figure 5. OTP Form

Figure 6. Home Page

5. CONCLUSION

The proposed system integrates the security techniques Image Based Password Authentication and Hash-MAC based one time password. Initially, the Image Based Password Authentication is done where user is authenticated using image password that was previously selected by the user himself, followed by the Hash - MAC based One Time Password which uses SHA-1 algorithm for the generation of a secure one time password. This authentication technique is simple and highly secure. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function and in this paper SHA-1 is used for the calculation of HMAC. SHA-1 being a most widely accepted cryptographic hash function due to its high security

as compared to other cryptographic hash functions such as MD5 adds to the security of HMAC. Recovery of lost password based on secret question and answers can be a future enhancement.

REFERENCES

[1] D. M'Raihi, M. Bellare, F. Hoornaert, and D. Naccache, "HOTP: An HMAC based one-time password algorithm, RFC 4226", Dec. 2005.

[2] Nitin ,Durg Singh Chuhan, Vivek Kumar Sehgal, Ankit Mahanot," Security Analysis and Implementation of *JUIT–Image Based Authentication System using Kerberos Protocol", Seventh IEEE/ACIS International Conference on Computer and Information Science, pp. 575-580

[3] Balkis Hamdane , Ahmed Serhrouchni, Adrien Montfaucon, Sihem Guemara." Using the HMAC-Based One-Time Password Algorithm for TLS Authentication" 978-1-4577-0737-7/11/ ©2011 IEEE

[4] Srinath Akula, Veerabhadram Devisetty ,"Image Based Registration and Authentication System",Department of Computer Science,aksr0201@stcloudstate.edu, deve0301@stcloudstate.edu

[5] Chun-Ying Huang, Shang-PinMaa, Kuan-TaChen," Using one-time passwords to prevent password phishing attacks" Journal of Network and Computer Applications 34 (2011) 1292–1301, pp.1292-1300

[6] Richard E. Newman, Piyush Harsh, and Prashant Jayaraman,"Security analysis of and proposal for image-based authentication",CISE Dept., University of Florida, Gainesville FL 32611-6120{nemo, pharsh, pjayaram}@cise.ufl.edu

[7] Confident Technologies, Inc. Delivers Image-Based Authentication and Verification Solutions for Consumer-Facing Web Applications, http://www.confidenttechnologies.com/

[8] ActivIdentity Strong Authentication Solutions, http://www.actividentity.com/

[9] Mastering Java Security (Cryptography, Algorithms & Architecture) by Rich Helton & Johennie Helton (Wiley/ Dream Tech)

[10] MXI Security Stealth MXP, http://www.Processor.com/MXI

[11] RSA Security SecurID**,** http://www.rsasecurity.com

[12] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[13] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.

[14] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.

[15] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[16] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in *Data Security*, 2004.

[17] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[18] W. A. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[19] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[20] VeriSign Unified Authentication Tokens, http://www.Processor.com/Veri

Authors

[1] Himika Parmar received the B.E. degree in Computer Science and Engineering in 2008 from Pt. Ravishankar Shukla University, Raipur, and pursuing M-tech in IT (Networking) from the VIT University of Vellore, India. Her areas of interests are ad hoc wireless networks and network security.

[2] Nancy Nainan received the B.E. degree in Computer Science and Engineering in 2011 from Mahatma Gandhi University, Kerala and pursuing M-tech in IT (Networking) from VIT University of Vellore, India. Her areas of interest are Computer networks, Cryptography and Network Security.

[3] Sumaiya Thaseen received her B.E. degree from Madras University and M.Tech from VIT University in 2004 and 2006 respectively. She is currently an Assistant Professor(Senior) in School of Computing Science and Engineering, VIT University, Chennai with 6 years of experience and also pursuing her PhD degree. A life member of Computer Society of India (CSI). Her areas of interests are ad hoc networks,Cryptography and network security. She has published several papers in international peer reviewed journals and conferences.