IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

Graphical Password Authentication

Mrs. SK. Rahimunnisa[1], Sarayu Ginni[2], Sathivilli Praveena[3], Ravalapodi Pavani[4], Velaga Neeraja[5], Potnuru Kranthi[6]

[1]Assistant Professor, Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women Visakhapatnam, India

[2-6]Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, India

Abstract: A graphical password is an authentication system that works by having the user to select from images, in a specific order, presented in a graphical user interface. Computer security largely depends on the passwords to authenticate the users from the attackers. Generally, the computer authentication method that is used is alphanumerical usernames and passwords. However, this method has some significant drawbacks. To address these kinds of problems, some researchers have developed the authentication methods that use pictures as passwords. In this project, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory and the domain is Block chain and Cyber security. The algorithm that is used in this project is Persuasive cued click points (PCCP) With Improved Advanced Encryption Standard (IAES). The PCCP and IAES features are implemented together for the graphical password authentication system. Graphical passwords have been proposed as an alternative to the text-based schemes, by the fact that humans can remember pictures better than text since pictures are generally easier to be remembered or recognized than text.

I. INTRODUCTION

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most of the authentication system nowadays uses a combination of the username and password. The problem with the password is that it requires user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate number, parent name, phone number sometimes their own name which are very much predictable or complex passwords which they overlook so they might be use the same password for different accounts or they jot down their password somewhere. Moreover, user is vulnerable to various attacks. Text based passwords faces issues with security and usability matters.

II. PROPOSED SYSTEM

Graphical passwords allow the users to click on the certain areas of the screen so that these are then converted by the computer to be used for the authentication.
In the proposed system we have 3 levels of authentication.

- 1st level is all about the user needs to enter the username and password to register or login to the page.
- 2nd level is all about th user needs to select the colors to register or login to the page.
- 3rd level is all about the user needs to rearrange the images in desired locations to register or login to the page.

III. SYSTEM REQUIREMENTS

1. Hardware Requirements

The minimum hardware requirements to execute the system are as follows:

- Processor - Intel I3
- RAM - 4GB and more
- Storage - 1GB

2. Software Requirements

- Operating System – Windows 10
- Backend – Node Js
- Frontend – HTML

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

3. Functional Requirements

- Data Collection
- Data Preprocessing
- Training and Testing
- Modeling
- Predicting

4. Non-Functional Requirements

- Performance
- Reliability
- Availability
- Security
- Maintainability
- Portability

IV. METHODOLOGY

The procedure and methodology involved at first, we need to create a user account for that we need to set username and text password in level one and then a graphical password for high security which uses either Recall based orRecognition based techniques in level two and save them. Now an account is created so log in into the account by giving the user details andpassword if the password given is true then enter into the account else enter into the first level of login page.
To create this project, we have used two types of algorithms namely Persuasive cued click point and Shoulder surfing shield resistant.

Persuasive Cued Click Point Algorithm:

The users will click on a particular part of imageto confirm authentication. The persuasive cuedclick will provide a series of images where the images needed to be selected in such a way thatthey can be selected either once or many times.The main advantage of this persuasive cued click points are to select the images randomly in any order. The most useful advantage ofPPCP is attackers have to improve theirguesses. Users have to select a click point within the highlighted viewport and cannot click outside of the view port unless they press the shuffle button to randomly reposition the viewport. At the of password creation usersmay shuffle as often as desired but it slows the process of password creation. We implementedthis algorithm in the level-2 where colors can beselected randomly and in any number of click points.

Shoulder Surfing Resistant ShieldAlgorithm:

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PIN), passwords and other confidential data by looking over the victim's shoulder. The unauthorized users watch the keystrokes inputted on a device or listen to the sensitive information that is being spoken, which is also known as eavesdropping. Attackers do not needany technical skills in order to perform thismethod, and keen observation of victim surrounding and typing pattern is sufficient.
To overcome this shoulder surfing shieldalgorithm is used in level-3 of implementation.This shield provides a top layer for grid clickingas well as confusing another person.
The images in the level-3 are not positioned inthe same order.

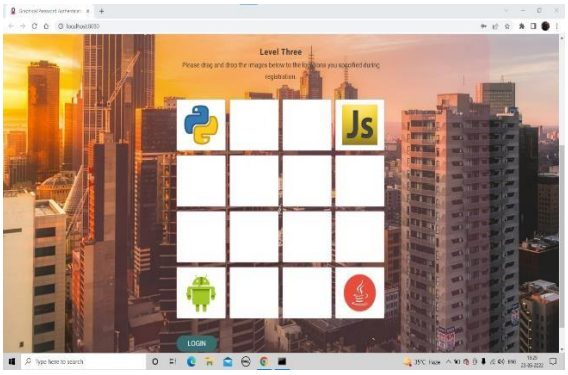

Fig 1: Shoulder Surfing Resistant Shield

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

V. IMPLEMENTATION

The method of implementation is divided into 3 levels. We implemented a registration page for new user and the login page for the existing user.
A three-level password authentication is
implemented each level has it's own prioritybased on the application used.
Level-1 implementation is a traditional alphanumerical password where the password isrepresented as either alphabets or numbers.
Level-2 implementation is about selection of colors in a sequence during registration and againgiving the same color sequences during login.
Level-3 implementation is about dragging anddropping the images to their respective grids without any following any sequences.
To implement this project, we used Persuasivecued click point and Shoulder surfing shield resistant algorithms.

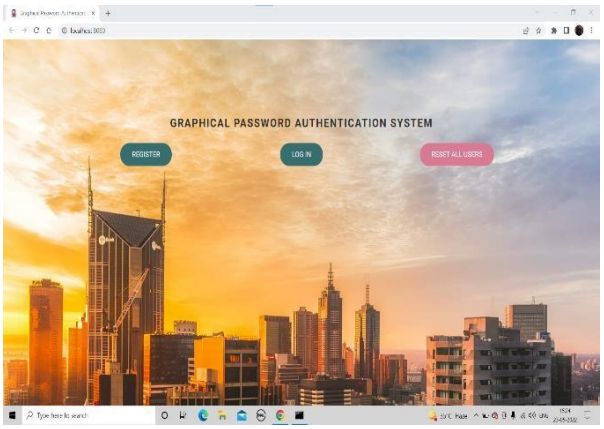

Fig 2: User Interface Screen

VI. RESULTS

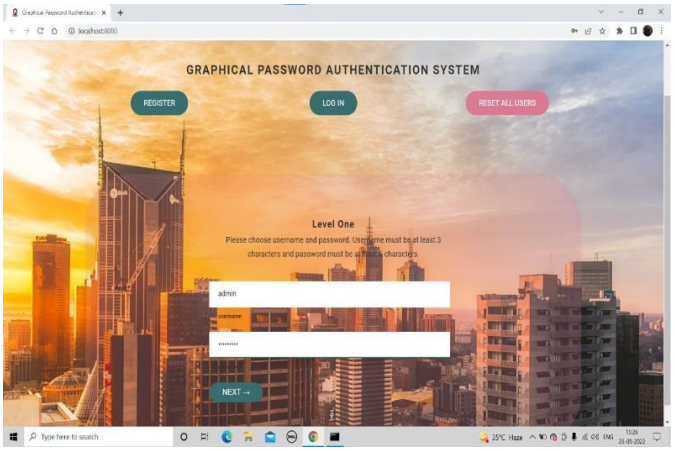

Fig 3: Level One Register Screen

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

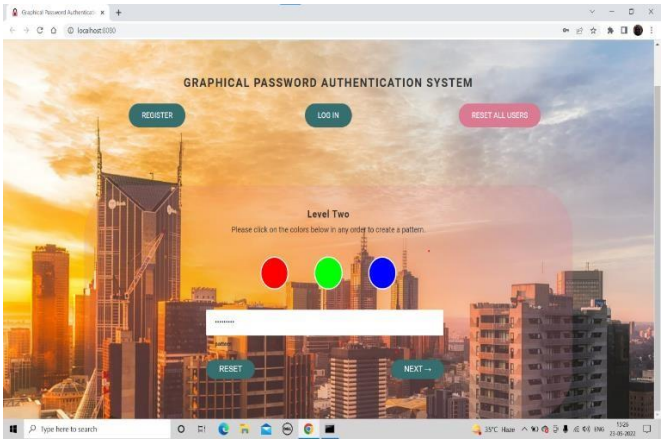

Fig 4: Level Two Register Screen

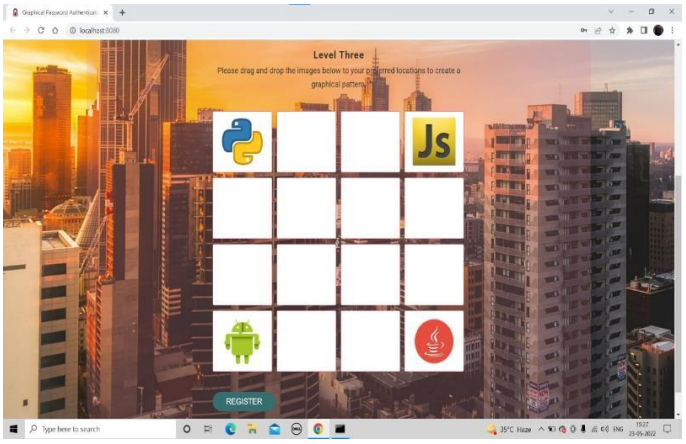

Fig 5: Level Three Register Screen

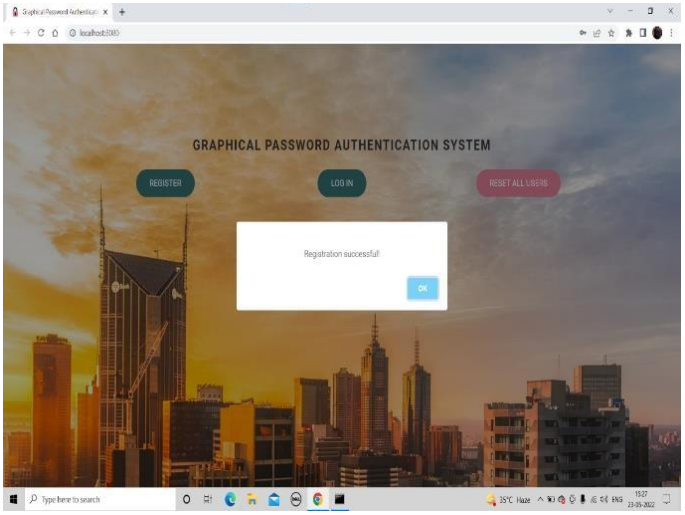

Fig 6: Registration Successful Screen

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

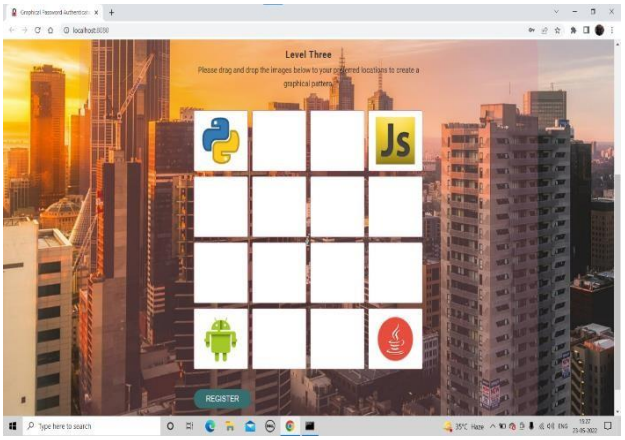

Image 7: Level One Login Screen

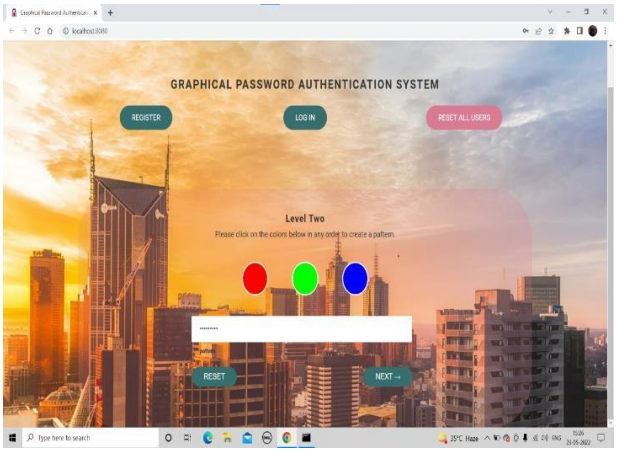

Image 8: Level Two Login Screen

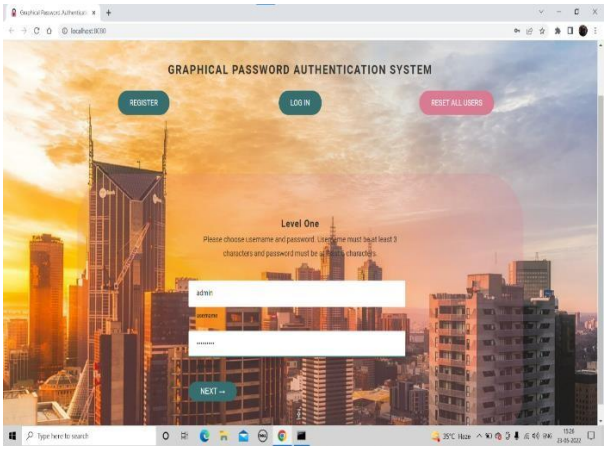

Fig 9: Level Three Login Screen

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10617

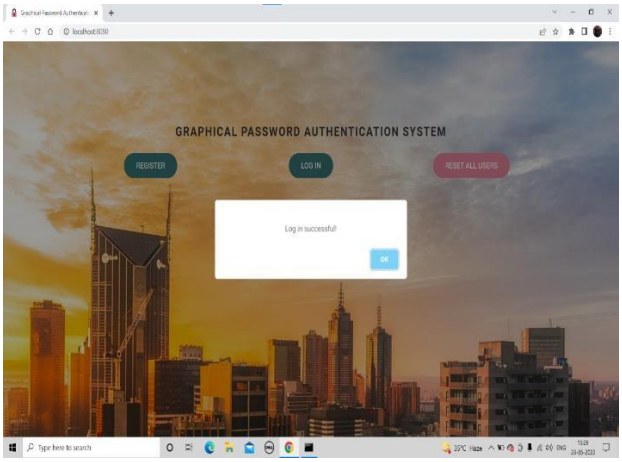

Fig 10: Login Successful Screen

VII. CONCLUSION

Our work mainly focuses on the graphical password authentication for the users who need atmost security for their credentials. User authentication is a fundamental component in most computer security contexts. Graphical passwords act as an alternative for the text-based passwordschemas. Graphical password authentication system which provides the more secure authentication than the text password scheme.

VIII. REFERENCES

[1] Nelson, D. L., Reed, V. S., & Walling, J. R. (1976). Pictorial superiority effect. Journal of experimental psychology. Human learning and memory, 2(5), 523–528.
[2] Dhamija, R. (n.d.). Hash Visualization in UserAuthentication . 2.
[3] Khan , W. Z., & Aalsalem, M. Y. (19 December, 2013). A Graphical Password Based System for Small Mobile Devices. p. 11.
[4] Tao, H. (2006). Pass-Go, a New GraphicalPassword Scheme. 11.
[5] Towseef Akram , Vakeel Ahmad, Israrul Haq, &Monisa Nazir. (2017). Graphical Password Authentication. 7.
[6] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, &Pranjal Rathod. (2013). Secure Authentication with 3D Password. 7.
[7] N.Asokan. (16 May, 2014). A Closer Look atRecognition-based Graphical Passwords. p. 13.
[8] Zheng, Z., Xiyu Liu , Lizi Yin , & ZhaochengLiu. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. 8.