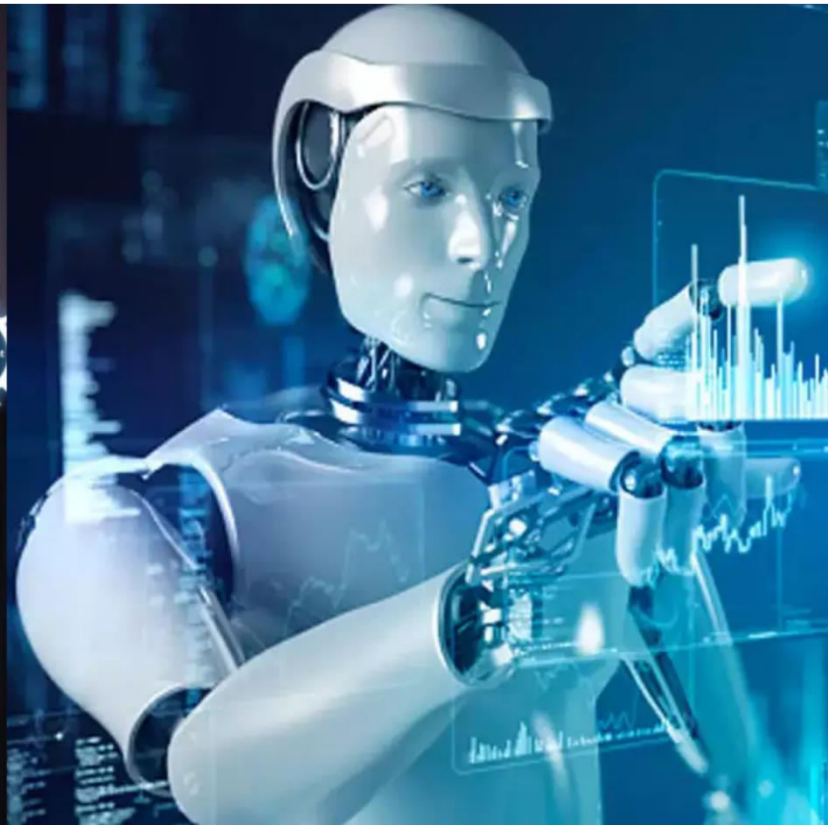
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

Graphical Password Authentication

Katepalli Nitish Kumar, Kolanu Shiva Krishna, Kindinti Sainath, Kanumari Karthikeya Varma, Dr.K.Baalaji

Dept. of CSE, Bharath Institute of Higher Education and Research, Chennai, India

ABSTRACT: Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, this method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own.The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area.

KEYWORDS*:* Hypertext Transfer Protocol, Graphical User Interface, HTML, CSS and Java Script, packages

I. INTRODUCTION

Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of use and accessibility. Current secure systems suffer because they mostly ignore the importance of human factors in security (Rachna Dhamija and Adrian Perrig., 2000). A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource. Traditionally, alphanumeric passwords are used for authentication but they are known to have usability and security problems. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. A password is a secret that is shared by the verifier and the user, they are simply secrets that are provided by the user upon request by a recipient and are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists (www.objs.com/survey/authent.html, 2011).Graphical passwords (GP) use pictures (Parkinson, 2005) instead of texts and are partially motivated by the fact that humans can remember pictures more easily than a string of characters.

The idea of graphical passwords was originally described by Greg Blonder in 1996 and since then several researchers have proposed different graphical password authentication schemes, in Blunder's description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. An important advantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. An important advantage of Graphical Passwords is that they are easier to remember compared to textual passwords. Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security.

II. OVERVIEW OF THE AUTHENTICATION METHODS

Current authentication methods can be divided into three main areas:
• Token based authentication
• Biometric based authentication

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

• Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

III. LITERATURE REVIEW

For over a century, psychology studies have recognized the human brain's apparently superior memory for recognizing and recalling visual information as opposed to verbal or textual information. The most widely accepted theory explaining this difference is the dual-coding theory (Pavio, 2006), suggesting that verbal and non-verbal memory (respectively, word-based and image-based) are processed and represented differently in the mind. Images are mentally represented in a way that retains the perceptual features being observed and are assigned perceived meaning based on what is being directly observed. The text is represented symbolically, where symbols are given a meaning cognitively associated with the text, as opposed to a perceived meaning based on the form of the text. A generally accepted fact in graphical password authentication is that graphical passwords are prone to shoulder surfing attacks. Because of this, several researchers have studied the graphical password scheme and come up with techniques that reduce the shoulder surfing problem. Another drawback graphical passwords have is that they can be guessed if the attacker is persistent to try all possible inputs. In order to make the password hard to guess; (Sobrado.L and Birget.J.C, 2002) suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of this algorithm is that the login process can be slow.

A shoulder-surfing resistant graphical password scheme

A shoulder-surfing resistant graphical password scheme (Sobrado.L and Birget Authentication

(Hong.D, Man.S, Hawes.B, and Mathews.M, 2002) proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

IV. GRAPHICAL PASSWORD

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should be more resistant to brute- force attacks, since the search space is practically infinite.
In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques.

With increasing technical advancements the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentication available for users to secure their accounts.

Recognition based Authentication: A user is given a set of images and he has to identify the image he selected during registration.
For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.

Recall based Authentication: A user is asked to reproduce something that he created or selected at the registration stage. For example, in the Passpoint scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.

Cued Recall: Cued Click Points (CCP) is an alternative to the PassPoints technique. In CCP, users click one point on each image rather than on five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

Cued Click Points (CCP)

V. RECOGNITION BASED SYSTEM

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. Recognition- based systems, also known as cognometric systems [4] or searchmetric systems [3], generally require that users memorize a portfolio of images during password creation, and then to log in, must recognize their images from among decoys. Humans have exceptional ability to recognize images previously seen, even those viewed very briefly [8], [9]. From a security perspective, such systems are not suitable replacements for text password schemes, as they have password spaces comparable in cardinality to only 4 or 5 digit PINs (assuming a set of images whose cardinality remains reasonable, with respect to usability).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

Recognition based systems have been proposed using various types of images, most notably: faces, random art, everyday objects, and icons. Renaud [3] discusses specific security and usability considerations, and offers usability design guidelines focusing on recognition-based systems.

In some graphical password schemes, the system must retain knowledge of some details of the shared secret, i.e.,user specific profile data e.g. in recognition schemes, the system must know which images belong to a user's portfolio in order to display them. This information must be stored such that its original form is available to the system (possibly under reversible encryption), and thus may be available to anyone gaining access to the stored information.
E.g. Phishing attack and shoulder surfing attack.

Dhamija and Perrig [4] proposed a graphical authentication scheme based on the Hash Visualization technique [9]. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (figure 1). Later, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Akula and Devisetty's algorithm [10] is similar to the technique proposed by Dhamija and Perrig [4]. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's.

Weinshall and Kirkpatrick [11] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images.

After one to three months, users in their study were able to recognize over 90% of the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training.

Sobrado and Birget [12] developed a graphical password technique that deals with the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects (figure 2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects.

VI. PROPOSED SYSTEM

In graphical authentication there are various techniques to secure your password. Here we are proposing a new algorithm of authentication using images. We used a grid based approach to authenticate by using image as a reference.

Shoulder surfing is a major drawback of graphical password authentication. To overcome this we have developed SSR (Shoulder Surfing Resistant) shield. The shield containing multiple fake mouse pointers are programed in such a way that it moves randomly in an image area and the original pointer will look exactly as fake mouse pointers. This shield provides a top layer for grid clicking as well as confusing other person.
At the time of registration, user will upload his/her image or set of images along with all details; then user selected image will appear on the page with transparent grid layer on it. So user will select certain grids to set his/her password as shown in the figure below.

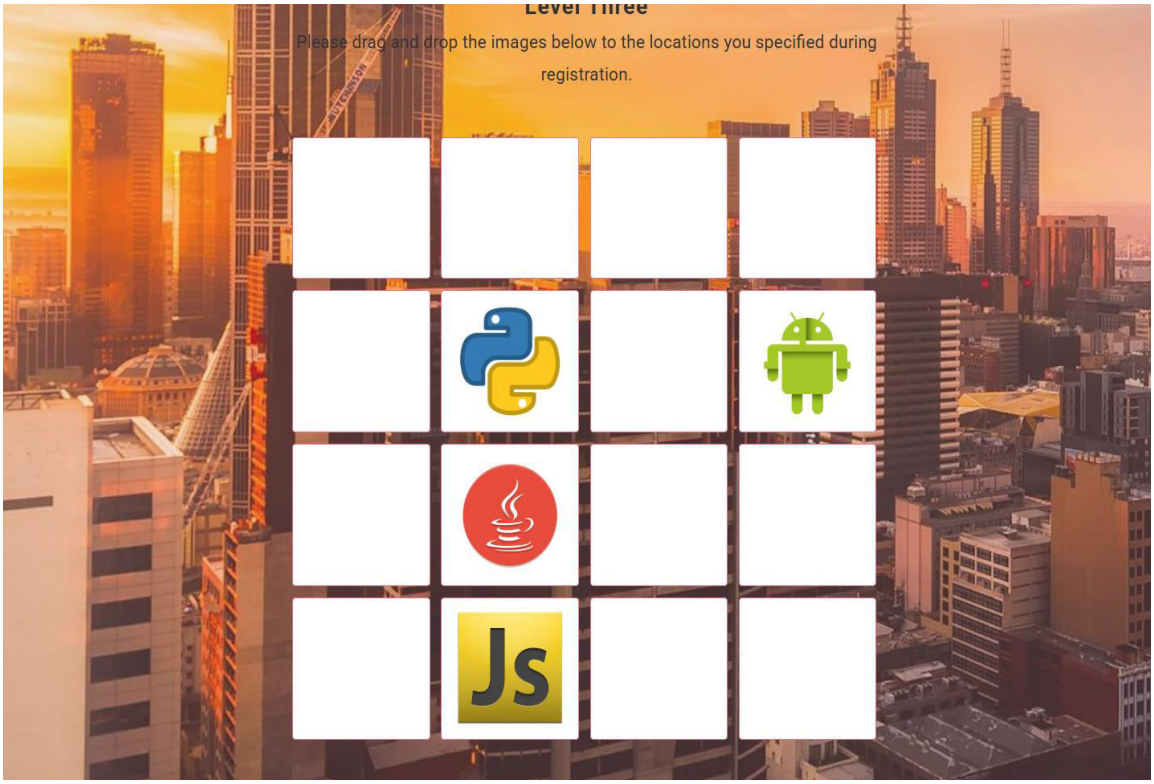
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558



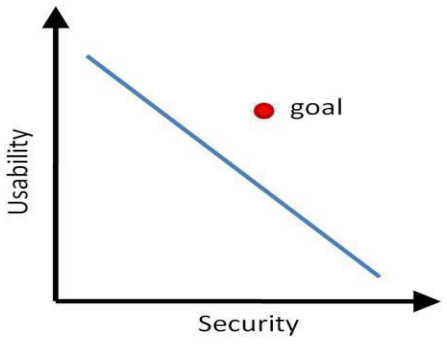
VII. IMPLEMENTATION

The proposed system was implemented using PHP, CSS, JavaScript and Macromedia flash 2008(Action Script 2).

This Graphical Password can be implemented in authenticating several systems and websites. The implementation has few focuses:

- **Login:** Contains username, images, Graphical password and related methods.
- **Grids:** Contains unique grid values and grid clicking related methods.
- Password
- Contain image as reference & encryption algorithm.
- Color Code: Contains colored password with encryption algorithm.

As shown in the figure below researchers are trying to stabilize the goal in text based system. However, the text based approach is not able to achieve the goal because as the password strength increases usability decreases.



Usability vs Security

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

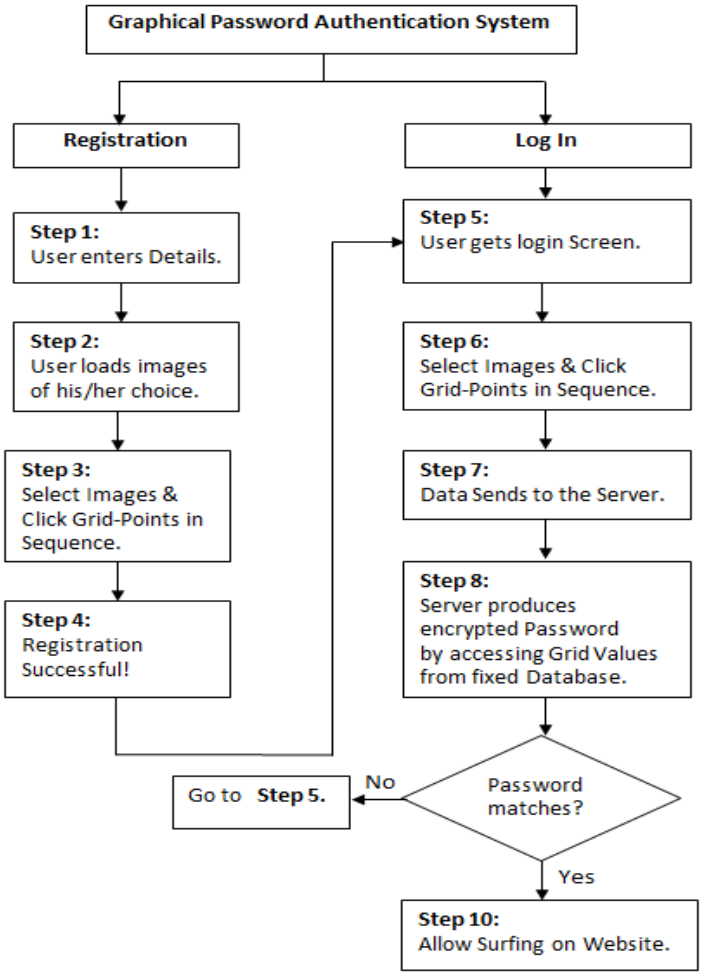
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

Our main aim is to achieve this goal. In which the usability as well as the security of the system is maintained in such a way that we don't need to compromise on either of these constraints.

The working of our system is shown with the help of a flow graph in given figure:-



Advantages

- It is user-friendly.
- It provides higher security than other traditional password schemes.
- Dictionary attacks are infeasible.
- CCP makes attacks based on hotspot analysis more challenging.

Disadvantages

- Registration and login take too long.
- It requires more storage space because of images.
- Shoulder surfing(Watching over people's shoulders as they process information)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

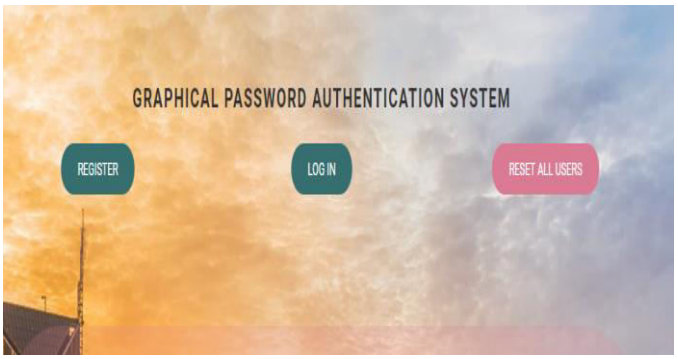
Impact Factor 8.699

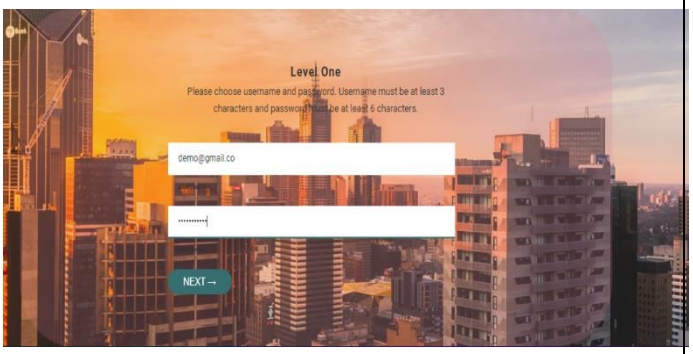
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

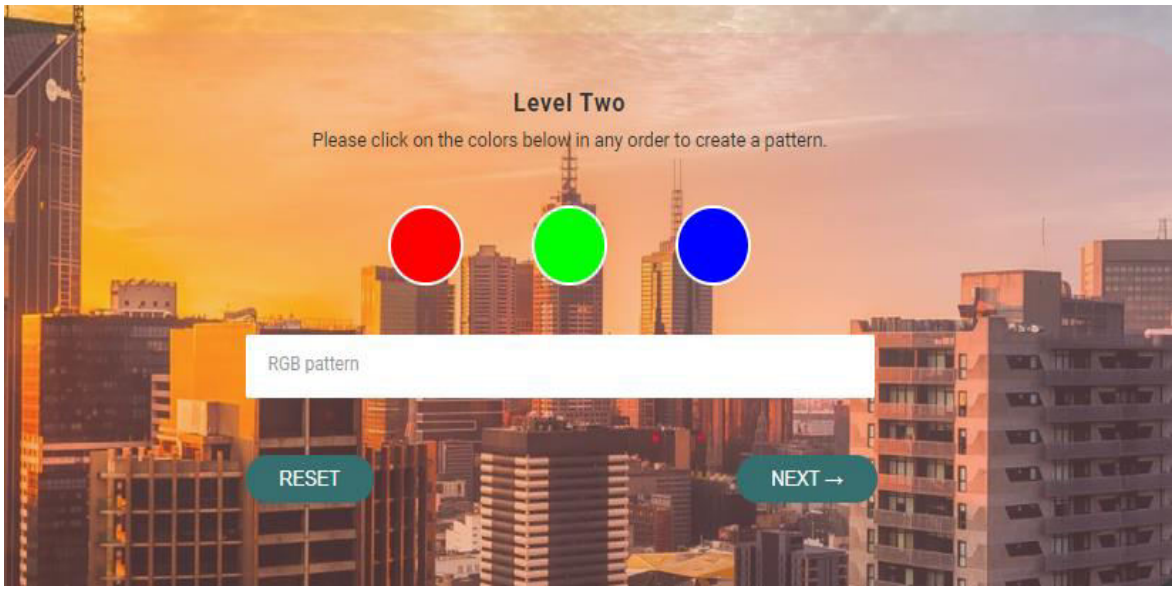
Volume 14, Issue 4, April 2025

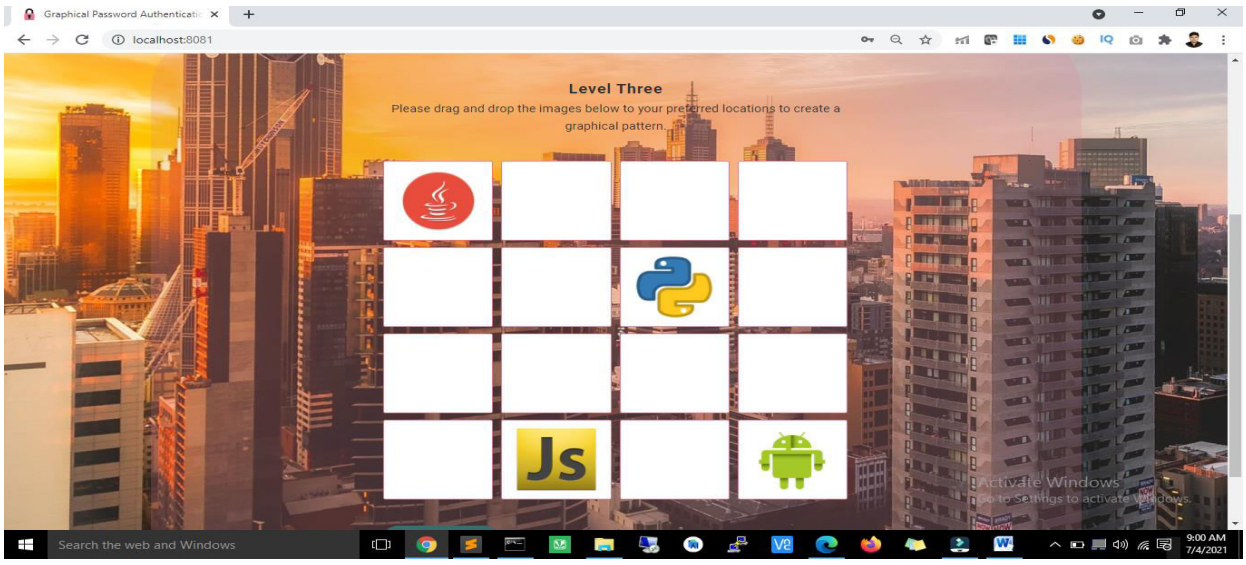
|DOI: 10.15680/IJIRSET.2025.1402558

VIII. SCREENSHOT









International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1402558

IX. CONCLUSION AND FUTURE WORK

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this report is a comprehensive research on existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. My research suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware.

In this extended abstract we are trying to make our authentication system more user friendly and also we have tried to implement mature & fast Shoulder Surfing Resistant Mechanism. We have considered both methods: text based and graphical based systems and tried to reduce the efforts required by end-user to remember passwords. A look at the advancement in technology over the past few years tells us that the next era will have system security at its core. Thus Graphical Password may be adapted in future as a major authentication system.

REFERENCES

1. Hong.D, Man.S, Hawes.B, and Mathews.M (2002).” A password scheme strongly resistant to spyware”. International conference on security and management. Las Vegas.

2. Hong.D, Man.S, Hawes.B and Mathews.M (2003).” A shoulder-surfing resistant graphical password scheme”. International conference on security and management. Las Vegas.

3. Parkinson, M. (2005).” THE POWER OF VISUAL COMMUNICATION”.

4. Pavio, A. (2006). Mind and Its Evolution: A Dual Coding Theoretical Approach.

5. Rachna Dhamija and Adrian Perrig. (2000). Déjà vu: A User Study. Using images for authentication.

6. Sobrado.L and Birget.J (2002). Graphical Passwords, “An Electronic Bulletin for Undergraduate Research”, vol.4.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details