International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 9, Issue 01, January-2024, http://ijmec.com/, ISSN: 2456-4265

GRAPHICAL PASSWORD AUTHENTICATION

Srikarnika Thaireddy, Mrs. Kiran Pakmode

[1]B.tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

[1]Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

Abstract: Authentication is performed using passwords that are alphanumeric in nature. However, users find it difficult in remembering a password that is long and needs to be recalled again and again while implementing it. Instead, they create short, simple, and insecure passwords that make the user's data vulnerable to outside attacks. Graphical passwords provide a way out of this dilemma by making passwords more remember able and easier for people to use as a password and, therefore, makes it more secure. Using a graphical password, users clicks on images rather than typing text passwords which contains alphanumeric characters. A new and more secure graphical password system has been developed which uses image Pattern. The image segmentation system presents the user with an image upon which the user selects a number of grids on this image; when entered in a proper sequence these points authenticate the user. The findings showed alphanumeric passwords and graphical passwords both worked in similar time but the graphical passwords were easier to recall and remember. Thus, Graphical passwords were found to be hard to crack as they are newly implemented and not many algorithms have been devised to break through them.

I. INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumerical password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word. Another proposed solution is to use graphical passwords, in which graphics (pattern) are used instead of alphanumerical passwords . This can be achieved by asking the user pattern rather than typing characters as in alphanumeric password approaches. In this extended abstract, we propose a graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds.

II. LITERATURE SURVEY

M. Alsaleh, M. Mannan, and P. C. van Oorschot has proposed the use of passwords is a necessity in computer security but passwords are often easy to guess by automated programs or tools running dictionary attacks. In the existing system, an automated test is implemented that humans can pass, but current computer programs can't pass. Any program that has high success over these tests can be used to guess passwords cause security risks. An example of such a test is a 'captcha'. A captcha is a test used in computing which ensures that the response is generated by a person and not by a tool. The process usually involves a computer asking a user to complete a simple test which can ensure a successful login. These tests are designed to be easy for a computer to generate, but difficult for a computer to solve, so that if a correct solution is received, it can be presumed to have been entered by a human.

X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., have been proposed as an alternative to alphanumeric passwords with their advantages in usability and security. However, most of these alternate schemes have their own disadvantages. For example, cued-recall graphical password schemes are vulnerable to shoulder-surfing and cannot prevent intersection analysis attack. A novel cued-recall graphical password scheme CBFG (Click Buttons according to Figures in Grids) is proposed in this paper. Inheriting the way of setting password in traditional cued-recall scheme, this scheme is also added the ideology of image identification. CBFG helps users tend to set their passwords more complex. Simultaneously, it has the capability against shoulder surfing attack and intersection analysis attack. Experiments illustrate that CBFG has better performance in usability, especially in security.

P. Andriotis, T. Tryfonas , G. Oikonomou and C. Yildiz had proposed that allow a user to unlock a smartphone's screen are one of the Android operating system's features and many users prefer them instead of traditional text-based codes. A variety of attacks has been proposed against this mechanism, of which notable are methods that recover the lock patterns using the oily residues left on screens when people move their fingers to reproduce the unlock code. In this paper we present a pilot study on user habits when setting a pattern lock and on their perceptions regarding what constitutes a secure pattern. We use our survey's results to establish a scheme, which combines a behaviour-based attack and a physical attack on graphical lock screen methods, aiming to reduce the search space of possible combinations forming a pattern, to make it partially or fully retrievable.

K. Lai, J. Konrad and P. Ishwar has proposed Video cameras are extensively used in modern surveillance systems to detect, track, and recognize, objects, people, and anomalies. Their use in user authentication, however, has been limited primarily to close-range face recognition systems. In this paper, we explore user authentication based on gestures captured by a video camera. Unlike pure biometrics, such as fingerprints, iris scans, and faces, gesture-based authentication combines irrevocable biometric information, such as the shapes and relative sizes of body parts, with voluntary movements which can be revoked. Our authentication method applies the empirical feature covariance matrix framework that has previously been used for tracking, face localization, and action recognition, to features extracted from body silhouettes.

ANALYSIS

The project focuses on implementing a secure authentication system using graphical passwords. Instead of traditional alphanumeric passwords, users will select images as their password. This approach aims to provide a more intuitive and memorable way for users to authenticate themselves. By leveraging visual cues, the risk of password guessing or theft can be reduced. The cost of the project will depend on factors such as the complexity of implementation, hardware requirements, and development resources. To successfully implement this system, you'll need to design and develop the graphical password interface, ensure its usability through testing, and integrate it into the authentication process. By accomplishing these tasks, you can create a more secure and user-friendly authentication experience.

Content diagram of Project

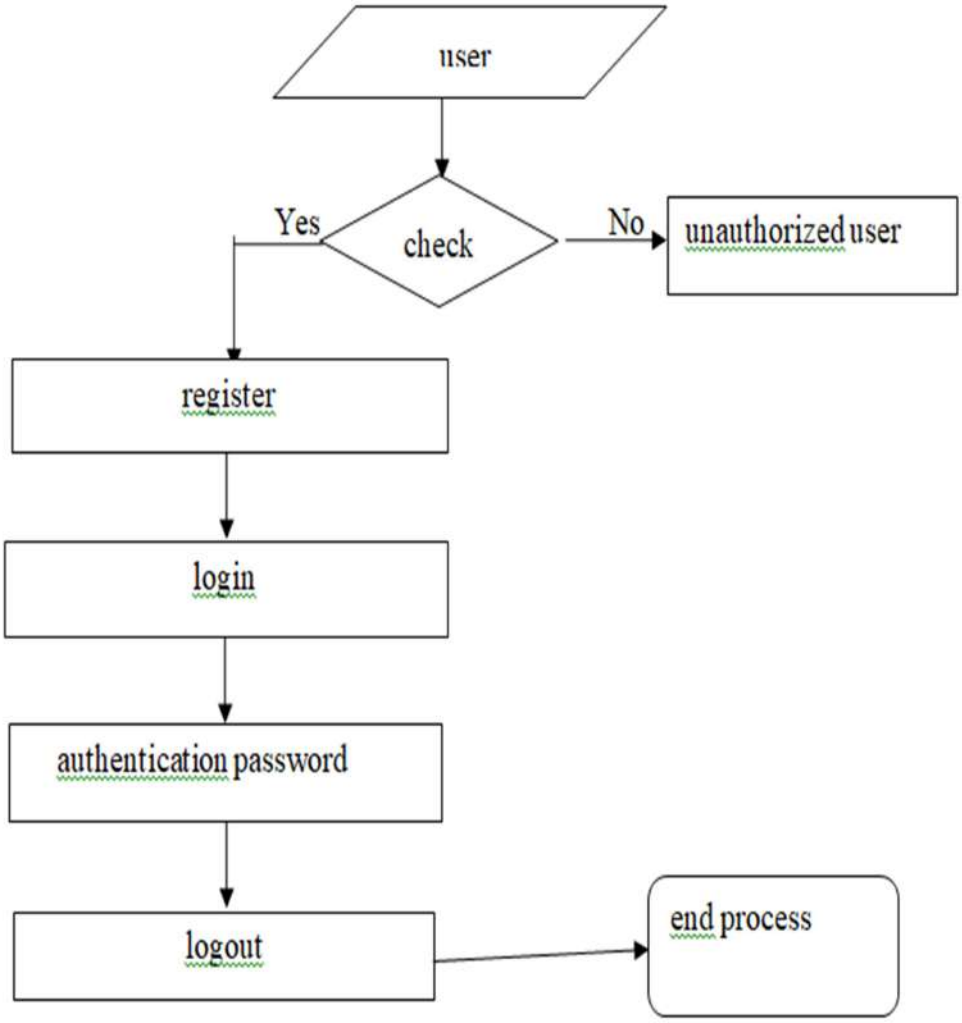

Fig: Content diagram

III. DESIGN

Designing graphical password authentication systems is driven by the need for improved security, enhanced user experience, reduced cost, flexibility, and compatibility with a wide range of devices and platforms.

Improved Security: Graphical passwords are more secure than traditional text-based passwords because they are harder to guess or crack using brute force attacks. The use of images, symbols, and patterns makes it more difficult for attackers to guess the password, as there are a larger number of possible combinations.

Enhanced User Experience: Graphical passwords provide a more intuitive and user-friendly authentication experience compared to traditional text-based passwords. Users can easily remember and recall their graphical passwords, which reduces the likelihood of forgetting or losing them.

Reduced Cost: Graphical password authentication systems can reduce the cost associated with traditional password security systems by eliminating the need for expensive hardware tokens or smart cards. Users can authenticate themselves using a simple graphical interface, which reduces the overall cost of implementing a secure authentication system.

Flexibility: Graphical password authentication systems offer greater flexibility in terms of customization and configuration options. Users can choose from a wide range of images, symbols, and patterns to create their own unique graphical passwords, which makes it easier to remember and recall them.

Compatibility: Graphical password authentication systems are compatible with a wide range of devices and platforms, including desktops, laptops, tablets, and smartphones. This compatibility ensures that users can easily access their accounts from any device without the need for additional hardware or software.

DFD OR UML DIAGRAMS

Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

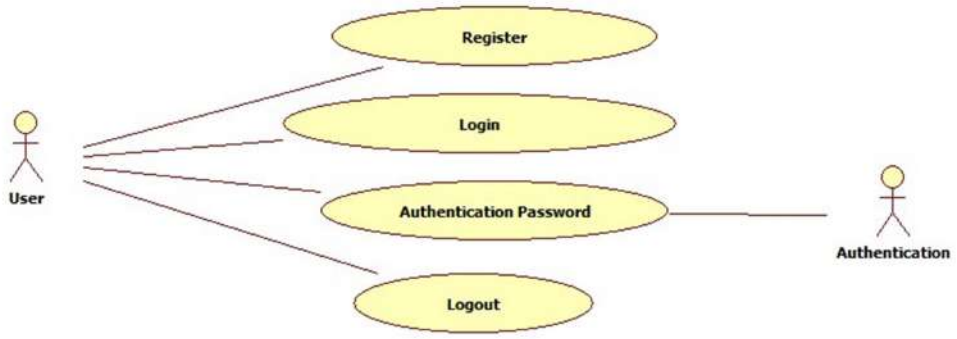

Fig: Use Case Diagram

Class Diagram

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class. Apart from this, each class may have certain "attributes" that uniquely identify the class.

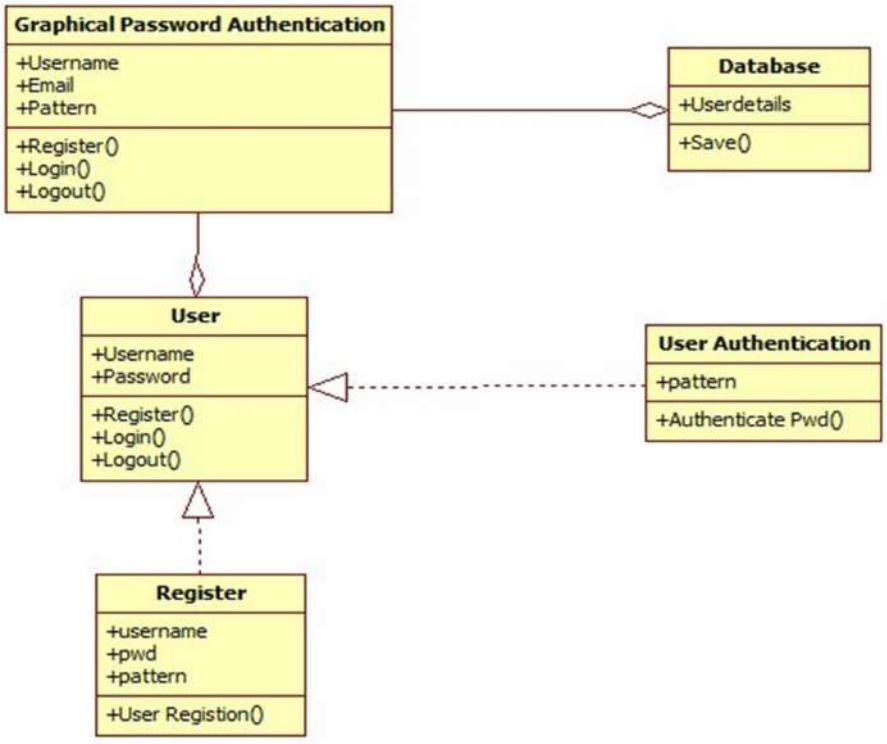

Fig : Class Diagram

Sequence Diagram

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages".

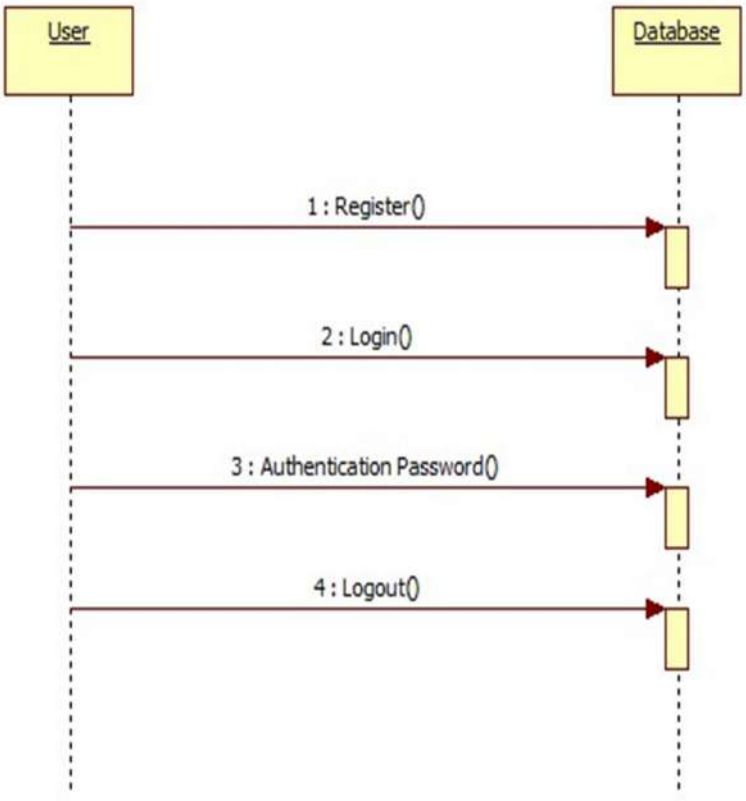

Fig : Sequence Diagram

Collaboration Diagram

A collaboration diagram groups together the interactions between different objects. The interactions are listed as numbered interactions that help to trace the sequence of the interactions. The collaboration diagram helps to identify all the possible interactions that each object has with other objects.

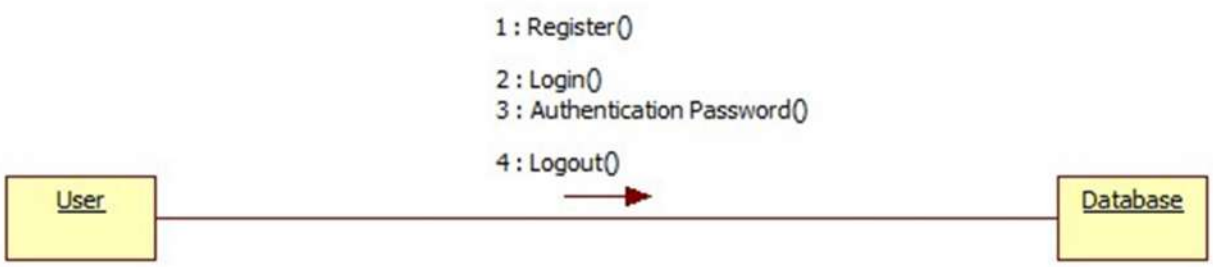

Fig : Collaboration Diagram

Activity Diagram

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

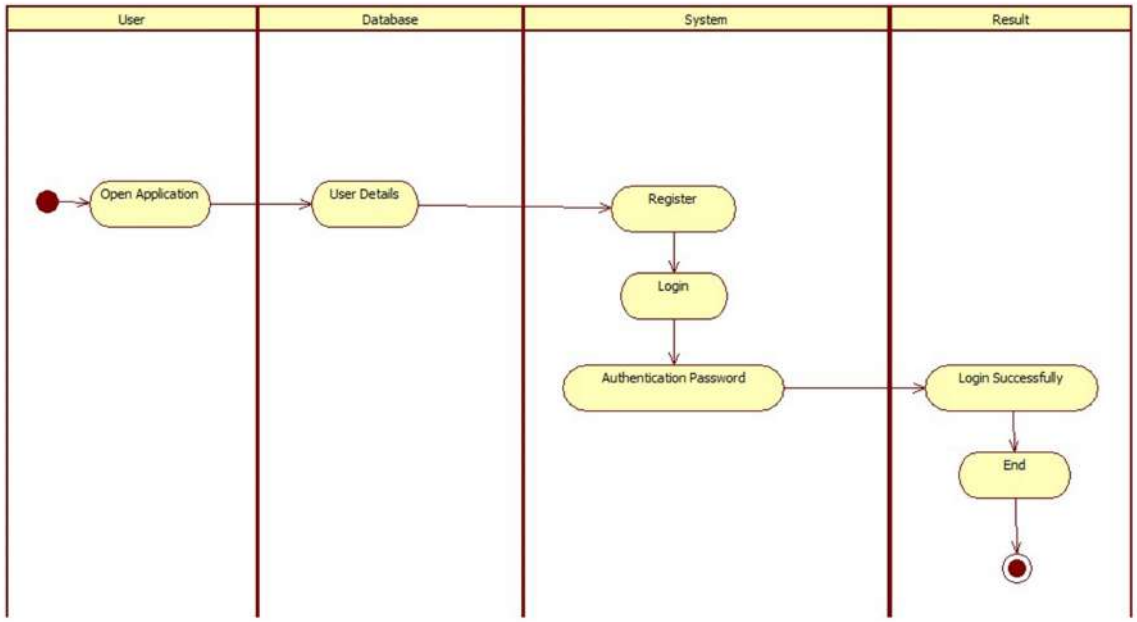

Fig : Activity Diagram

State Diagram

A state diagram, as the name suggests, represents the different states that objects in the system undergo during their life cycle. Objects in the system change states in response to events. In addition to this, a state diagram also captures the transition of the object's state from an initial state to a final state in response to events affecting the system.

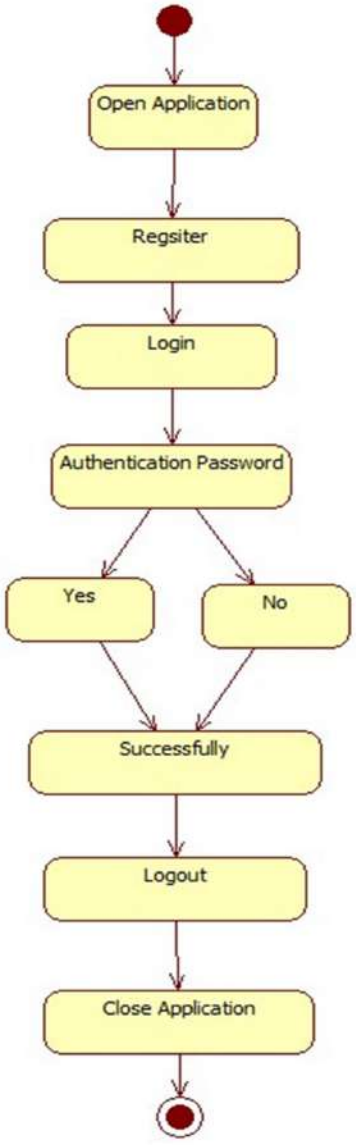

Fig : State Diagram

IV. IMPLEMENTATION AND RESULTS

The chapter tells about the implementation part of the Entity Recognisation. In the codebase, you'll find key components like data preprocessing, where the input text is tokenized, cleaned, and transformed into a suitable format for training. The implementation of graphical password authentication involves presenting users with a set of images, allowing them to select and order the images, and validating their gestures or actions on the images during the authentication process. These steps aim to provide a more intuitive and secure authentication experience.

Output Screens

Main page:

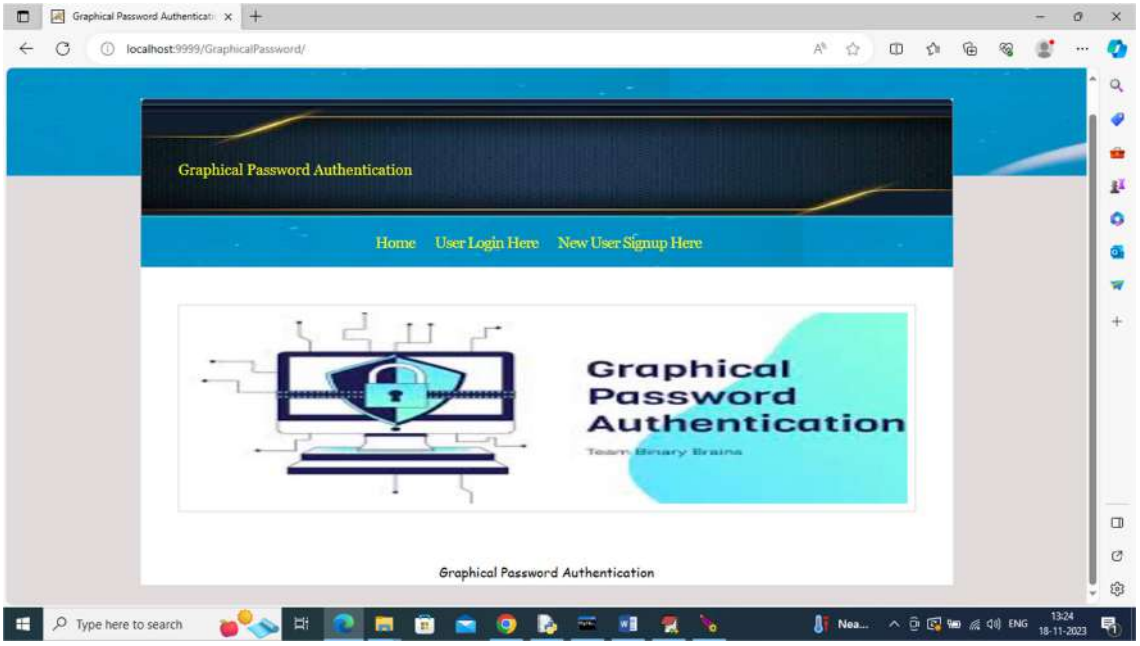

Fig : Output Template

In above screen click on 'New User Signup Link' to get below signup page

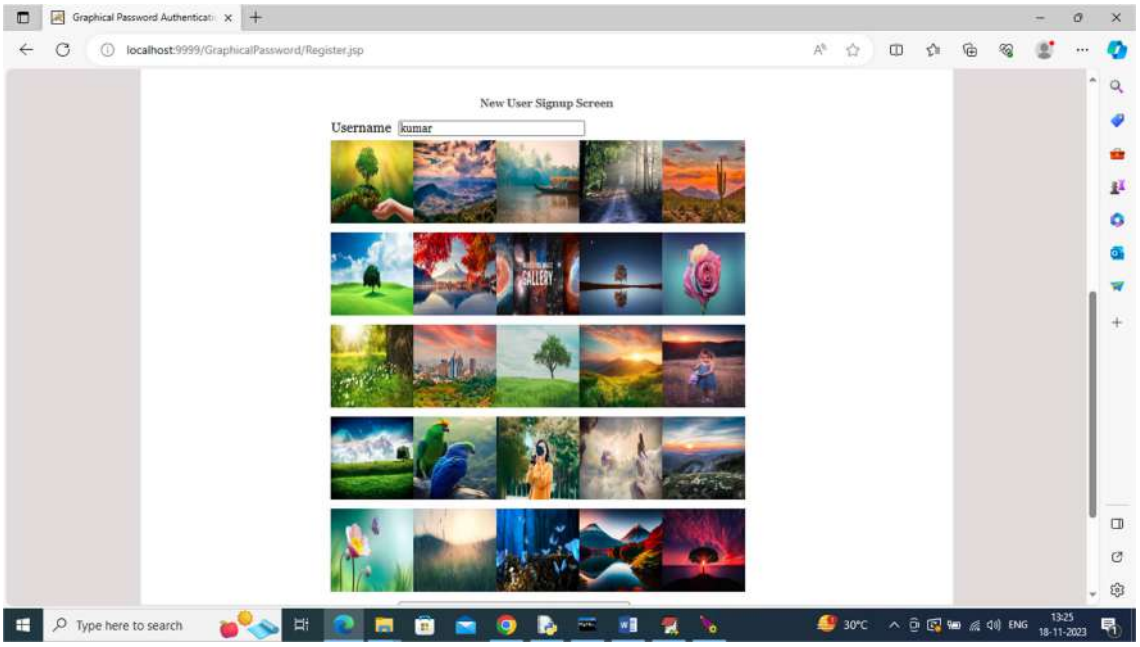

Fig : Output Template of signup page

In above screen for signup user can enter username and then click on desired image to get password like below screen

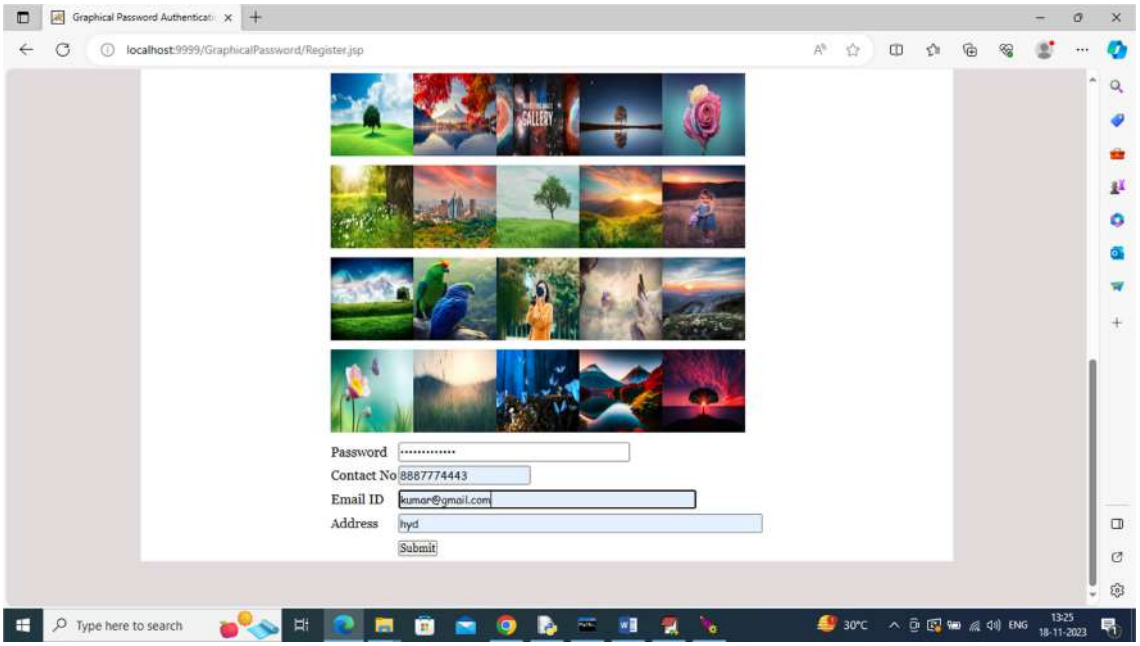

Fig : Output Template for selecting password

In above screen password will be generated automatically when you clicked on image and then enter remaining details and press button to get below page

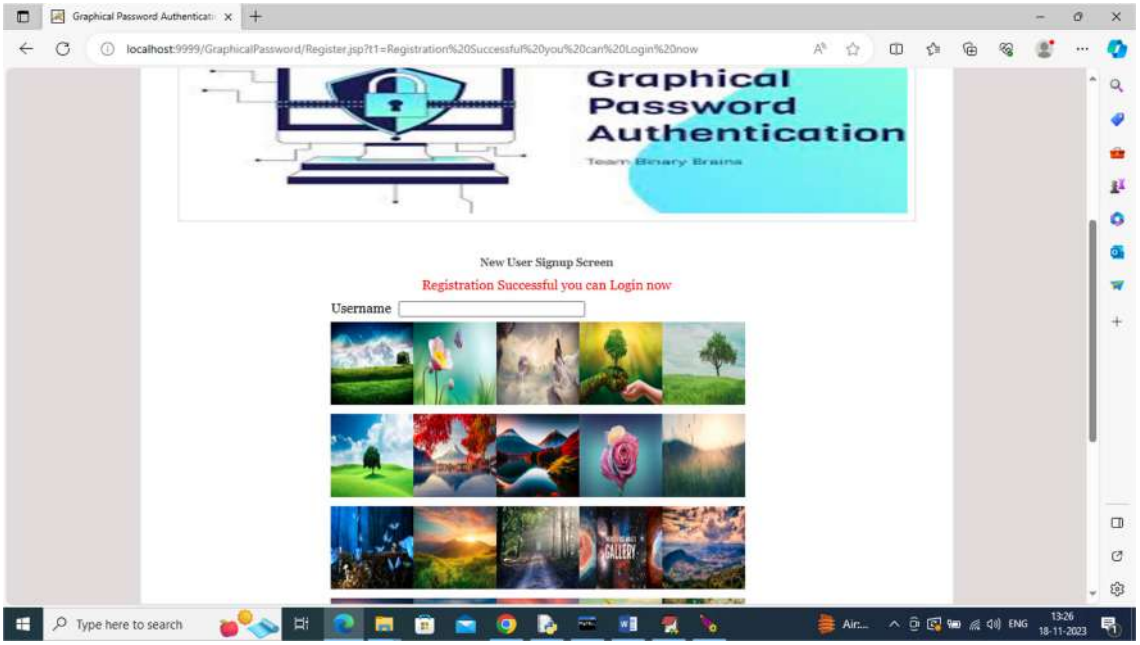

Fig : Ouput Template of Registration successful

In above screen in red colour text can see Registration successful and now click on 'User Login Here' link to get below page

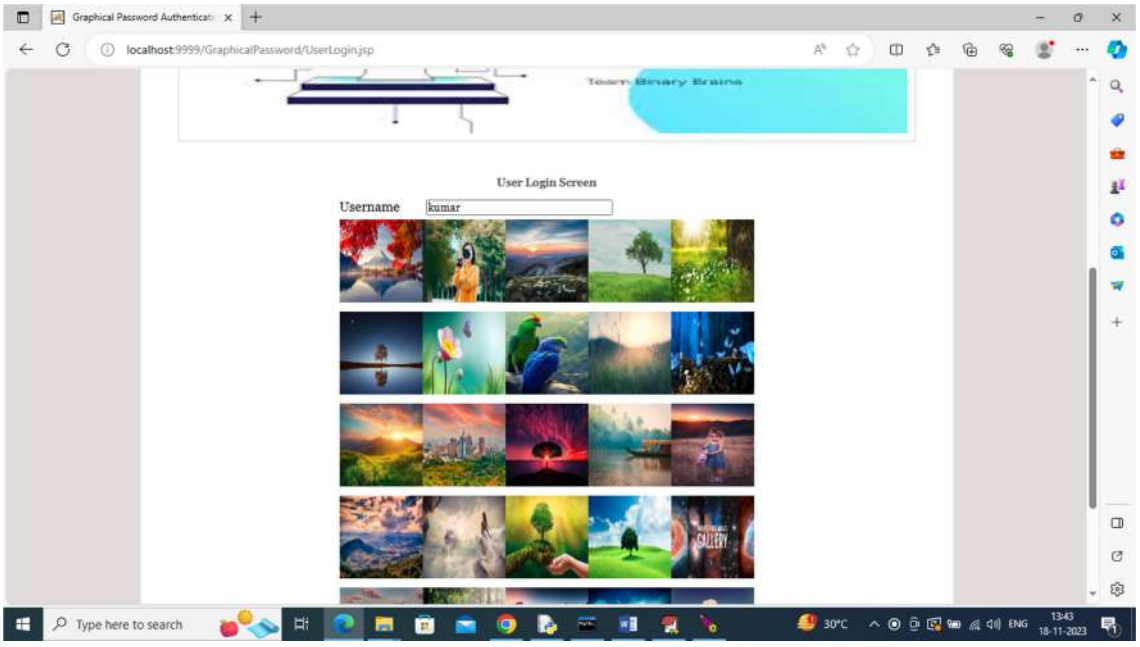

Fig : Output Template of Login page

In above screen to login enter username and then click on correct image to generate password and then press login button like below screen

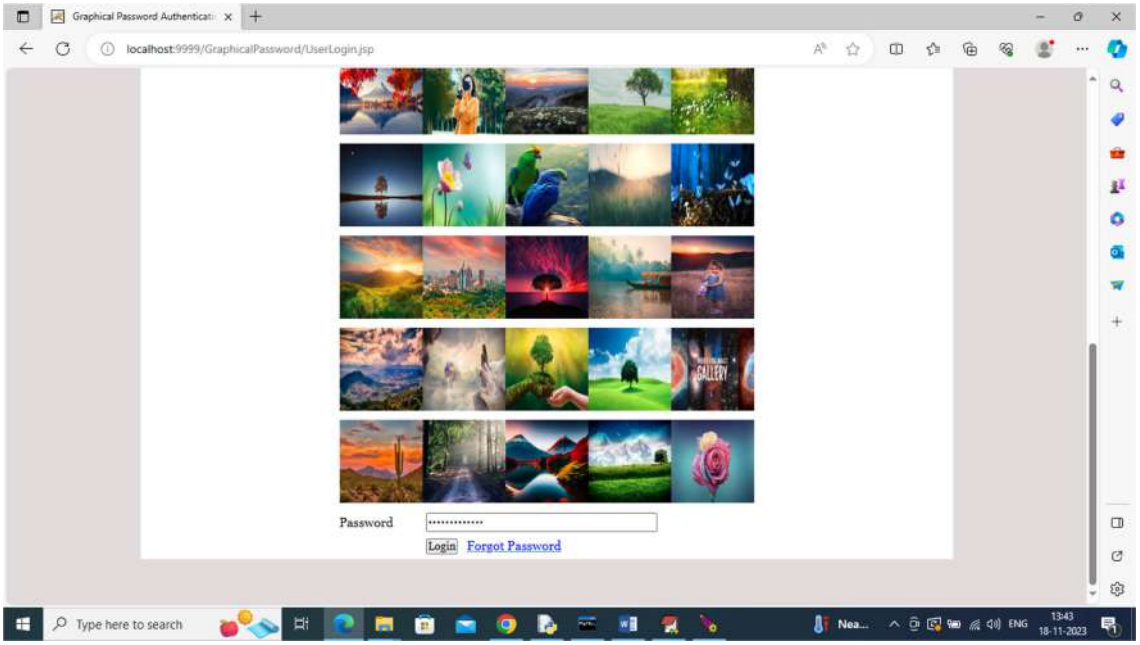

Fig : Output Template of Enter the password

In above screen after clicking on image password is generated and now press 'Login' button to get below output

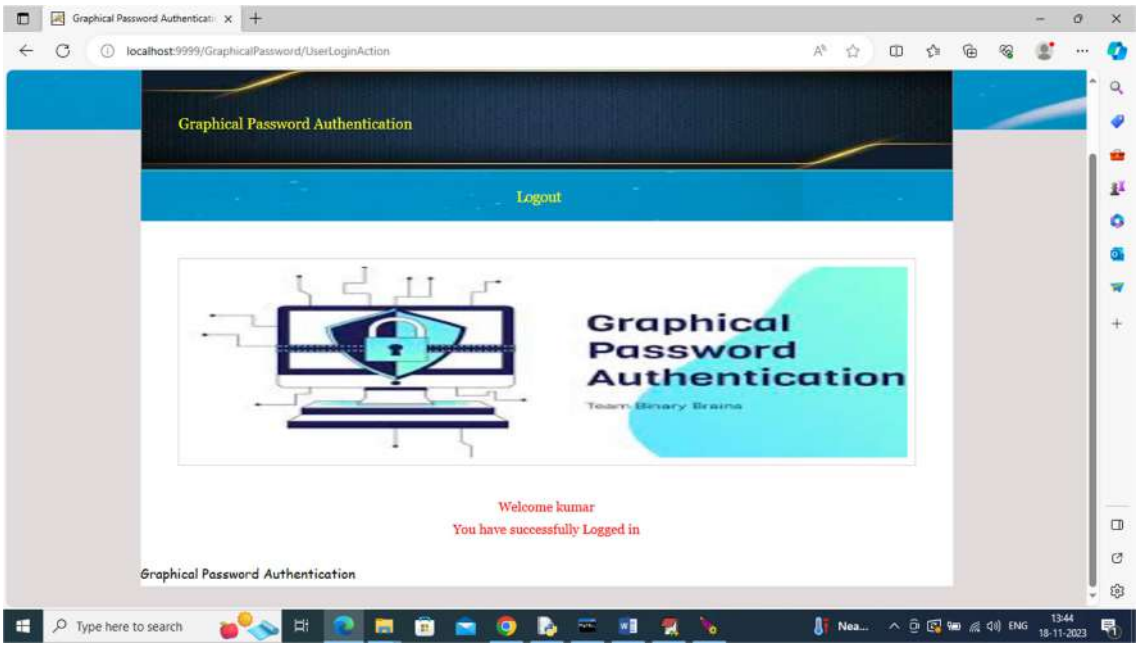

Fig : Output Template of Successfully Logged in

In above screen login is successful and similarly by following above screens you can generate image based password and now in below screen click on 'Forgot Password' to reset .

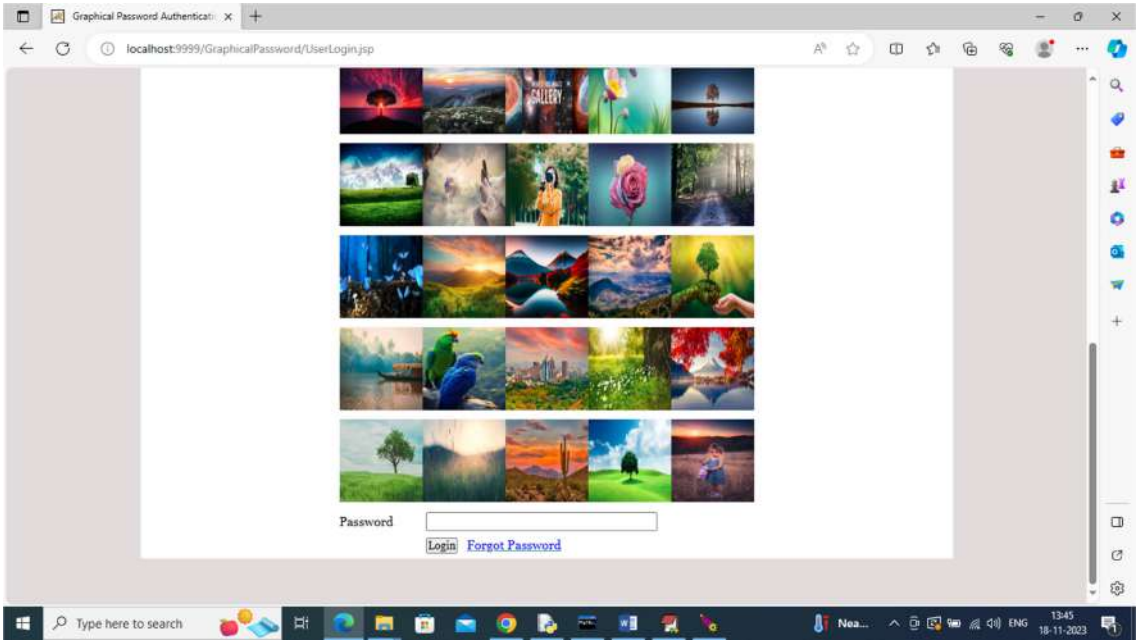

Fig : Output Template of Forgot Password

In above screen click on 'Forgot Password' link to get below page

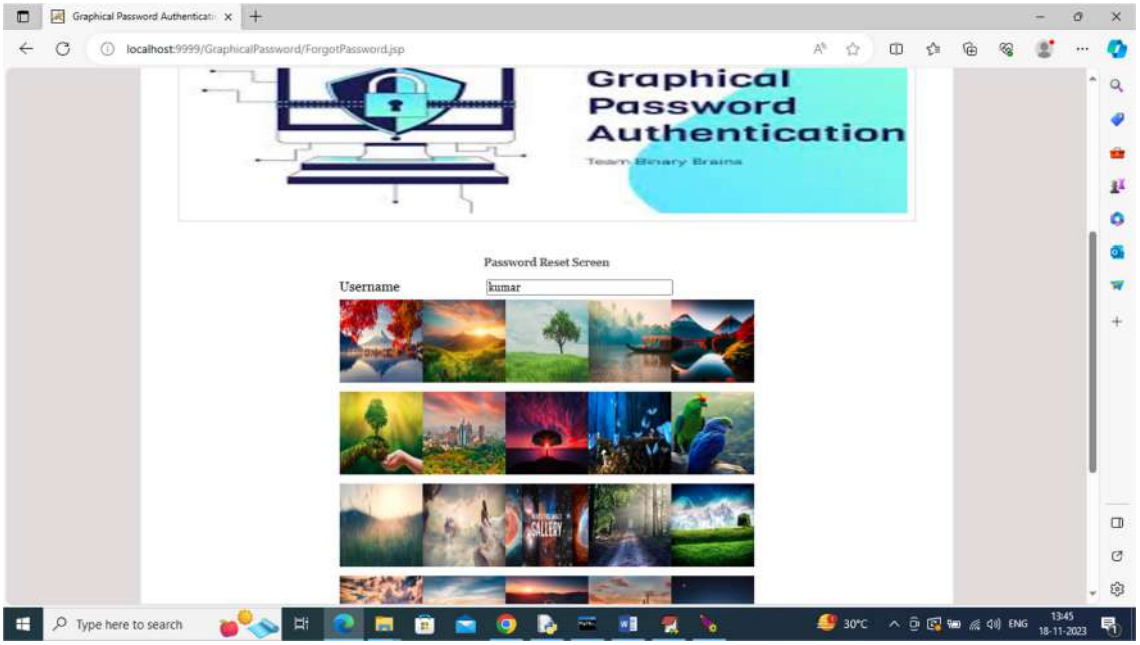

Fig : Output Template of Reset Password

In above screen enter correct user name and then select new image as password to generate password to get below page

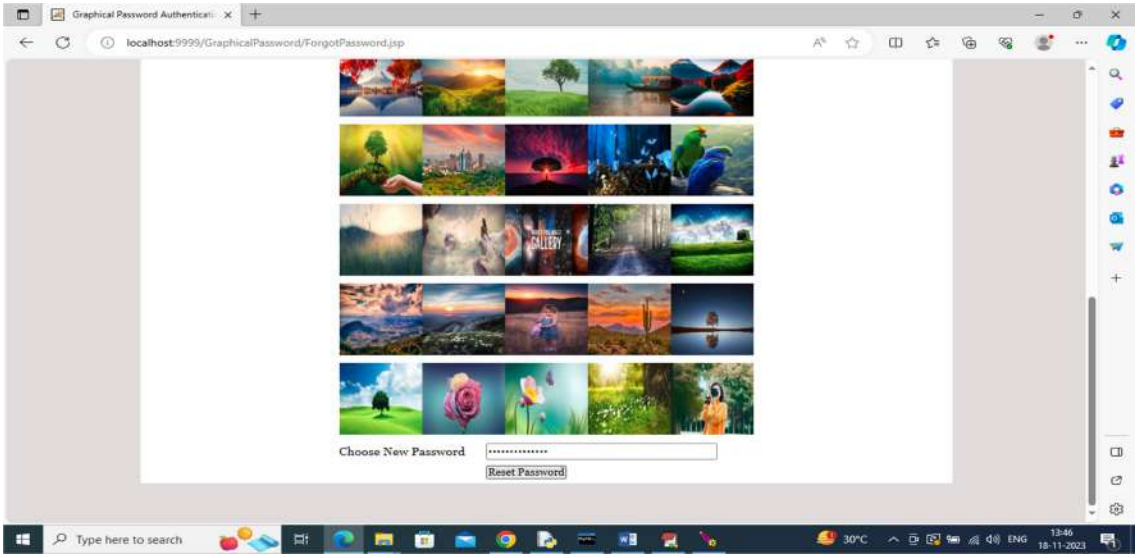

Fig : Output Template of New Password

In above screen password is generate and now click on 'Reset Password' button to get below page

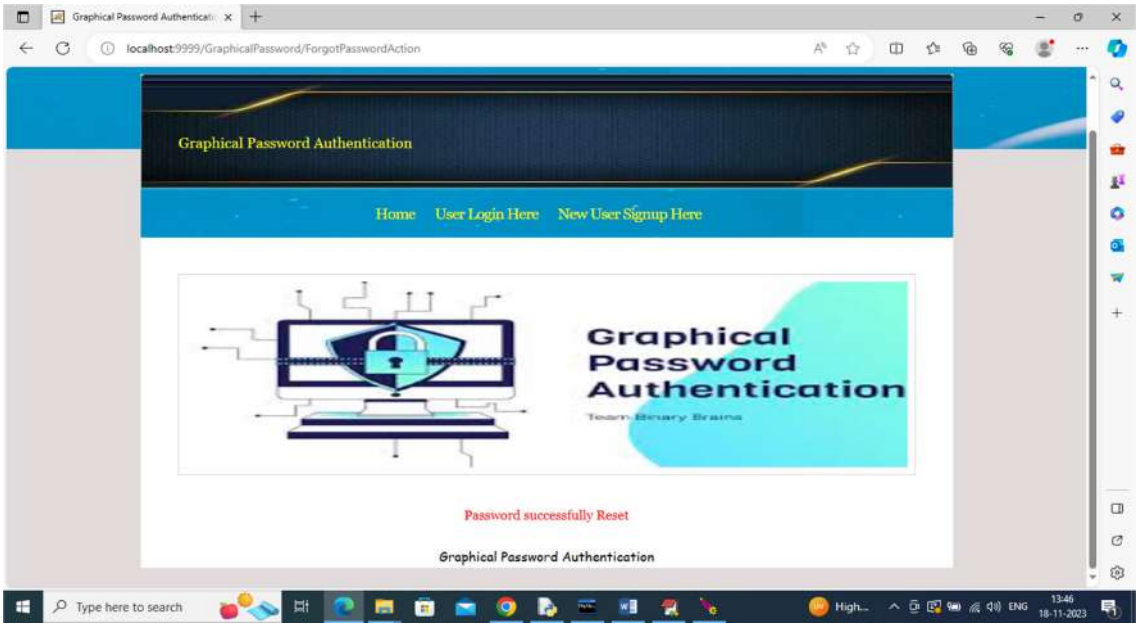

Fig : Output Template of Password Successfully Reset

In above screen in red colour text can see new password is generated and similarly you can generate and resets passwords.

Result Analysis

This chapter provides information about the website's implementation phase. This section provides a succinct overview of the key features that were used to develop the graphical password authentication. It is made up of numerous source codes that were used to create this website. Additionally provides the results of each area, which clarifies the various possibilities available to correctly finish project.

V. CONCLUSION

The Graphical Password Authentication is one step forwarding the paradigm of using patterns for security. Of reasonable security and usability and practical applications Thus the proposed system will be more effective authentication system that provides more security to data and protection against different attack. The authentication system is based on graphical password which provided different pattern based on various difficulty levels. For successful login user selected in the same pattern which is chosen by user during a registration and this system also provides alert message which provides more security to data.

Future Scope

One area of focus is enhancing the security measures to make the system even more robust and resistant to attacks. Researchers and developers are also working on improving the usability and user experience, making the process more intuitive and accessible. Another interesting direction is the integration of graphical password authentication with IoT and mobile devices, enabling secure authentication for a wide range of devices. Additionally, advancements in gesture recognition technology can further enhance the accuracy and reliability of graphical password authentication. Continuous research and development efforts are crucial to stay ahead of emerging security risks and ensure the effectiveness of these systems.

REFERENCES

[1]. M. Alsaleh, M. Mannan, and P. C. van Oorschot, “Revisiting defences against large-scale online password guessing attacks,” IEEE Transaction on Dependable and Secure Computing, vol. 9, no. 1, pp. 128-141, Jan./Feb. 2012.

[2]. X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., “A Novel Cued-recall Graphical Password Scheme”, In sixth International Conference on Image and Graphics (ICIG), pp. 949-956, 2011.

[3]. P. Andriotis, T. Tryfonas, G. Oikonomou and C. Yildiz, ”A pilot study on the security of pattern screen-lock methods and soft side channel attacks”, Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec ’13, 2013.

[4]. T. Kemp,"The Problems with Passwords", Forbes.com, 2011. [Online]. Available: http://www.forbes.com/sites/tomkemp/2011/07/25/thepro blems- with-passwords/. [Accessed: 08- Aug- 2016].

[5]. K. Lai, J. Konrad and P. Ishwar,"Towards GestureBased User Authentication", 2012 IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance, 2012.

[6]. M Anwar and A Imran, "A comparative study of graphical and alphanumeric passwords for mobile device authentication," In MAICS 2015, pp. 13-18.

[7]. Elham Darbanian, Gh. Dastghaiby fard," A Graphical Password against Spyware and Shoulder-surfing Attacks", IEEE 2015.

[8]. J.C. Birget, D. Hong, and N.Memon, "Graphical Passwords Based on Robust Discretization," IEEE Transactions on Information Forensics and Security 1(3), 20016, pp.395-399.

[9]. Jina Marin Bijoy, Kavitha.V.K, Radhakrishnan.B," A Graphical Password Authentication for Analyzing Legitimate User in Online Social Network and Secure Social Image Repository with Metadata. " IEEE-2017.

[10]. Elham Darbanian, Gh. Dastghaiby fard," A Graphical Password Against Spyware and Shoulder-surfing Attacks." IEEE 2015.

[11]. Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng," A Shoulder Surfing Resistant Graphical Authentication System" IEEE-2016.

[12]. Swaleha Saeed, M Sarosh Umar," PassNeighbor:A Shoulder Surfing Resistant Scheme. "NGCT-2016.