ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Review on User Authentication Using One Time Password

Kaustubh Satpute, Mohan Pande

Assistant Professor, Dept. of CSE, DMIETR, Wardha, AVBIT, Wardha, India

ABSTRACT: In today's computer world network security is most important for user; due to the internet facility People is communicate openly with each other. The private data also available in network because of online communication. The security is given to data with standard procedures only requiring a simple username and password authentication it has become increasingly easy for hacker to gain access to a user's private data such as personal and financial details and then use that information to commit fraud or harm the person or company.

The security and privacy threats are always constantly growing. In this Paper the conventional login/password authentication is taken into account inadequately secure for several security-critical applications. Considerate more than one independent factor increases the difficulty of providing false credentials. Two level authentication proposals guarantee a higher protection level by extending the single authentication factor. We focus on the implementation of two level authentication methods by using both users friendly traditional Alphanumeric Password and One Time Password (OTP) or graphical password. With this we are providing the extra layer for the security check.

KEYWORDS: Data Security, One Time Password (OTP), Authentication, Verification

I. INTRODUCTION

Sharing of information or data over network has become a very common and important part of today’s communication world, Without sharing of knowledge or information the person or organization can’t survives in this fast growing technological world. Whenever we want to share the information with other user we make sure that the user is the legitimate user who accesses the information. Accessing information by the user is not legitimate user then it become harmful to the person or organization because this information used against the organization or person to affect the financial or damage the goodwill.

To verify the legitimate user most commonly used login password mechanism in this process centralize system create the user id and password for individual user with help of some personal information such as us name, date of birth, mobile no etc. using this login password credential user can access the information from anywhere at any time this process is called as single level of single factor authentication. Single level authentication process is not much effective because the hacker easily crack the login-password because of the similarity of the pattern and use of personal information to create the login password, or may be misuse by the family member or colleague who know the login-password.

The single level authentication is break because maximum time user selects the login password as name, date of birth, etc. because it easily remembers to them that’s why the login password easily compromised. To avoid this whenever the user can be authenticated always ask to the user for some addition info to conform the login user is the legitimate, this type called as two level authentication. In two level authentication process user authentication verify by two different identification the first one login password from existing system and second one is graphical password, hardware security key specially design for user authentication that carry by the users only, or use a special kind of code generated by the system & send only to the lawful user by email or SMS.

In this paper we are focus on the system generate unique code that delivered by email or SMS to user. This unique code is called as One Time Password (OTP). The process of sending the OTP through email is take some extra time due to availability of internet connection and opening the email account. The SMS is the better way to send OTP.

DOI: 10.15680/IJIRCCE.2016. 0405014

II. RELATED WORK

Communication is the important aspect in today's world because of the telecommunication system people easily interact & close with each other. Communication media also used for sharing of knowledge and information. Whenever the user share the information there is a chance to misuse the information. Before allow to access this we are verify the user authenticity.

Authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of the human or machine is validated, access isgranted.

Single Factor Authentication (SFA) is using only check the user id and password to authenticate the user.

Two Factor Authentication (TFA) is a mechanism which implements two of factors i.e. User id -password and security key that carry by the authenticated user. The security key may be hardware or a code that send to the user. Therefore TFA is more secure than the traditionally implemented one factor authentication [1]. In this system the hardware device is special design for authentication and may cost effective that's why the best solution is to generate the software base unique code that only know by the legitimated user.

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device [4].

III. PROPOSE SYSTEM

In this client server mechanism the centralize system contain user database and the application. When user want to access the information user request to the server the server receive the user request, server send response to user for login and password. After verifying the login password store in server database, it allows only those users which are already registering into the system. Login credential match then user is pass level one authentication & process for next level in the second level we use the OTP mechanism for that the OTP generation module is used it is unique 4-6 character code that can only be used once and is sent only to user registered mobile number. User will enter the correct OTP to complete the login process. In the verification process user OTP match then user can access the information from the application otherwise the request is discard by the server. The fig show the two level authentication process. Basically there are two modules first one is login module. In this database is connected to verify the user login details.

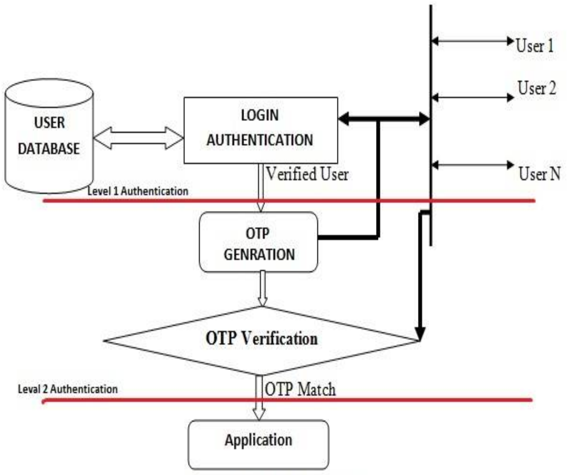

Fig.: Two Level Authentication process

The second module is OTP Generation and verification, OTP is Typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an hacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an hacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to calculate future OTPs by observing previous ones.

IV. CONCLUSION

In today computer word data security is more challenging for us to protect information from the attacker it is necessary to implement multi level authentication to secure the data or information.

In this paper we are trying to design a system to use two level authentications with the help of One Time Password.

REFERENCES

[1]FadiAloul, Syed Zahidi, Wassim El-Hajj. “Two Factor Authentication Using Mobile Phones”.
[2]Anders Moen Hagalisletto, Arne Riiber, “Using the mobile phone in two-factor authentication”.
[3] S. Vaithyasubramanian, A. Christy,D. Saravanan “TWO Factor Authentications For Secured Login In Support Of Effective Information Preservation and Network Security”
[4]https://en.wikipedia.org/wiki/One-time_password