An Enhanced Method of OTP Generation Using Image Encoded Method

Shweta Gupta[1], Amit Ranjan[2]
[1]Dept of CSE
[2] Assistant Professor Dept of CSE
[1, 2] Shri Ram Institute of Science & Technology Jabalpur, Madhya Pradesh, India

Abstract- *Now a day's security is a big concern in every field of web applications, like money transaction, mail transfer, document sending etc. So for providing security the authentication is done at the time of the transaction. The authentication is done by the OTP for providing more security. This paper attempts to provide authentication by image encoded OTP. Two types of OTP's used, symbolic and numeric, and both OTP's are image based encoded, used for providing more security. In proposed work, random image is used to select symbol and for generating the OTP and the virtual keyboard is given to input the OTP. The Image Based Password System (IBPS) approach is used for OTP generation. One Time Password (OTP) is typically generated by a token possessed by the user and it is the input to the authentication system. The input OTP is compared to an OTP generated by the system. If it matches, the user is allowed to access the system.*

Keywords- Authentication, Graphical password, One Time Password, Security.

I. INTRODUCTION

Internet security is recently becoming an important issue with the increasingly wide range of Internet applications. However, since the Internet is an open network, it is weak to various attacks such as system intrusion and tapping, etc. User authentication is a necessary security element in the open network environment. An authentication method that creates one time new password each time was normally used for Internet banking. OTP is first security medium for stability strengthening of electron financial transaction. Image based OTP generation generates more secure OTP. The Image-based Authentication is based on Recognition Technique. The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. 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.

1.1 Authentication

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. [2] Main area of information security is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method.

[3] Authentication is defined as the verification of the "identity of a user, process, or device, often as a prerequisite to allow access to resources in an information system" Authentication is a component of Information Assurance (IA), confidentiality, integrity, and availability .CIA triad which constitutes the core principles of information security.

Authentication can be considered to be of three types:

- Password Authentication
- Smart Card Authentication
- Biometric Authentication

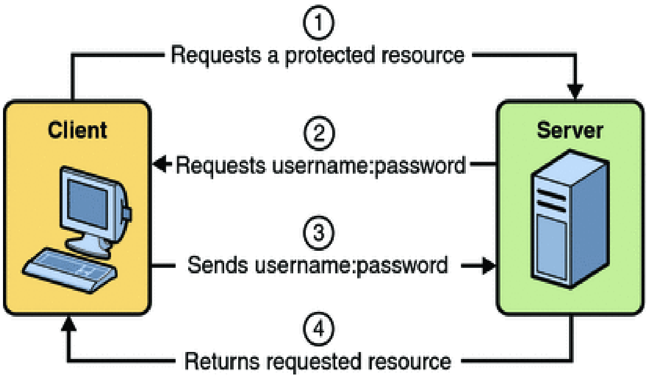

1
Requests a protected resource
Client
2
Requests username:password
Server
3
Sends username:password
4
Returns requested resource

Figure 1: Authentication Process

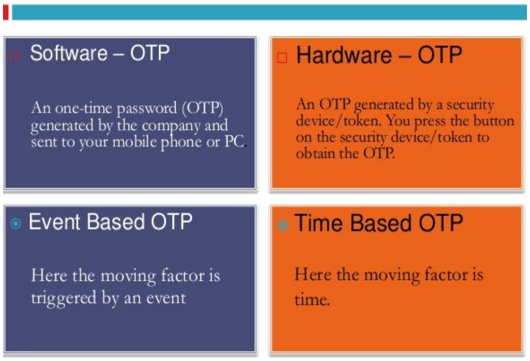
1.2. OTP

[4] A one-time password (OTP) is a password that is valid for only one login session or transaction. [5] One time password (OTP) systems provide a mechanism for logging on to a network or a service using a unique password which can be used only once, as the name suggest. This prevents some forms of identity theft by making sure that captured username/password cannot be used second time. Typically

user logon name stays same, and one time password changes with each login. One time passwords are a form of so-called strong authentication, provides much improved protection to on-line banking accounts, corporate networks and other systems containing sensitive data.

OTP generation algorithms typically make use of pseudo-randomness or true-randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Various approaches for the generation of OTPs are listed below:

- Time based OTP
- Event based OTP



Software – OTP

An one-time password (OTP) generated by the company and sent to your mobile phone or PC.

Hardware – OTP

An OTP generated by a security device/token. You press the button on the security device/token to obtain the OTP.

Event Based OTP

Here the moving factor is triggered by an event

Time Based OTP

Here the moving factor is time.

Figure 2: Types of OTP

[5] Three factor authentication is another attractive strategy. It is a method of computer access control in which user is granted access after successfully presenting several pieces of evidence to an authentication mechanism; of following categories: knowledge (something user know); possession (something user have), and inherence (something users are).For authentication procedure, the user must enter a password and input a pass code generated by the token, and scan the biometric features. Two factor authentication is more eye-catching and convenient than three-factor authentication. Two factor authentication is an authentication procedure in which user has to provide two means of identification from different categories; first is a personal token, such as a card, and second is the memorized security code.

II. RELATED WORK

In [4] authors proposed approach is, after user entering the username and password web server generates the Encrypted OTP using AES algorithm and send it to the users mobile. OTP is an encrypted format, so users can't read it. Instead of that, user needs to forward that OTP with system logging password to the system. At the system end encrypted OTP is decrypted and verify the OTP, Password and mobile number for a particular username.in this approach user's information are verified in many levels. It avoids the unauthorized logging.

In [1], authors, proposing an approach Image Based Password System (IBPS) which generates an OTP based on the image selected by the user. In this work, random numbers are generated from extracted features of image, used as OTP which forms a strong factor for authentication. Image based password system (IBPS) depicts how One time password is generated by using the features of images which is used for authentication process. IBPS shows generation of numerous OTP's from a single image and is highly secure compared to the conventional methods. A registered user is supposed to provide user-id, pin number for doing online transaction like credit/debit card operations during authentication. After verification on server, IBPS displays a set of images where the registered user has to select an image of his/her choice. IBPS accepts the selected image entered by the registered user and uses the extracted features of image in generation of One Time password. Now this generated One-Time password is passed to the registered user mobile number. This OTP is to be entered for successful completion of authentication process.

In [6] authors used an enhanced type of physical security method is proposed which is authentication using Random Number Generated (RNG) Keypad based on One Time Pad Concept. It is a computational physical device designed to generate a sequence of numbers or symbols that will appear randomly using Pseudo-random numbers algorithm each time One Time Password (OTP) is keyed in. It is typically generated by a token possessed by the user and it is the input to the authentication system.

In [7] authors describes a scheme which allows strengthening the authentication process in the cloud environment using the password generator module by means of a combination of different techniques such as multi-factor authentication, One-time password and SHA1.

In [8] authors introduce an E-payment system that provides an unrivalled security using visual and quantum cryptography. Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one time password .Image steganography embeds the share with one time password which results in secure transmission of share to bank.

In [9] authors proposed the system in which OTP will be generated and encrypted using the Elliptic Curve Cryptography. The private and public key used for the encryption and decryption will be generated from the voice print provided by the user. The hash function is used to generate private key of the particular user.

In [10] authors introduced an efficient biometrics based user identification has been introduced. This includes the features such as palm print, finger print and iris for providing more accurate personal identifications. The proposed system is most suitable for personal identification and it needs high security during online purchasing, net banking etc.

III. CONCLUSION

Now a day's, many important and risky works related with personal information and also money are done over the internet. For these kind of work user authentication is done to provide security. The authentication is done by some related information like user id, password and One Time Password also. In this study, different methods of authentication and secure OTP generation like, encryption of OTP using AES algorithm, IBPS (Image Based Password System), Random Number Generated keypad, multi-factor authentication, Image steganography etc. are reviewed and surveyed. During our survey we get a new idea to generate One Time Password in two types, symbolic and numeric, by the random encrypted image and input the OTP by given runtime virtual keyboard, for enhancing the security of One Time Password.

REFERENCE

[1] KalyanapuSrinivas (2016), "A Novel Approach For Generation Of OTP'S Using Image's", Procedia Computer Science 85(2016) 511 – 518

[2] Saranya Ramanan, Bindhu J S (2014), "A Survey on Different Graphical Password Authentication Techniques" (ijircce)Vol. 2,Issue 12, 2014

[3] Jyoti I. Nandalwar, Viteshkumar Gaikwad, Shripad Kulkarni (2016), " A SURVEY AND COMPARISON ON USER AUTHENTICATION METHODS", (IJIERT-NITET-16), Paper ID: NITETCSE01

[4] Ms. E.Kalaikavitha, Mrs. Juliana gnanaselvi (2013), " Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology", (International Journal Of Engineering And Science) Vol.2, Issue 10 (April 2013), Pp 14-17

[5] Mirza Tanzila Maqsood1, Pooja Shinde2 (2016), "A Survey on One Time Password", (IJSR) Volume 5 Issue 3, March 2016, Paper ID: NOV161818

[6] HernyRamadhaniMohdHusny Hamid, NorhaizaYa Abdullah (2015), "Physical Authentication using Random Number Generated (RNG) Keypad based on One Time Pad (OTP) Concept"

[7] AbderrahimAbdellaouia,YounesIdrissiKhamlichib, HabibaChaouia (CMS 2016), "A Novel Strong Password Generator for Improving Cloud Authentication", Procedia Computer Science 85 (2016) 293 – 300

[8] Shemin P A (ICETEST - 2015), "E –PAYMENT SYSTEM USING VISUAL AND QUANTUM CRYPTOGRAPHY", Procedia Technology 24(2016) 1623 – 1628

[9] Komal K. Kumbhare (ICISP2015), "A Review on Noisy Password, Voiceprint Biometric and One-Time-Password", Procedia Computer Science 78 (2016) 382 – 386

[10] Malathi.R (CMS 2016), "An Integrated Approach of Physical Biometric Authentication System", Procedia Computer Science 85 (2016) 820 – 826.