JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

TWO FACTOR AUTHENTICATIONSYSTEM TO AVOID SHOULDER SURFING ATTACK

[1]M R Suresh, [2]Bhavana D C, [3]Madiha Mehrin, [4]Nisha Jain, [5]Spandana H G

[1]Associate Professor, [2]Student, [3]Student, [4]Student, [5]Student [1]Department of Information Science and Engineering, PESCE,

Mandya, India

Abstract: Authorization is the technique of allowing only authorized personnel to have access to an account or data. With our world advancing in technology, new authentication techniques have been proposed. Alphanumeric Passwords being the traditional methods of the authorization technique it is widely adopted around the globe. Users tend to use similar alphanumeric passwords for every one of their accounts putting all their accounts at risk to breaching.

These traditional passwords are vulnerable to the most common and easiest attack which is Shoulder Surfing Attack. The Shoulder Surfing is an assault which can be can be performed by unapproved user to acquire the approved user's password by looking from the user's shoulder when he enters his password. In a Jam-Packed place, these passwords can be seen over from the users shoulder easily. Not just in a crowded area but also when an attacker uses a camera or a zooming in device from a distance to look at the user's password.

If the user keeps his password simple for them to remember, the password becomes easier to guess for the attacker too and if the password set it difficult to guess by the attacker it can easily be forgotten by the user. Biometrics and Graphical Passwords are utilized to defeat these issues related with the traditional authorization technique of Alphanumeric Password method, which assures safety of user's account and data. In this paper we have proposed a two factor authentication to avoid shoulder surfing.

Index Terms **– Authentication, Shoulder Surfing Attack.**

I. INTRODUCTION

In many applications, computer security and confidentiality based on passwords are widely used. The most commonly used computer authentication method is the use of malicious passwords and numbers. In order to overcome this problem, we have tried to integrate both texts and graphics making the authentication more secure.

The demanding problem is to design a fixed user authentication method which involves humans in authentication procedure. As expected, to the convenience of the user, the most commonly used method of authentication is password. The use of weak or bad passwords will result in a person's shoulder attack, criminal identity theft, video recording, etc. To overcome this problem, we have developed a novel verification system, based on two-factor authentication to avoid shoulder surfing, using colors and images.

A two-factor authentication system can address the problems and weaknesses associated with text-based passwords. As per psychology, humans can remember images for a longer period of time when compared to numbers and words. Hence, we have integrated texts, images and colors in our proposed system to avoid shoulder surfing.

II. LITERATURE SURVEY

In 2015 author Priya More proposed Pair-based authentication scheme in which a userselects pair of letters corresponding to the intersection of the letter. The first letter in the pair is used to pick the row and the second letter is used to pick the column. If the password is verified the user will enter the system.

In 2017 author Veena rathanavel proposed Graphical password as an OTP .They have provided an Additional layer of security by generating one-time password(OTP) which is send to the users mobile. The OTP is the set of images where the user need to click on those images. The user need to confirm by selecting the images based on the details sent to them. It aims to avoid other attacks like dictionary attack, brute force attack and guessing attack. The OTP is sent on the user's mobile number from the database.

In april 2021 author Bhumika Patel proposed Graphical Password Authentication using colour login technique. Here the user should use the key colour to enter the password to prove user's authenticity. The user first need to select the colors from the set of colors in registration process, then while the user is logging the user has to use the key colour to enter the password.

In 2017 Author Aayush Dilipkumar jain proposed a scheme which mainly focuses on shoulder surfing. In this system, they proposed a new click-based colour password scheme called Colour Click Points(CCP). A password consists of one click-point per Colour for a sequence of Colors. The next Colour displayed is built on the previous click-point. In the proposed scheme, the user can easily and efficiently login to the system. Afterwards, we look in to the security and usability of the proposed system, and show the resistance of the proposed system to shoulder surfing. The benefit of this system is that it reduces the login time and it is an efficient system.

In 2011 author Ahmad Almulhem proposed graphical password authentication system in which user creates a graphical password by first entering a picture. The user then picks the several point-off interest (POI) regions in the picture. For every POI, the user types a word that would be associated with that PO.

III. METHODOLOGY

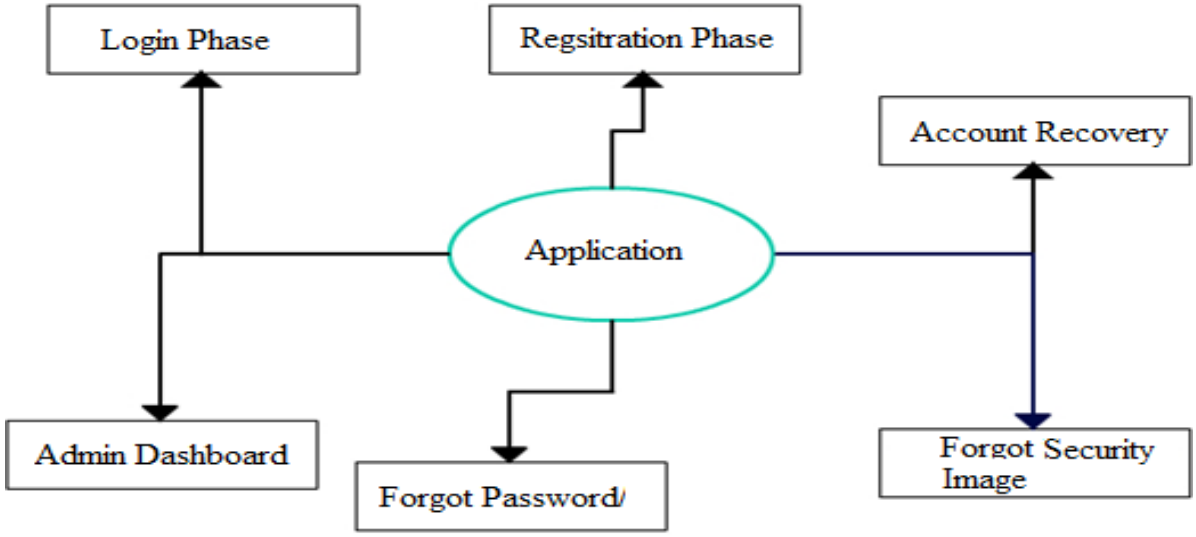

Figure: System architecture of the proposed system

This project focuses on the use of two-factor authentication methods using both users' traditional alphanumeric friendly password and a picture password as a verification gateway. The effort was made using two-factor authentication, and in this project we describe the design of a two-factor authentication system and the application of the design. So providing an additional password adds anextra layer of security

In order to use the proposed system, the user needs to first register for the system by entering their basic information.

The overview of the proposed system is as follows:

- The proposed program includes the Registration and Login section.
- The first phase is the registration phase.
- The registration category contains color choices (10 colors) out of which the user needs to select 1 key color which will be used in login,basic information and a password category(Both alphanumeric and image).
- After successful registration, the user can access the login section where they need to verify their record by entering the email id entered during registration. Once the email id is verified, the user may continue with the password field where they need to select alphabets using the key color.
- Once the textual password is verified the user will be redirected to second phase of login where he/she have to select images which were chosen during the registeration in the same order.
- Once the user is verified, they will be redirected to their profile page.

IMPLEMENTATION

Modules

- ❖ User Registration
- ❖ Login Phase
- ❖ Forgot Password/Security Image
- ❖ Account Recover
- ❖ Admin Dashboard

Registration Phase:

The user needs to set his passcode K of length L (4<L<8) characters, and pick one colour as his/her key colour from 10 colours appointed by the system. The user needs to provide his/her email address and basic information in the registeration phase.

This also support to select graphical authentication images where user have rights to select minimum 3 and maximum five security images and also provide the hint of the images selected so that it will be helpful to remember the image.

Login Phase:

In the login phase,at first, 20 characters along with the key color are displayed in a table format.

The user will have to use his/her key color to select characters corresponding to his/her password. The user can switch to next set of characters by clicking on right button and previous set of characters by clicking on left button. Once the user's credentials are verified he/she is redirected to graphical authentication images page where the user have to select images as per the existing order created during registration. User will have 3 attempts to login if user fails account will be blocked.

Forgot Password/Security Image:

This module supports user to reset the password whereas when user select forgot password option application will lead to security check where user have to answer for security question selected while registration. User will have 3 attempts to verify this account if user fails then his/her account will be blocked. If the user provides valid answer, application will lead to password reset option where user will have the option to provide new password.

This module also supports to identify the security images selected during registration with the application. This module displays the hint provided by the user. Based on this user can try to remember security images.

Account Recover:

This module enables the user to recover/Re-activate the account without the support of the administrator. In this module user's email id will be verified and OTP will be sent to email ID, if user provides valid OTP his/her account will be activated.

Admin Dashboard:

The admin module is one of the major module of the application where admin can control all the activities done in the application. This module supports to maintain city, state & country details.

This module also supports administrator to manage the security questions and images. Where he/she can add, edit and delete the security questions & images. Administrator can create, edit, delete & Block/UnBlock the user. Administrator also have the option to view all users log information.

IV. Conclusion

The primary point of this authentication system is to secure every user's account from external threats. Traditional password authentication system are prone to shoulder surfing attacks.Hence We have demonstrated a unique two factor authentication system which prevents shoulder surfing attack and also add an extra layer of security to traditional passwords.Though our system requires extra time to login, but it has accuracy just like traditional keyboard input..

V. References

[1] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu, "YAGP Yet Another Graphical Password strategy" (December 2008).
[2] Ziran Zheng, Xiyu Liu, Lizi Yin, Zhaocheng Liu, "A Stroke-based Textual Password Authentication Scheme" 2009 First International Workshop on Education Technology and Computer Science.
[3] Haichang Gao, Xiyang Liu, Ruyi Dai, Sidong Wang, Xiuling Chang, "Analysis and evaluation of the colour login graphical password scheme" (2009).
[4] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar, Department of Computer Science and Engineering, "Authentication schemes for session passwords using Colour and images" (May 2011).
[5] Ahmad Almulhem, "A graphical password authentication system" (2011).
[6] VeenaRathanavel, Swati Mali "Graphical Password as an OTP "(2015).
[7] Vikas B "Authentication Scheme for Passwords using Color and Text" (2015).
[8] Priya More, Ankita Singh , Prakash Singh "Authentication with Colours and Session Password" (2016).
[9] Aayush Dilipkumar Jain1, Ramkrishna Khetan2, Krishnakant Dubey3, Prof. Harshali Rambade "Color Shuffling Password Based Authentication" (2017).

[10] Nilesh B. Khankari, Prof. G.V. Kale "One Time Password Generation for Multifactor Authentication using Graphical Password" (2020).

[11] Bhumika Patel, Amaan Sarwar, Prof. Sachin Chavan, "Graphical Password Authentication Using Colour Login Technique", Vol. 8 IRJET 2021.