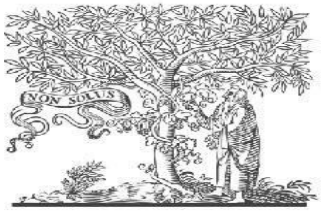
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# COPY RIGHT



ELSEVIER SSRN



IJIEMR Transactions, online available on 31st Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

**10.48047/IJIEMR/V12/ISSUE 03/96**

Title **GRAPHICAL PASSWORD AUTHENTICATION**

Volume 12, ISSUE 03, Pages: 656-659

Paper Authors
**Dr. Ch. Rajendra Babu, G. Sai Prasanna Bhavani , T. Arpitha, R. Gayathri**


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

# Graphical Password Authentication

**Dr. Ch. Rajendra Babu,** Professor, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
**G. Sai Prasanna Bhavani** , Student, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
**T. Arpitha**, Student, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
**R. Gayathri,** Student, Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.

**ABSTRACT**
"A Graphical password or graphical user authentication" is a form of authentication using graphical images rather than alpha numeric characters, where mostly the authentication process is done when alphanumeric characters are used as passwords. The user may forget the alpha numeric password which is build strong, hard to guess and remember. To address this problem, we have developed authentication methods that use Pictures as passwords. The type of images used and the ways in which users interact with them vary between implementations. Instead of alphanumeric passwords we can use graphical passwords.

**INTRODUCTION**

These days there are many cyber attacks in to our systems and they result in the leakage of our Personal and Professional Data. Thus, the Attackers generally use Brute Force approach, Installing Spyware, Dictionary attacks. This needed to be overcome by any approach that deals with all the certain possibilities in our daily life. Now all the software and online sites make sure the user to have at least 8 – character length password and that has to be mixed of all Alphabets (small and capital), numeric and special characters. This may provide better security from Brute Force Attacks, but the spyware installation can easily get the details of the user. This also gives the user extra burden to remember the various lengthy passwords for various accounts. This results the user to frequently forget the password.

**LITERATURE SURVEY**
In Different ways, the Graphical passwords can be used to set the passwords. For the user two options are provided either sign up or sign in. If the user is new then he/she goes to sign up option and enter the details and set a password by selecting two images.so now the password is set successfully. After that user can sign in to the system at any time. When user clicks sign in then it asks username first then the system verifies the username and provides group of images in which user has to select two images which he/she selected during the sign up process. If he/she selects images correctly then it shows login successful otherwise incorrect. In this manner the graphical authentication can be occurred. Graphical passwords can also used in the mobile authentication process, instead of using the four or six pin patterns here these pins can be replaced by the graphical passwords.

Graphical passwords helps in the resistance of shoulder surfing attacks and brute force attacks.

In the brute force attacks, the hacker decodes the login information and gain the information that is hidden in it.

These hackers can also decrypt the encrypted information by using the keys and get the information which is hidden in it. If we use graphical passwords it is hard to find the patterns that are encrypted because images are used as passwords here. So finding the pattern of

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

the images is a tough process and cannot be hacked.

**EXISTING SYSTEM**

Recognition based Authentication: In Recognition based, Number of Images are provided in the password setting process. The user need to select images to set as password. These images need to be remembered for the login process. This scheme helps for the shoulder surfing attacks. Here remembering is an issue.

Recall based Authentication: In recall based Authentication, a Clear background is provided to the user. The user need to draw lines on the screen and need to memorize it. In the login process, the same background is provided to the user, the user then has to draw the same line on it for the login process. Hints can also be provided to the user to draw the lines correctly. This method prevent user from brute force attacks and spyware attacks.

Cued Recall based Authentication: In Cued Recall based Authentication, an Image is provided to the user. The user need to click on particular spots of the image. The spots are saved in the database in the for of x-coordinate and y-coordinate. Both x and y coordinates are saved in the database. During the login process, the user need to select on the exact spots of x and y axis coordinates for the authentication. If the spots are matched correctly then the authentication becomes successful. This method provides an higher security to the system and protects the system from any types of attacks.

**PROPOSED SYSTEM**

In the proposed system we follow cued recall based Authentication. A image is provided to the user. User can select any number of spots in the image. While selecting the spots the user also need to provide a word in the selected spot. The spot and word both are saved in the database. In the login process the user have to correctly Identify the spot correctly and need to type the word correctly. Providing word is not necessary, it was based on the user interest. In this manner a high security is provided to the system by the hidden spots and the words.

**METHODOLOGY**

Initially, If the user is new user then he/she need to register otherwise they can directly go for the login process. When user clicks on register then initially he/she need to provide information about personal details like username, place, Gmail id, phone number. This information is stored in the database. In the password setting process the user need to upload an image from the system and need to select some spots, if he wants he can provide words for the selected spots. Finally user need to click on register button to register successfully. Once the registration is completed, then the user can login to the system.


At the time of login, user has to provide the username then the system verifies the username and displays the image which is stored to the user. Then the user need to identify the correct spots on the image. When the spot is identified correctly then if an word is hidden the it shows to the user in a * form. Then the user need to type the word for the successful authentication. If spots and words are correct then the system login becomes successful.

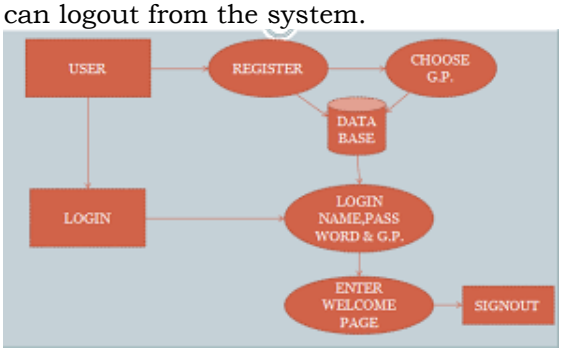
If the user forgets the password, the he/she can change it. There is an other option called admin where only admin of the system can only access it. If the admin provide his/her username and password then it logins into it. There the information about all the users are saved and monitored. If the process is completed we can logout from the web application.

**SYSTEM ARCHITECTURE**

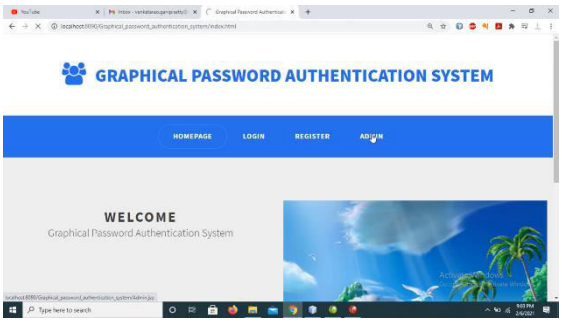
The system Architecture works as follows, user can register by choosing a

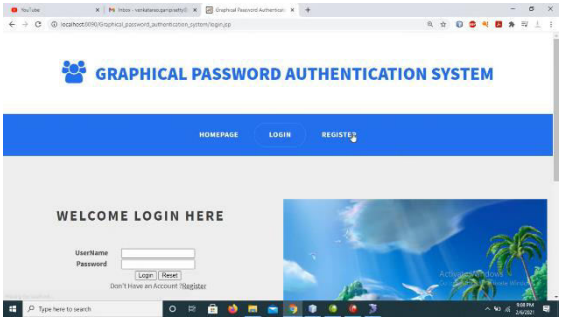
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

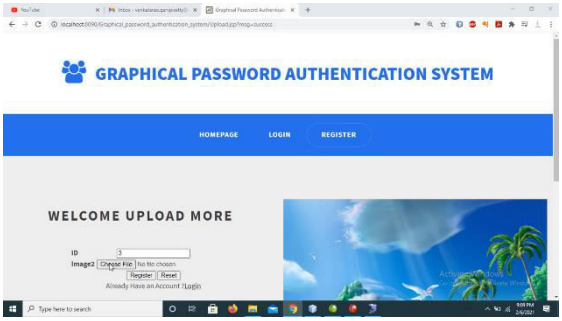
picture and setting the password and that is saved in the database. Then the user login to the system by providing the username and password. If the login is successful then welcome page is appeared in the user interface. User can logout from the system.




## RESULTS




## CONCLUSION

User Authentication is fundamental factor for providing security to the information which is hidden in it. So for the authentication process, using images as passwords is much better than using the alphanumeric characters. Graphical passwords provides higher security by preventing from the shoulder surfing attacks, spyware attacks, dictionary attacks, brute force attacks.

## REFERENCES

▪Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015

▪ Graphical Password Authentication. ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE

▪ A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices. Teoh joo Fong, Azween Abdullah , NZ Jhanjhi School of Computing & IT, Taylor?s University, Subang Jaya, Selangor, Malaysia, 2019

▪ A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K

▪ Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme. Prof. S. K. Sonkar, Prof. R. L. Paikrao , Prof. Awadesh Kumar, Mr. S. B. Deshmukh, Computer Engineering Dept. Computer Engineering Dept. Amrutvahini College of engineering, February – 2014

▪ A Graphical Password Against Spyware and Shoulder-surfing Attacks. Elham Darbanian Master of Engineering, College of e-learning Shiraz University, Gh. Dastghaiby fard Department of Computer science & Engineering, College of Electrical and Computer & Engineering Shiraz University,jun- 2015.

▪ Text based Graphical Password System to Obscure Shoulder Surfing. Khazima Irfan, Agha Anas, Sidra Malik, Saneeha

Amir Department of Computer Science COMSATS Institute of Information Technology Islamabad Pakistan, 13th January,2018