International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Image Based One Time Password

Neha Vishwakarma[1], Kopal Gangrade[2]

[1]Computer Science Department, Rajiv Gandhi Technical University, Student, Shri Ram Institute of Technology Jabalpur, India

[1]Computer Science Department, Rajiv Gandhi Technical University, Shri Ram Institute of Technology Jabalpur, India

Abstract: ***Most people now access all the important areas of their life—banking, shopping, insurance, medical records, and so on—simply by sitting at their computer and typing a username and password into a website. Getting access to something this way is called one-factor authentication, because you need to know only one thing to get into the system: the combination of user name and password. In theory, this kind of protection should be reasonably secure; in practice, it's less and less trustworthy. This paper presents an approach to further increase security using a two-factor authentication scheme. This approach required the user to login with a username and password and also generate a One Time Password which will be sent to his email. The One Time Password will be used for authentication any time the user wishes to access a restricted resource. The one time password as the name implies will expire after a single use and after a period of 60 seconds. The system uses random image and text based OTP generation with SHA-512 algorithm and again encryption by using ECC to develop a more secured two factor, one time password. Java Enterprise Edition (JEE) technology was used.***

Keywords: One Time Password (OTP), Image Based OTP, SHA based One Time Password, Time-based One Time Password (TOPT), Cryptography, Email, Authentication.

1. Introduction

Private and sensitive information about everyday life is becoming more and more stored and passed across on the internet. People can now access such important data about all areas of their life — banking, shopping, insurance, medical records, and so on— simply by sitting at their computer and typing a username and password into a website. 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

- 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 [1].Image based OTP generation generates more secure OTP. Proposed work involves generation of image & text based OTP with randomized selection and multiple encryptions using HMAC & ECC.

2. Related Work

Authentication Systems based on one-time passwords are more secure than one is that rely on reusable passwords. For example, remote access usually requires the user to enter a password or pass phrase. This secret usually travels across insecure network in the clear. In the case of one-time passwords, the danger of eavesdropping is eliminated because once a password is used, it is no longer useful. If a one-time password system is implemented properly, breaking it requires sophisticated, active attacks that are beyond the abilities of most attackers, such as play in the middle attacks[3]. Time-synchronized OTPs are widely deployed but are subject to problems caused by clock skew. 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[3].Dhamija and Perrig [5] proposed a graphical authentication scheme based on the Hash Visualization technique [6].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 [7] is similar to the technique proposed by Dhamija and Perrig [8]. 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 [9] 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. [10-11] 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 [12]. 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.Multi-factor Authentication is a method of computer access control which a user can pass successfully presenting various authentication stages. In this, instead of asking just single piece of information like passwords, users are asked to give some additional information which makes it more difficult for any intruder to fake the identity of the actual user. This additional information can include various factors likefinger prints, biometric authentication, security tokens etc. It has emerged an alternative way to improve the security by requiring the user to provide with more than one authentication factor rather than only a single password [4].

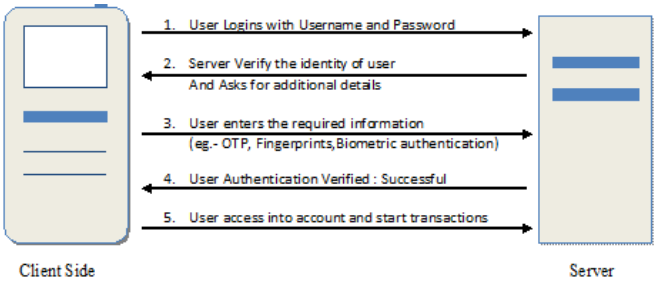

Figure 1: Multistep Authentication Process

3. Generation of Image Based OTP

The Image-based Authentication is based on Recognition Technique. It is almost similar to text one time passwords as in this also the user is provided a shared secret as an evidence of his/her identity. However, text-based OTPs use alphanumeric characters to represent the secret and IBA uses visual information. When the user registers for the first time on the website, they are required to select a set of four images randomly from predefined large set of images such as natural scenery, automobiles etc [8]. Every time a user login into the website or service, they are provided a user id and password. After first authentication our system generates OTP using one of image selected at the time of registration with sha-512 encryption along with randomly selected text fields given at the time of registration. Than system select first 8 characters of cipher text and encrypt it with ecc . Than produced OTP will be sent to users email. When user enters OTP for validation again it will be decrypted using ecc and matched for authentication.

Our proposed model contains three stages:
3.1 User Registration
3.2 OTP Generation
3.3 OTP Authentication

3.1 User Registration

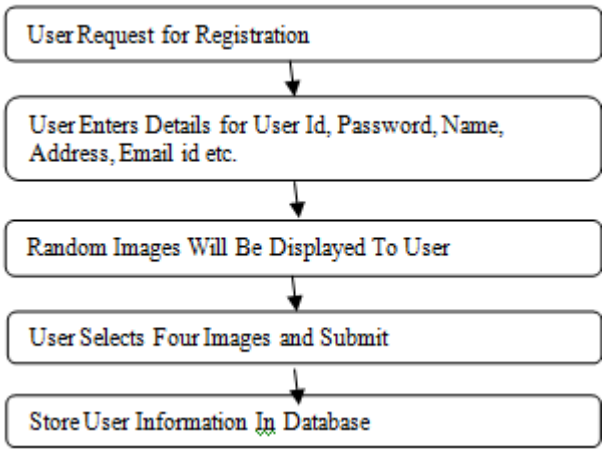

Figure 2: Registration Process

3.2 OTP Generation

The system is based on a synchronous stream cipher that uses images, instead of passwords, as the secret key. A synchronous stream cipher is a type of symmetric key algorithm that generates a pseudo-random sequence of bits, called the key stream, independent of the plaintext and cipher text. These bits are then combined with the plaintext bits (usually using exclusive-or) to produce the ciphertext, and then we select first eight character and again encrypted by ECC method to produced encrypted OTP. That will be send to users email id. Selection of images and text fields are random so it will be more secure.

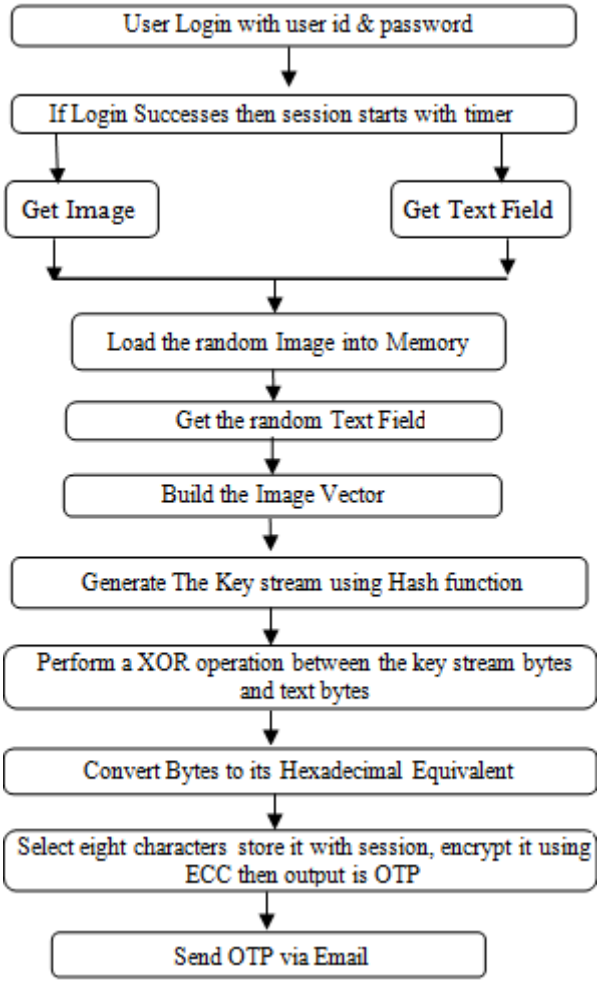

Figure 3: OTP Generation

3.3 OTP Authentication

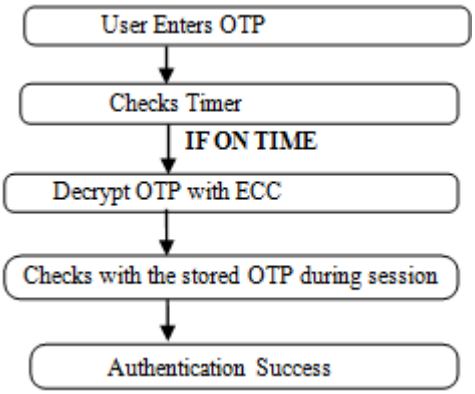

Figure 4: OTP Authentication

4. Result

The proposed system has been evaluated on two main parameters
1) OTP Generation Time
2) Key stream Generation Time

For evaluating different algorithm we have taken three samples with fixed image and fixed text field. Experimental parameters are represented below in terms of table and chart for each sample.

Table and chart below represents comparison of OTP generation time for all samples:

Table 1: Comparison of all Samples

Algorithm	*OTP Generation Time (ms) Sample 1*	*OTP Generation Time (ms) Sample 2*	*OTP Generation Time (ms) Sample 3*
SHA 128	81	89	83
SHA 256	42	43	48
SHA 512	39	37	36

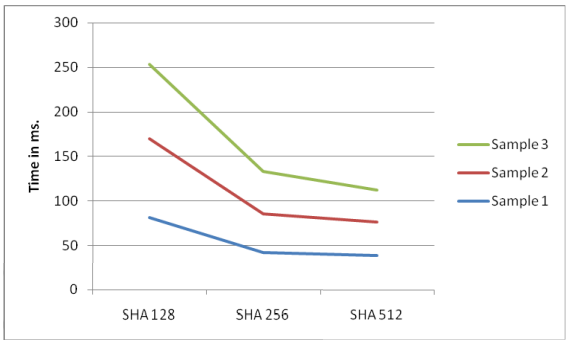

Figure 5: Comparison Chart for All OTP Sample

Table and chart below represents comparison of key stream generation time for all samples:

Table 2: Comparison of All Key stream Generation Sample

Algorithm	*Key Stream Generation Time (ms) Sample 1*	*Key Stream Generation Time (ms) Sample 2*	*Key Stream Generation Time (ms) Sample 3*
SHA 128	58	67	65
SHA 256	23	22	27
SHA 512	20	19	18

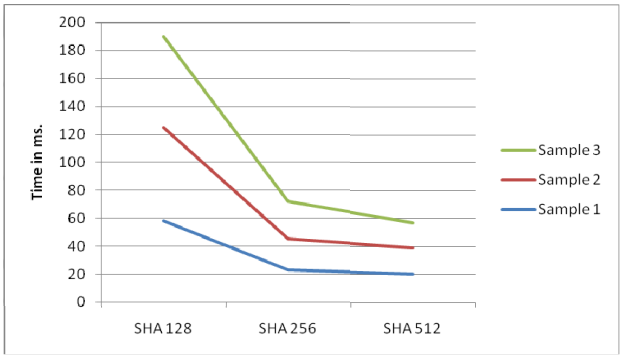

Figure 6: Comparison Chart for Key stream Generation

5. Conclusion

Today, we do many of our banking and shopping transactions by a simple click of mouse. While this means a lot of comfort, convenience and cost savings to us, it also exposes us to new age risk like phishing and other attacks. Today, OTPs are commonly used for authentication and authorization for many different applications.

Through this research paper we are presenting an image based time synchronized OTP generation method using SHA 512 & ECC to counter man in the middle attack in order to secure our applications. This work is more secure than using

other encryption methods according to literature survey. We are developing the system using Java.

References

[1] Himika Parma, Nancy Nainan and Sumaiya Thaseen, "Generation Of Secure One-Time Password Based On Image Authentication," *Cs & It-Cscp 2012*.
[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] K.Aravindhan, R.R.Karthiga, "One-time Password: A Survey", International Journal of Emerging Trends in Engineering and Development Issue 3, Vol.1 (January 2013)
[4] Navpreet Kaur, Mandeep Devgan, "A Comparative Analysis of Various Multistep Login Authentications Mechanisms", International Journal of Computer Applications (0975 – 8887) Volume 127 – No.9, October 2015
[5] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[6] 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.
[7] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.
[8] 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.
[9] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.
[10] 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.
[11] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.
[12] 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.

Author Profile

Neha Vishwakarma pursuing M.E. (CSE Branch) degree from Shri Ram Institute of Technology Jabalpur (Rajiv Gandhi Technical University Bhopal M.P.).Completed B.E.(Information Technology Branch)from SRIT in 2005.