IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 9, September 2016

An Enhanced Technique on Security System Using Multifactor Authentication

Tirupati Bala[1], Surinder Singh[2]

Research Scholar, Sachdeva Engg College for Girls, Gharuan, Mohali[1]

Department of Computer Science & Engineering, Sachdeva Engg College for Girls, Gharuan, Mohali[2]

Abstract: In the today's world with the remarkable development in computer system, single factor authentication, is no more examined as secure way to protect our confidential data. It is very simple and easy to guess passwords most often, they are short and based on subjects close to the user birthdays, partner names, children's names and they are typically only letters and can be found via the secret key gathering programs. Multifactor authentication guarantees a higher level of protection by extending the single authentication factor. Authentication is basically the process of verifying the identity of a user. Our proposed idea focuses on the implementation of multifactor authentication methods by using OTP password and image based Password and question based password as gateway for authentication. An attempt has been made to provide extra layers of security by adding additional passwords.

Keywords: Multifactor Authenticaction; Security; OTP (One Time Password); Graphical Password; Biometric based authentication.

I. INTRODUCTION

Today security is the main or important issue in every field. Likewise it is also important in the field of computer**.** Use of simple and easy to guess password in present time, invites the hackers, fraudsters itself to use your confidential data for wrong purpose. Hackers knew various techniques to steal your passwords so as to gain access to your login account. Multifactor verification is a security process in which confirmation of more than one password is executed to confirm the authenticity.

Multifactor authentication is a system in which two or more different factors are integrated to be used to increase the security level [1]. It act as hindrance layer and make it more difficult for the unauthorized user to get to the target. The basic objective of multifactor authentication is to create a layer of protection and make it more difficult for an unauthorized person to access the confidential information. If first security level is cracked or broken by the attacker, the attacker still has more security levels to crack to enter the target. Multifactor approval is a system where in two or more methods are used as a piece of conjunction to approve. Using more than one method for security is very so often called "strong affirmation". In general the multifactor authentication method demands various procedures to test the request of the user [7].

II. EXISTING METHOD

Authentication is the use of one or more mechanisms which confirms that you are the authorized user. If the identity of the human or machine is validated, access is granted and if the identity of the user is not validated he or she cannot access the information. Today Security is the main issue all over the world. New methods are developed one after another for the providing the security. The most common methods which are used all over the world are (i) Alphanumeric passwords, Graphical Password (ii) ATM card or tokens and (iii) Biometrics authentication like Finger print, Thumb Impression, Iris recognition, heart beat [6].

Biometric-based authentication is relatively very expensive as compared to the other ways of authentication. Alternative to common mode of authentication are developing for providing the better ways of security [3, 2, 4]. To reduce the risk that the private or confidential data can be used by somebody else One Time Passwords (OTP) offers a best alternative for multi factor authentication systems. In this paper we are proposing a new method in which we are going to add one more feature to the two factor authentication. We are combining or integrating the three techniques i.e one time password, image based authentication and knowledge based authentication.

III. RELATED WORK

Himika Parmar, Nancy Nainan and Sumaiya Thaseen[5] they proposed an authentication service that is image based and eliminates the need for text passwords. Using the instant messaging service that is available in internet, user will get the One Time Password (OTP) after image authentication. By using this OTP user will access their personal accounts. The image based authentication method depends on the user's ability to recognize pre-chosen categories from multiple pictures. This paper combines the Image based authentication and HMAC which are based one time password to acquire high level of security in authenticating the user over the internet.

DOI 10.17148/IJARCCE.2016.5913

Dhamija and Perrig [9] proposed a graphical authentication system which is based on the Hash Visualization technique [10]. In this technique, the user is asked to select or choose a certain number of images from a set of different set of pictures generated by a program. Then the user will be authenticated by identifying the preselected images. This technique fails to impress because the server has to store the various portfolio images of each user in plain text.

Akula and Devisetty's algorithm [8] is same as the technique proposed by Dhamija and Perrig [9]. The difference is that by using hash algorithm SHA-1, it produces a 20 byte output by which authentication is more secure and requires less memory. The authors suggested a possible future improvement by increasing persistent storage and can be implemented over the Internet, cell phones and PDAs.

Lamport's method [11] is a one-time password authentication method and uses a one-way function, but this method has two practical difficulties: high hash overhead and the need of resetting the verifier.

IV. PROPOSED METHOD

Multifactor authentication method, equips customers with a cost effective way of providing flexible and strong authentication. However, fraud is still being done with Two-Factor authentication; it shows that it is not totally secured. The goal of computer security is to maintain the integrity and privacy of the information thus can be obtained by using this authentication technique. The various proposed factors used in this authentication method are:

i) One Time Password (OTP) Method
ii) Image based Authentication
iii) Knowledge Based Authentication

The process starts when the user tries to login into the system. As the user enters its username and password he will get an OTP (One Time Password). An OTP is a set of characters that can be used as a form of identity for one time only. Once the password is used, it cannot be used for any further authentication. The algorithm which is used to generate OTP is very simple and known as the Lamport's Algorithm. One-time password authentication method changes the verifier every time by sending the present verifier along with the next verifier. Not only the Lamport OTP scheme provides effective security for distributed client/service interactions, but it's also simple to comprehend and implement.

After getting the OTP, the next step is image based authentication in which there are multiple images and user have to choose pre-mentioned one from random set of multiple images. Every time when the user logs in they are provided with multiple images that are generated randomly. The user an easily identify the images that are previously selected by him. This technique is very simple for the user because there is only one task to be done by the user and the task is to remember the previously selected image. After the confirmation, next step is knowledge based authentication in which user have to answer the question from the pre-mentioned details. This technique will provide a high level of security to the user from the systems to the hand held devices such as mobile phones. The working of the proposed system is explained below with the help of diagram.

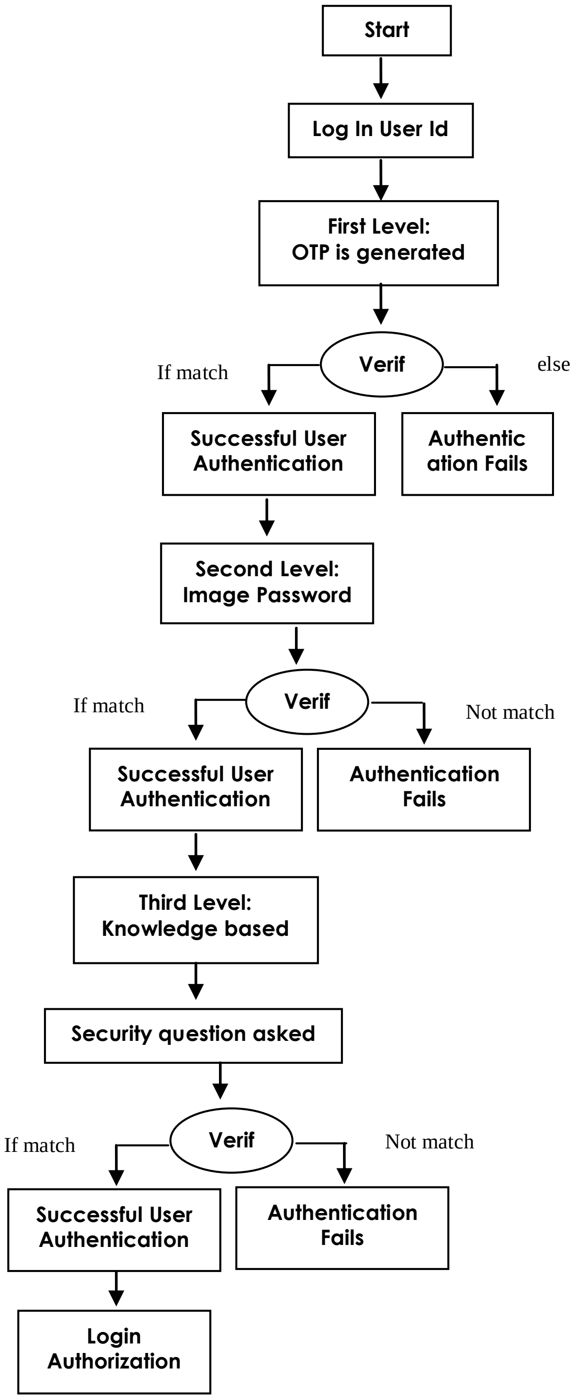

Fig.:-Working of the proposed work

DOI 10.17148/IJARCCE.2016.5913

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

V. FUTURE SCOPE

The future scope of project involves evolving a mechanism to enhance login security by adding additional biometric authentication mechanisms. With evolution of Smart Telephone more and more people tend to access the applications using their smart phone and these days smart phones have started coming with fingerprint scanners which can be incorporated into our application for enhanced security.

VI. CONCLUSION

The proposed system integrates the security techniques One Time Password, Image Based Password Authentication and Knowledge based Authentication. Using multi factor authentication mechanisms automatically enhances the security of the application to a great extent and makes the application almost hack proof.

REFERENCES

[1] S. Vaithyasubramanian, A. Christy and D.Saravanan, “Two Factor Authentication for secured login in support of effective information preservation and network security” Asian Research Publishing Network , VOL. 10, NO. 5, MARCH 2015

[2] S. Vaithyasubramanian, A. Christy “A Scheme to Create Secured Random Password Using Markov Chain” Advances in Intelligent Systems and Computing, Springer India, Vol. 325, pp. 809-814, 2015

[3] S. Vaithyasubramanian, A. Christy “A practice to create user friendly secured password using CFG” International Conference on Mathematics and Engineering Sciences, Chitkara University, Punjab, p. 39, March 2014

[4] Haichang Gao, Wei Jia, Fei Ye, Licheng Ma “A survey on the use of Graphical Passwords in Security”, Journal of software, Vol. 8, No. 7, July 2013

[5] Himika Parmar, Nancy Nainanand Sumaiya Thaseen “Generation of secure one-time password based on image authentication” pp. 195–206, 2012

[6] Sharifah Mumtazah Syed Ahmad, et al“Technical Issues and Challenges of Biometric Applications as access control tools of Information Security” International Journal of Innovative Computing, Information and Control Vol8, No. 11, pp 7983 - 7999 Nov 2012

[7] Alireza Pirayesh Sabzevar, Angelos Stavrou “Universal Multi-Factor Authentication Using Graphical Passwords”, Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems. pp. 625-632, 2008.

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

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

[10] 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

[11] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol.24, no.11, pp.770-772, 1981.

DOI 10.17148/IJARCCE.2016.5913