Implementation of Security System using Multifactor Authentication

Tirupati Bala
Research Scholar
Sachdeva Engg.
College for Girls
Gharuan (Mohali)

Surinder Singh
Department of computer
science & Engineering
Sachdeva Engg.
College for Girls Gharuan,
Mohali

ABSTRACT
As we know one factor authentication does not provide required security to a user while accessing the areas like banking, insurance, medical records etc. Users have to simply type a user name and password on the website So there is a need to increase the level of security for these users. This paper introduces an approach to increase the security level by using multifactor authentication scheme. This approach requires the user to login with a username and password. As the user enters his password, he will get the OTP generated by the system on his cell phone. We are integrating this approach with image based authentication and question based authentication. To develop this system we are using SHA algorithm and Lamport's algorithm. By using these algorithms we can develop more secured multifactor authentication. We are using visual studio as the front end and My SQL as the back end. The results show a more secured system.

Keywords
Multifactor Authenticaction; Security; OTP (One Time Password); Graphical Password; Knowledge based Authentication

1. INTRODUCTION
Every user is worried to store his/her personal information in such a way that it remains confidential and no one else can have access to it. Everyone is sharing their personalized data in different areas of life like shopping malls, insurance companies, banking, medical records etc. No one wants to go outside and stand for longtime in large queues so they simply use the online applications for their work. All they have to do is to enter a username and password sitting at one place. But there is more risk that the confidential data can be stolen by some unauthenticated person or by the malicious software. So it is necessary to authenticate the user by using some technique. If a user log in every time with the same password, his password can be easily cracked by using several methods including the keystroke logging programs that sit quietly on the system and remembering all the keys you press. To protect our data from the unauthorized persons we are using the multifactor authentication concept. Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories [3].

i. Knowledge factors ("things only the user knows"), such as passwords.

ii. possession factors ("things only the user has"), such as ATM cards.

iii. inherence factors ("things only the user is"), such as biometrics.

In 1981, Lamport proposed a One Time Password (OTP) authentication scheme using cryptographic hash functions. The purpose of an OTP is to make it more difficult to gain unauthorized access to restricted resources [8]. Therefore a user requires the new technique called One Time Password which is valid for only one login session. This is our first step of authentication. Now we are combining this approach with image based authentication and the Question based authentication or knowledge based authentication. An image based authentication eliminates the need for text passwords. This method depends on the user's ability to recognize pre-chosen picture from multiple pictures. And our last step is knowledge based authentication in which user has to answer the simple question according to his knowledge.

2. LITERATURE REVIEW
Akula and Devisetty's [2] According to Akula & Devisty that by using hash algorithm SHA-1, which gives 20 byte as output, the authentication is more secure and requires less amount of memory. The authors proposed a future improvement by providing unrelenting storage and this could be placed over the Internet, cell phones and Personal digital assistant.

Ankitet al [7] they proposed a user friendly three level security based on cued click points in an image. It is user-friendly and named as Three Level Security because it ensures its security through three levels. The three levels are Text based password, image based password and One Time Automated Password. If the image been clicked lies within the level of tolerance, next proper image is presented to the user. If not then the user is shown up a random image which immediately will be projected to the authentic user. In that case hacker won't get to know what a correct or incorrect image is whereas the real user will come to know. In that case he/she can scrutinize the real user.

Dr.D.S.Rao [4] provided us with electronic banking which proved as a benchmark for economic services through internet services. This in turn changed the business trade in banks severely. This is very user friendly in terms of cost and up gradation facility. It resulted in transactions made on smart phones from calling to online shopping and banking. This will give rise to mobile banking. Mobile phones replace the desktop computers. The mobile banking can be described as: "the execution of accounting services inside an electronic formula- where the customer or purchaser use the mobile statement methods in integration with mobile devices" Mobile banking allows or permits easy access to services stated by banks at anyplace anytime. The only catch in this whole process is the security and authentication mechanisms used which can be very easily accessed by hackers.

Humaira Dar et al [5] in the area of computer networking user authentication as well as authorization is a matter of concern in security system. Authentication is the method of verifying the user where as authorization is the methods of verifying that user have an access to resources.

R. Dhamija and Perrig [1] proposed a graphical authentication system which is based on the Hash Visualization technique. In this technique, the user is presented with the certain number of images generated by the program and then users have to select the picture from set of pictures. Then the user will be authenticated only if he is able to identify the preselected image. This technique fails to impress the users because the server has to store the number of images of each user in plain text.

Sagar Acharya [6] explained a technique that how two factor authentication can be implemented using SMS OTP. OTP is generated by Smartphone. It is the One Time Password that provides security user accounts. The proposed method ensures that online banking features are authenticated and secured. This method is also useful for e-shopping & ATM machines. The proposed system generates an OTP and sent One Time Password to mobile phones. For creating OTP's smart phones are used as tokens and in the form of SMS OTP is sent on mobiles. The generated OTP is valid for only for one login session and it is generated and verified using Secured Cryptographic Algorithm.

3. METHODOLOGY

The methodology used in this research is the Object Oriented approach. The approach is described as follows:

Stage-1: User Profile Registration: Before the multifactor authentication on the system, the user must be registered.

He must provide his basic information like first name, last name, DOB, username and password. After the registration when the user logs in by simply type a user name and password immediately he would get one time password on his cell phone via SMS. The generated OTP is valid for only one login session. One time password is generated by using Lamport's algorithm.

Stage-2: Image Based Authentication: This scheme is very simple to use and used in many systems today. After getting the OTP, the next step in this approach is image based authentication in which there are number of images and user have to choose pre-mentioned one from the set of multiple images. The pictures are generated randomly every time when the user logs in. The user can easily identify the images that are previously selected by him. The simple and minute thing the users have to do in this system is to recall the image selected by them. . If the user is correct, he moves on to the next stage of authentication otherwise, he is redirected to the login page.

Stage-3: Knowledge Based Authentication: After the image based authentication, the next step is knowledge based authentication. In this authentication users have to answer the question from the pre-mentioned details. This approach will provide a high level of security to the user from the systems to the hand held devices such as mobile phones.

4. RESULTANDIMPLEMENTATION

We have designed a Multi Factor Authentication System in ASP.NET with SQL Server

4.1 Registration

The first page of the system is the login page. Before login the user must register itself. Figure 1 below shows the user registration page. Registration page contains the First Name, Last Name, Email, Phone Number, Username and Password fields. After filling all these fields user gets registered by pressing the submit button.

Now the user is required to login using the username and password provided at the time of registration.

Figure1. Registration Page

We have designed a Signup System in which Password is encrypted and user is asked for a Pass Phrase and 4 Digit Pin along with a image from Users Computer.

A. LOG IN PAGE

Now when User has to Login he/she needs to provide their username only.

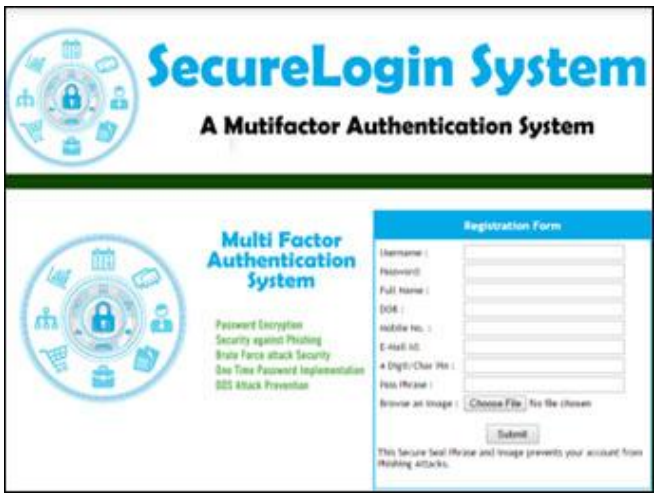

Figure 2. Login Page

And proceed to second screen.

4.2 OTP, Image Based and Knowledge based Authentication

After successful login, the OTP is sent to the phone number provided during registration. The received OTP is then entered for authentication. If the user fills up the correct OTP, he or she get the authentication and can proceed further for the next step of authentication.

The next step in multifactor authentication is image based authentication. After getting authenticated by filling the correct OTP, The user is presented with different images and he has to select the pre chosen image at the time of registration. The user will get authentication if he is successful in recognising that image. This is the last step in multifactor authentication. User is asked to fill some information provided by him at the time of registration.

The user needs to provide

a) Password

b) OTP Received on Mobile Combined with PIN

c) Pass Phrase

d) Image to be Selected from total of three Images

If any authentication fails the user is not permitted inside. And if the users fails authentication in total Five Times the account is locked for the session and user cannot even proceed to Login Screen thus eliminating the Possibility of Brute Force Attack.

Figure3. All three type of authentications

5. CONCLUSION

Mostly applications uses login system in which user have to simply insert username and password. But this technique is not secure because the hackers can easily crack the passwords by using modern techniques and can access the confidential information. The proposed system overcome this problem and improves the security by integrating three different authentication systems into single authentication system.

The One Time Password, image based authentication and knowledge based authentication system will help to deal in securing applications and transactions. Even if an attacker is somehow able to intercept on OTP, he has two more authentication system to deal with. To crack the whole security system is very difficult and time consuming. So, if we are using multi factor authentication mechanisms it will surely enhances the security of the application to a great extent and makes the application almost hack proof.

6. REFERENCES

[1] R. Dhamija and A. Perrig, 2000 "Déjà Vu: a user study using images for authentication," USENIX Association Berkeley, CA, USA, pp. 4-4.

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

[3] D.de Borde,"Two-Factor Authentication, 2008" Siemens Enterprise Communications UK-Security Solutions, whitepaper.

[4] Dr.D.S.Rao, Gurleen Kour, 2011 "One Time Password Security through Cryptography For Mobile Banking", IJCTA, Vol 2 (5).

[5] Humaira Dar, WajdiFawzi Mohammed Al-KhateebAnd Mohamed HadiHabaebi, 2013. Secure Scheme For User Authentication And Authorization In Android Environment. Int. Journal of Engineering Research and Applications. Vol. 3, Issue 5, pp.1874-1882.

[6] Sagar Acharya, A. P, 2013. Two Factor Authentication Using Smartphone Generated One Time Password. IOSR Journal of Computer Engineering (IOSR-JCE), 85-90.

[7] Ankit Aggarwal, Darshil Doshi, Vijay Gore and JigneshSisodia, 2015. Three Level Security Using Cued Click Points in Image Based Authentication.International Journal of Innovative and Emerging Research in Engineeringe-ISSN: 2394 – 3343 p-ISSN: 2394 – 5494.

[8] Niharika Gupta and Rama Rani, 2015. Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2.