

Graphical Based Authentication Using Cued Click and Binary OTP

MSc Research Project
Cyber Security

Umesh Popat Salunkhe
Student ID: x19215169

School of Computing
National College of Ireland

Supervisor: Prof. Imran Khan

**National College of Ireland
Project Submission Sheet
School of Computing**



Student Name:	Umesh Popat Salunkhe
Student ID:	x19215169
Programme:	Msc Cyber Security
Year:	2018
Module:	MSc Research Project
Supervisor:	Prof. Imran khan
Submission Due Date:	16/12/2021
Project Title:	Title
Word Count:	XXX
Page Count:	16

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	31st January 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Graphical Based Authentication Using Cued Click and Binary OTP

Umesh Popat Salunkhe
x19215169

Abstract

In every sector, user authentication is the main factor for security purposes. The motive of user authentication is to provide security and stop being victims of shoulder surfing attacks. Shoulder surfing is a real-world threat that the user loses their data. Over a year, many authentication techniques have been introduced to prevent this attack that may be based on password-based authentication, color and image-based authentication, and token-based authentication. The most used authentication technique is password-based authentication, but it has limitations where the user has to create a password according to the limitation. It causes the user to forget the password. Looking at this concern, the new approach is introduced in this research project. It is a combination of images, click pass, and binary OTP. This authentication will provide multi-layer security in which users can generate a password that is secure and easy to remember. In addition, graphical-based authentication has more chance of being victims of shoulder surfing attacks. The binary OTP is used for secure and successful authentication to overcome this concern.

1 Introduction

1.1 Background

What idea hits into mind when we think about "user security"? Authentication is a factor that keeps the user or the whole organization from getting an account used by an unauthorized person. In theory, authentication is a technique where users enter valid credentials (Password, OTP, etc.) to prove the user's identity. It prevents attacks that lead to data breaches, brute force attacks, or shoulder surfing. To avoid these types of attacks, multifactor is used. Multifactor authentication is a primary security level that helps the user keep the account secure and cannot be unlocked without valid credentials. For example, the user has to prove as a good user. Then the user has to go through the authentication technique such as password-based authentication, biometric, FIDO, graphical-based authentication, OTP generation. In the current world, most users use password-based authentication to keep their accounts secure. The most important thing is that it has password limitations, like password must include upper case and lower case with symbolic characters. But a strong and secure password is hard to keep in mind. If the user keeps the password too easy to remember, the attacker can easily guess the password and take control of the victim's system.(Bošnjak and Brumen; 2019) In addition, password-based authentication has a significant drawback: some application use access

control technique that is not suitable for password-based authentication. To overcome this problem, graphical-based authentication provides secure authentication for users. It is also easy login authentication for users because, as per psychology, the human can easily remember the watch picture compared to the text-based password.



Figure 1: Authentication Techniques

The benefit of using graphical-based authentication is reducing user memory limitation, retaining the complicated password. Graphical-based authentication is also known as image-based authentication. It is divided into multiple systems to provide more secure authentication, such as the Searchmetrics system, Drawn metric system, Locimetric system. In the Searchmetrics system user has to select the fixed images to make a successful login. In the Drawnmetric, the user must draw a registered pattern on the canvas for login. And for the locimetric, the user has to click on the particular point on the selected images. This research project comes under the locimetric system.

This research project aims to develop multifactor authentication using the graphical authentication technique and binary OTP. In this project, a new approach is defined of graphical-based authentication, known as Cued Click authentication using the binary code(OTP). This mechanism helps the user proceed with secure login to the account and prevent them from being victims of a shoulder surfing attack. The password is a click point on the image in this graphical authentication. The Users have to select the three images or system-generated images and click on a particular point on images that the user feels can be easily remembered. While the login phase, the user will click on a selected point, displaying the following correct images. If the user clicks on the wrong point, then the false image will be displayed. In short, right-click right image will be displayed.

Currently, graphical-based authentication suffers from shoulder surfing attacks. In Searchmetrics based system, the user has to select the images in the sequence which are all visible to the screen. An attacker can easily guess the password. So to overcome this

problem, the concept binary OTP is formed. If the value is one, then the user has to click on the right point, and if the value is 0, then the user has to do a false click.

1.2 Research Question

This research concentrate on the victims who suffer from shoulder surfing attack. The research is carried out to overcome this issue, which provides graphical-based authentication by clicking points on the images. This security technique is carried out to protect against the eavesdropping attack, brute-forcing attack, shoulder surfing attack. This research project uses a new approach called binary OTP(0,1).

- Can the graphical-based authentication prevent the shoulder surfing attack?
- Do this mechanism (Cued Click with binary OTP) provide secure authentication?

In this project, the password consists particular point on the sequence of images by referencing the binary one time password. The graphical authentication carries multiple methods like images selection, OTP with the color shuffling, color grid, etc. The authentication used in this research project is Cued Click Image by using Binary OTP. It is a secure and simple mechanism that prevents threats.

1.3 Structure of document

This research project is carried out to get the user or the organization a secure multi-factor authentication against cybercrime. And the deep explanations are given in the following sections. This research report consists of seven sections that elaborate on the project's important information. Section 2 is related work that carries all secure authentication used in previous research to protect users against shoulder surfing attacks and why this mechanism is chosen. Section 3 is the Methodology that will give an overview of the research procedure and techniques used in this project. Furthermore, Section 4 shows the research project's design specification, including project architecture and related diagrams. Section 5 is the research implementation which shows the overall technical solution like the output of the code. Section 6 is an essential part of this project which is Evaluation. It consists of multiple experiments on the proposed Methodology to evaluate the project and expect the required goal. At last, section 7 is a conclusion that gives a reasonable opinion and the desired result, and in addition, it will provide future work of this research project.

2 Related Work

The purpose authentication mechanism will provide secure authentication to the user. In this section, the illustration of the research paperwork has been done of the previous years. It will state the benefits and drawbacks of the earlier years of research carried out.

2.1 Graphical-based Authentication

Graphical-based authentical plays a very influential role in providing secure authentication. It helps the user to remember the password and make login easily. In 2017, the

multifactor graphical authentication was introduced using color code and OTP by Mallaiyah, Shivamurthaiah Sinha. Mallaiyah et al. (2017) In this research project, the user has to give the rating to the colors for the first authentication. During the second authentication, the user will receive the four shuffled OTPs according to the colors and the rating. So, in the end, the user has to enter the received OTP as per the priority set for the colors. Once it is done, the user can login into the account. This research project is carried out for online fund transfers. It is a secure authentication, but the users must remember the color's priority set. If the user fails to give correct input of OTP as per the color priority, the login will get stuck, and transactions will get canceled. To unlock the account user has to set the priority to color again. It looks time-consuming mechanism.

Another authentication technique was proposed by the waller J in 2018. This mechanism was introduced to prevent the eavesdropping attack. This authentication is known as "Zero-Knowledge Protocol" because the user knows the password without authorization (Mohamad et al.; 2018). In short, the user did not send the login password for verification through the network. As a result, hackers will not be able to access the password. During the registration phase, the user has to register the user id, select the three images, and submit it. While the user has to login, the user will enter the user id, and after verifying it, the three random images will appear. The user should click on the "yes" for the password if the selected image has appeared; otherwise, the user must click on the NO button. The system will run a couple of rounds for password matching. If the user answers are correct, then the authentication is successfully done. Like it, another authentication technique was presented by Shah Pintu published the image-based authentication with the grid in 2013, where it showed the combination of image-based authentication and password-based authentication (Shah; 2013). It is multifactor authentication which consists of the user details, images, grid, and text password. The difference between these two authentication techniques is they combined the password with images. Before login, the user has to set the personal information and create a password that includes upper case characters and lower case characters. After this, the second authentication user must select the three images from the 3X3 grid. For authentication, the user has to provide the user id and the password, along with giving the first pass of the image. Pass pictures are distributed at random throughout the login rounds. At any time, any part or all of the images may show. Users must have at least one round of images to combat an intrusive attack.

Image Color Based Authentication System by Johns Hopkins University Baltimore in 2020 Pramod (n.d.). Essentially, the user picks a color sequence along with the pictures. The system to identify phase requires the user to repeat the color sequence on the identified pictures. When switching between pictures, the user must recall the same order without remembering the exact place of the initial few clicks during setup. In the login phase, the user selects the colors with the images. And the most important point in this technique has to draw patterns according to the color sequence. In short, the user has to draw a pattern on the selected images according to the set color sequences like [Red-Green-Blue]. Once the drawn pattern is verified, the user can login successfully.

The recent year authentication mechanism was introduced known as color shuffling with password-based authentication Jain et al. (2017). This technique provides Single Sign-On to the client-side. For user authentication, the user must click on a particular

point on the color. To enter the text password, the user has to click on the specific region of the color. The attacker can quickly examine the password because the attacker can see the password while entering it. To overcome these issues, in the proposed system new technique is implemented by using the images and binary OTP(0,1). It will prevent the attacker from understanding the password and how to do right click? One more authentication was introduced by the Swaroop Phatak, known as the Color shuffling using OTP, where the user has to register the color and email id. It also consists of wheels with divided sectors. That sector includes OTP and the colors. The user will receive the OTP on the registered email during the login phase. The user's role is to shuffle the wheel until the registered color and received OTP will gather into one sector. Once it has been done, user authentication gets to perform.

2.2 Password-Based Authentication

The security of the user authentication procedure is everything in implementing an information system. Password-based authentication has become the most widespread technique since its adoption over 30 years ago. Aside from its popularity, various studies have been conducted to evaluate its safety, management, and effectiveness. Because of human thinking ability limitations, the users choose to use weak passwords, which has long been a drawback of passwords (that is, passwords that are easy to remember but are also quick to crack). Several recent papers have been devoted to explaining the structure of a user password. In 2017, the two researchers(Wantong Zheng, Chunfu Jia) introduced the password-based authentication technique known as password authentication using the separators in between keystrokesZheng and Jia (2017). In this research, the user has to register the user id and password with blanks, and the separator indicates the blanks. It can use any separator that the user selects during the registration phase. When the user has to login, the user must know the password with the blank spots. If the user enters the password, it will be checked and correct, but the blank location is not accurate, then the system will refuse the authentication request. The user has to enter both the password and blanks for a successful login. The module checks the database entry and verifies the password with the blank location. If they match, the authentication is done, or the login fails.

The interesting module called Password authentication code-based RMPN was introduced by the Salah refish in 2018Refish (2018). This mechanism was invented to stop being victims of online or offline cyber attacks. This research project provides the security of session keys and the privacy of passwords. The researcher combined the password with the RMPN, where every login new password is generated as well. Once the account is logged out, the password will also get expire. It means a new session new password—the module RMPN help to send data to the destination on a secure path. In addition, this main research motive is to convert the original password to a new password, and the key is sent to the destination for secure user authentication.

The researcher from the University of the Aligarh invented password-based authentication using the pattern key in 2017Zaki et al. (2017). It is a combination of the password with the texture pattern scheme. At the registration phase, the user will receive the 5X5 grid with the numbers from 1-25, in which the user has to select the location from the

grid for the pattern. Along with it, the user has to register the key-value between 0-9. The key's purpose is to allow the user to match the model numbers in the grid with the key in order to generate a more secure password. To confuse the attacker, the user has to register the dummy values before and after the actually entered password. These mechanisms prevent the shoulder surfing and brute force attack.

Today's world is more active on the social media. To provide secure authentication to it. Sanjeev Kumar proposed password-based authentication in 2017, known as "Identity-based Authentication Protocol Mandal (2017)." This system shows new password authentication with the help of user and server system unique number (Serial Number)—the motive of this authentication technique is to stop the attacks like SQL injection, brute force attacks. The user has to fulfill the personal data (Name, Address, Government Number, etc.). After this, when the server receives the user-sensitive information. The server gathers the details with the user system's serial number, combines the user serial number and server system serial number, and generates a new key.

The authentication will happen by the server asking for the user system serial number for every authentication. There are different password-based authentication introduced in the market by the other researchers. One researcher explained the techniques used in password-based authentication by Martin Drasar Boonkrong (2020). This research paper gives an overview of mechanisms like Plain text passwords, Encrypted Passwords, Hashes Passwords, etc. This technique is used to stop the attacks like Dictionary attacks, brute force attacks, Rainbow attacks, etc. The plain text password is more vulnerable because any user or machine can easily read the password. There are a lot of chances to get to know the user password. To overcome this problem, a new method was introduced called encryption password. In this scheme, the plain text is converted in the ciphertext that the attacker will be unable to see the password. Only the server can read the password. But in the market, there are various encryption and decryption that can easily covert the plain text and get the password to explore. A new technique is introduced to solve this problem called "Hash Password." The password is combined with the key to forming the hash value. It divides the text into multiple sections. It will confuse the attacker to guess the password. It helps the user to keep the password safe.

2.3 Biometric Based Authentication

The use of Biometric-based authentication is used in the IT organization and industries and warehouses for employee authentication. The user authentication is done by using the Finger, Smart card and smartphones sensors, etc. There is some research project carried out to identify the user identity. The smart card is a well-known user identity system where users have to swipe for authorization. The organization provides the smart card. This type of authentication is primarily used in warehouses, Gyms, colleges Park et al. (2016) (Jayapriya and Manimegalai; 2018). But the smart cards can be stolen and maybe get misused it. So to prevent the tailgating attack, the researcher invented finger-based authentication where the user has to register the fingerprint on the system. While authentication, the user has to keep the finger on the fingerprint sensor. As a result, the user will be identified Taralekar et al. (2017). In addition, the new technology authorization is a smartphone sensor that helps users pay and prove for trusted entities (Laghari et al.; 2016).

3 Methodology

A graphical password is a key input into a computer by a user using the computer's graphical information and output devices. Combining images with the texture can be used to generate graphic passwords. In brief, a graphical password is an authentication mechanism that allows the user to select from a couple of images that display in a specific order in the graphical user interface. It will be represented as a password.

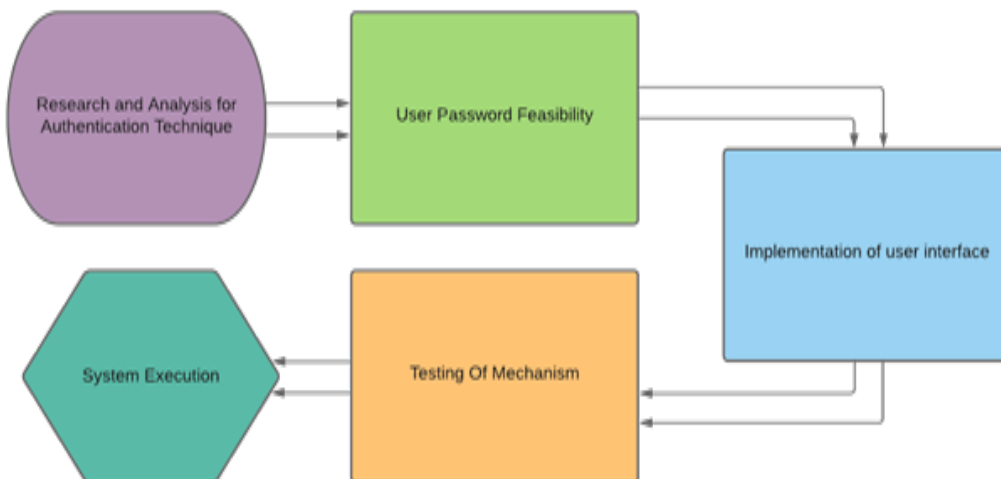


Figure 2: Methodology

3.1 Research and Analysis for Authentication Technique

The introduced mechanism is multifactor authentication. It is a combination of the imaged-based authentication and the OTP. The OTP is in the binary format(0,1). One will represent right-click, and zero is represented as a false click. This project is carried out to give secure authentication to users with the help of a graphical-based password. In this research, the password is a click point on the images. Firstly, at the registration phase, the user has to full fill the data such as user id, name, address, and email address where they will get received. In addition, there is an option given to the user if the user has to select the images from the own system or application-generated system. Once the option is selected, the user has to register the click for three images. At login, the user has to enter the user id, and then the user will receive the binary OTP on the registered email id. by referring to it, the user has to perform clicking on the image. And for the password, the images will be displayed. At that time user has to click on the selected region according to the OTP. For example, the OTP is 101, and then the clicks will be True-False-True. In the same sequence, the user has to do click on the images. If the given click is correct, the following image will appear. The same round will happen for the next two images. By chance, the click gets false the random image will appear. It means authentication is being refused. This project implements the random images if the user clicks on the wrong region. Again the user has to do login for successful authentication.

3.2 User Password Feasibility

According to psychology, the human brain is more attracted toward the graphical thing as compared to the other technique. If the password is too complicated and lengthy, the user will get puzzled and get confused. Then the user performs multiple attempts for login. Once the limit of attempts is exceeded, the account will get blocked. At this stage, the user will face such kinds of issues. So this proposed system will provide a secure and straightforward graphical password by using the images and particular clicks on the image region. The user can easily remember the exact location on the images, and for the binary otp, the calculation of OTP is understandable.

3.3 Implementation of user interface

This is the most challenging stage when the research is carried out for the Implementation. It is a desktop application that will be used for the banking sector, industries, etc. For the Implementation of this application, the framework is used in the research project is "Visual Studio." Visual Studio is known as the integrated development environment(IDE). It is used to design web applications, desktop applications, mobile application. Visual code is to create manage code as well native code. It uses the Microsoft software development platform like windows API, Windows Forms, etc. It allows thirty-six programming languages for project implementation. And the programming language is used for this project implementation is C sharp(C). It is an object-oriented programming language. This language is easy to understand, and it takes less debugging time. And for the back-end, "MySQL" is used to store the data like Name, User ID, Address, Email Id. The chosen images and preserved regions are stored in the database and binary OTP. A brief explanation will be discussed in the implementation section.

3.4 Testing of mechanism

In this stage, the testing is carried out to check whether the developed research project reached the objective and fulfill the accepted result. The testing is performed for the database, compatibility, and system, and validation testing for the username, Click point authentication, login, and password verification time. The motive of testing is to reach the project system efficiency.

3.5 System Execution

At last, after the successful testing result, the project is ready to execute at the user end. This user will register by entering the asked details and required click point on the image. After the registration, when the user tends to login, it will be asked for the username, an OTP will be received on the email, and the user has to click on the selected region on the images according to the OTP. Once the input matches with the registered data, the login is successful, or else the user has to log in again.

4 Design Specification

The given figure will show the architecture of the project. This project is divided into two phases which are the registration phase and login. Every Phase carries its own function to reach the efficiency of the project security. This architecture will explore step by step working of the project. Some components give an idea regarding the entity presented in the project, like the user, login, registration, logs, set of images. With the help of UML diagrams, the work o this project will be explained in the other section.

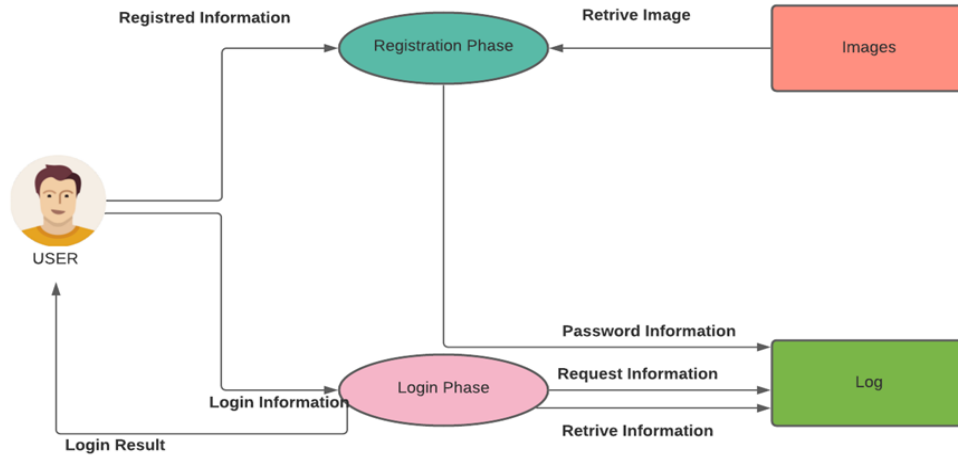


Figure 3: Architechture

4.1 UML Diagrams

UML diagram is the visual language that is used to develop the blueprint of the projects. Although UML is not a programming language, UML diagrams may be used to write code in a number of languages and integrated with object-based analysis and design using UML. The first diagram is the sequence diagram. It is shown in the below figure.

4.2 Sequence Diagram

The sequence diagram is the one the most used UML diagram for software development. It is used to show how the object works together. It illustrates the interactions between the group of objects. There are essential components like object symbol, Activation box, Actor, Lifeline Symbol, etc. In this given figure, the symbols play the following role, and the object symbol illustrates the GUI and the application. The activation box is used for user requests and application responses. The users play the actor's roles. The lifeline is used to represent the continuation of the process till login. The other UML diagram will explain in the next section.

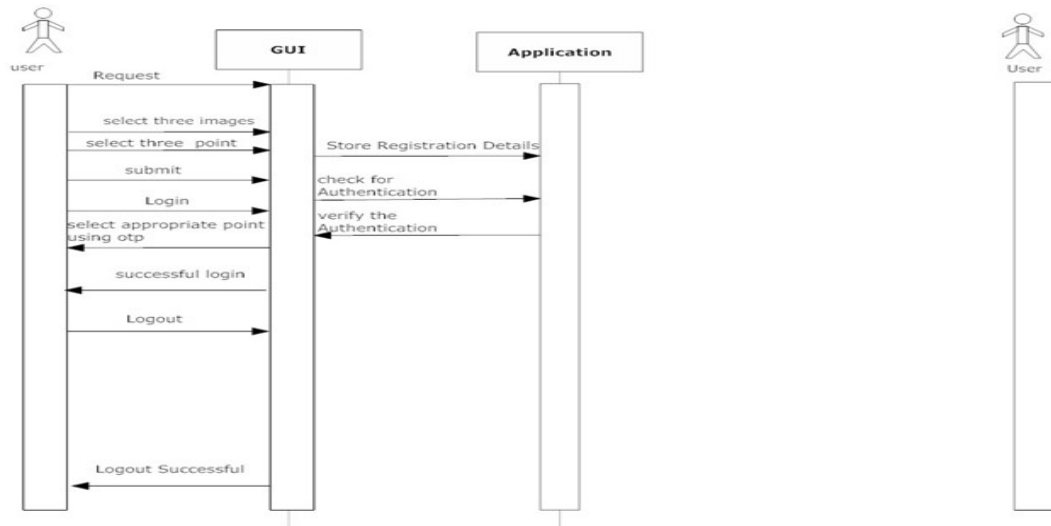


Figure 4: Sequence Diagram

4.3 Use case diagram

The use case diagram's objective is to capture the system's dynamic features. This definition, however, is too wide to identify the aim, given the purpose of the other four diagrams (activity, sequence, collaboration, and StatChart). The user is playing the actor role, and the method is represented by the module used in the project. The brief work of the project is explained in the implementation section.

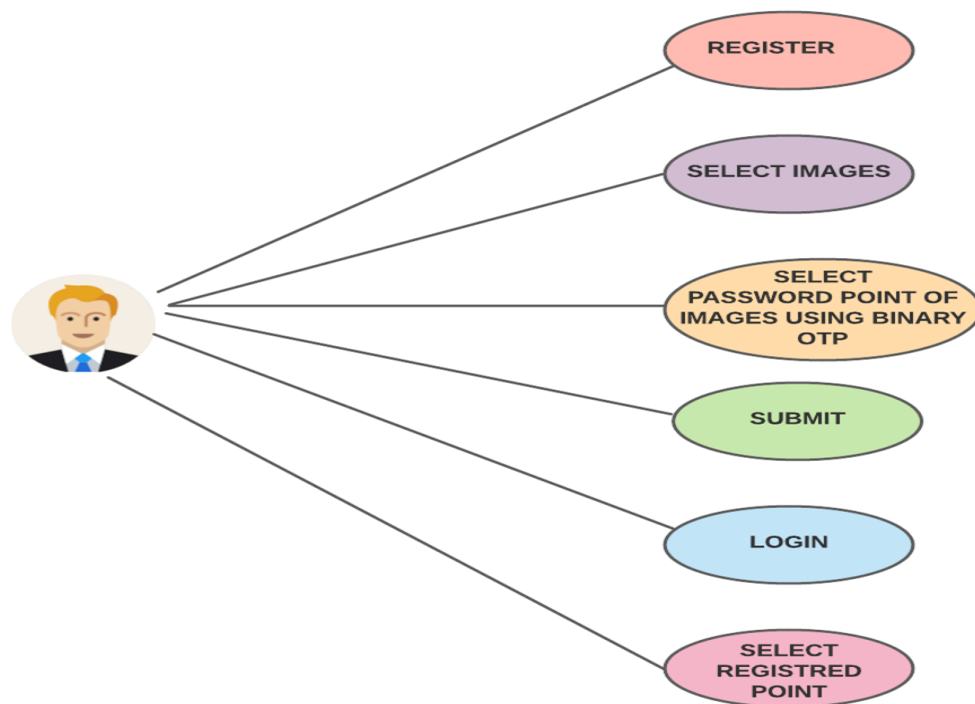


Figure 5: Use Case Diagram

5 Implementation

This research is carried out to provide graphical-based authentication. The module's implementation is done, which is used in this mechanism. To understand the project flow, the figure will elaborate on the work step. This research is mainly focused on the user security and the user password feasibility. The password selection is made into the registration, where the user has to select the particular region on the images. To make it easy, there is an option provided that help user to choose the image of their own system. It will help to remember the user password because the image is selected by the user who is familiar with it. And for the additional secure authentication, the email id is registered to get the binary OTP. The user password will authenticate in the background by referring to the binary OTP. To implement the project, the Microsoft form library is used. This mechanism is divided into three parts: Registration Stage, Login Stage, Rechange the Password.

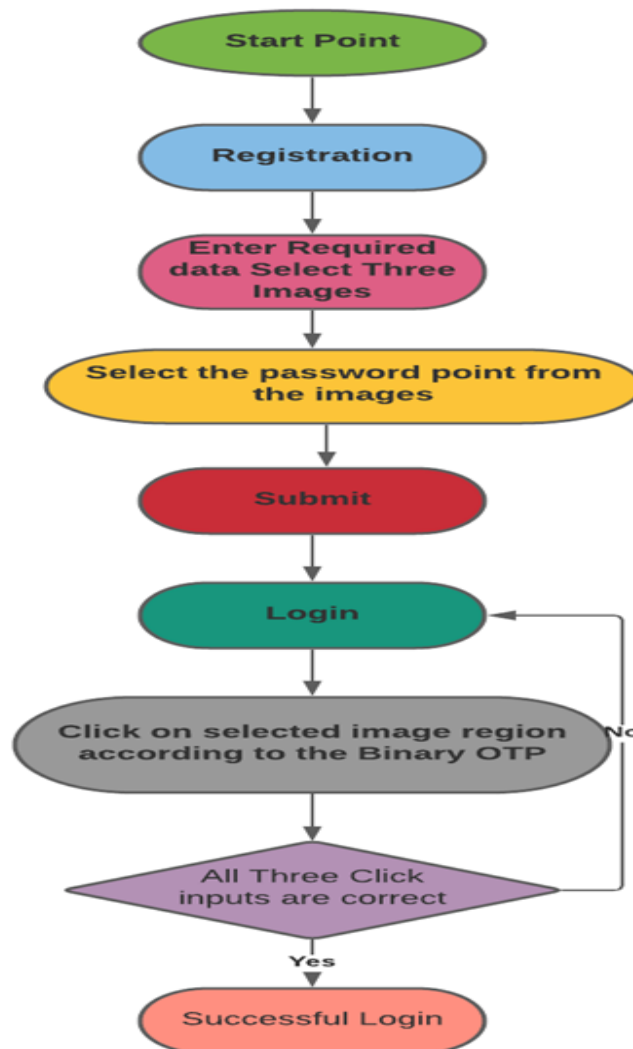


Figure 6: Implementation Flow

5.1 Registrartion Stage

Firstly, the user has to provide sensitive information which it helps them to identify themselves, such as name, username, contact number, email id. On the other hand, the option is provided to the user to select the image, or else the user can do system-generated images. The main thing is that the user must select the images and their click point. For the clicked point, the system provides the red color square. It will help the user to choose the particular region on the image. Once it is done, the user clicks on the register button then the user will receive the one pop-up windows which says that the clicked point is fixed and details are saved.

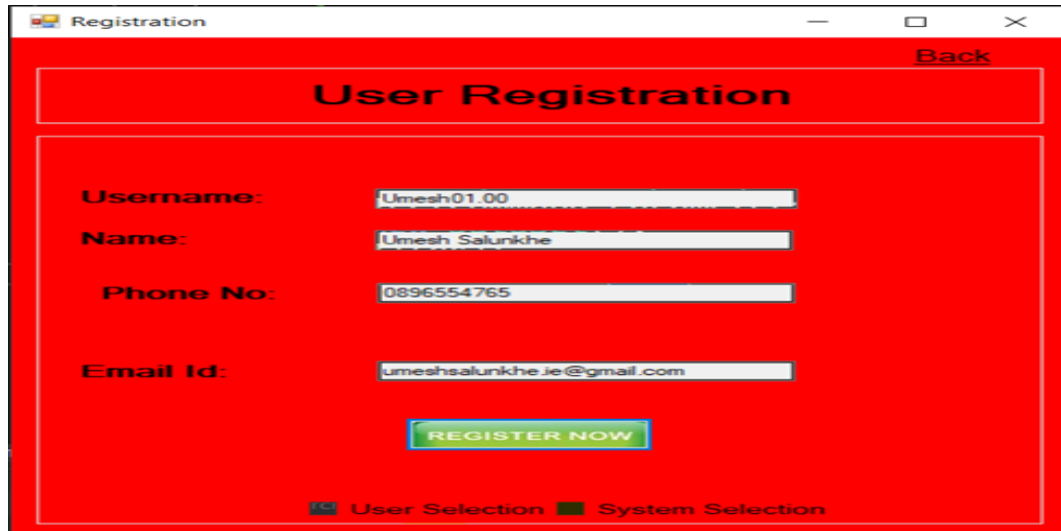
The image shows a web browser window titled "Registration". The page has a red background. At the top right, there is a "Back" button. The main heading is "User Registration". Below this, there are four input fields: "Username:" with the value "Umesh01.00", "Name:" with the value "Umesh Salunkhe", "Phone No:" with the value "0896554765", and "Email Id:" with the value "umeshsalunkhe.je@gmail.com". Below these fields is a green button labeled "REGISTER NOW". At the bottom, there is a legend with two items: "User Selection" with a small red square icon and "System Selection" with a small green square icon.

Figure 7: User Registration

5.2 Login Stage

After the registration stage, Once the user is registered itself, after providing the details and password selection. When the user enters the username and clicks on the start button. Within the second user, the binary OTP of three digits will be received on the registered email address. Three-digit because the three images are used in this project. Furthermore, the image will appear, and the user has to click according to the binary OTP., where one is for the right-click, and 0 is for the wrong click. Moreover, the probability of OTP will be like 000, 111,110,001, and many more. Suppose the user fails to give the correct input according to the binary OTP. The random will have appeared. The expected image will not display when the user gets fails to give proper inputs. Then the user has to click on the start button for another attempt. The user will receive one binary OTP again. The process will happen again until the user gets logged in. In other conditions, if the user forgot the location of the image selected, there are options called to forget the Password.

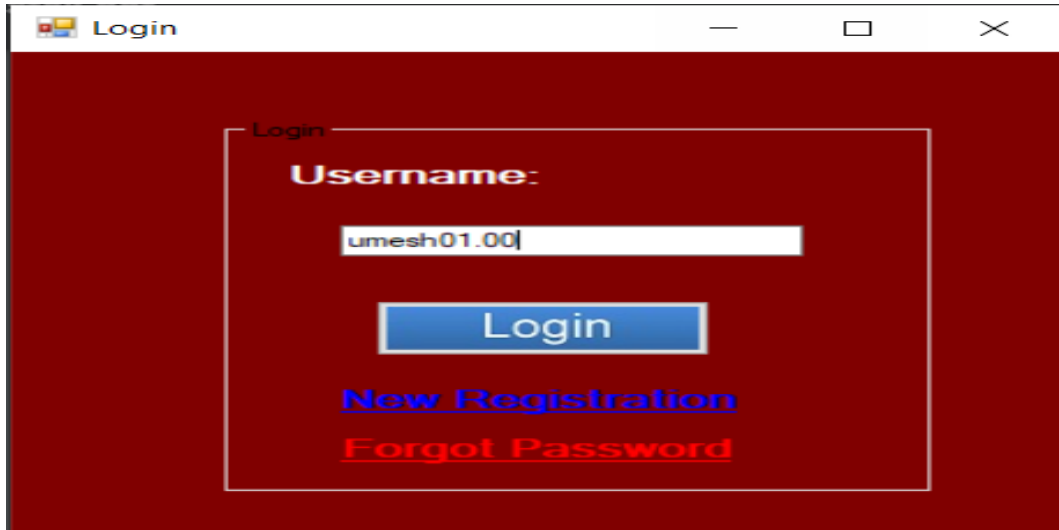


Figure 8: Login Stage

5.3 Forgot Password

When the user wants to change or by chance the forgot the clicked point of the images. Then the user has to enter the username and click on the Password forgot option. It will take towards another section. Furthermore, the user will receive the six-digit OTP on the registered email address for authorization. The OTP is submitted the will be taken to another window and asked to change the report and enter the login details.

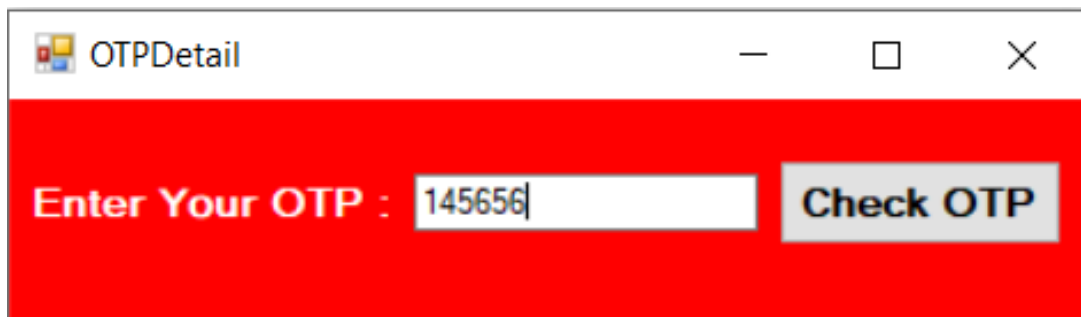


Figure 9: OTP Authorisation

6 Evaluation

6.1 User Authentication Test

The complete the user authentication, the two stages need to be completed. Login stage and registration stage. In this section, the comparison of the multiple user's login and registration is executed. We executed 12 users to register and log in to the mechanism to check the accuracy for successful authentication. It will get to know how many attempts did the user used to complete the whole authentication procedure. The overall analysis of the user login and registration attempts is shown in the figure. The average number

of attempts taken by the user is one, the maximum attempt is 3, and the minimum attempt is 1. After a study conducted on the users shows that after getting familiar with the security mechanism. The count of attempts will drop to the minimum value. This mechanism provides a bit complex password that the attacker will get tricked and unable to guess the password because the password consists of images binary OTP and click pass.

6.2 Security of Mechanism

This mechanism is performed due to the attacks which can spy on the users is and passwords, such as shoulder surfing attacks, brute force, and many more. To check how this user authentication will defend the attacks which are mentioned. We had executed a test with three teams with pairs of two people. One user will login, and another user will perform as an attacker role. This test was performed in three different rounds. As a result of the test, all three teams' users logged in successfully, and the attacker user got failed to know the password. An attacker played characters. Just guess the clicked point of the images. We gave their teammates the user ID to crack the password for the password cracking procedure. However, the outcome of these tests was failed because they do not have binary OTP. If the attacker knows the clicked point of the images and does not have binary OTP, the authentication will fail. According to the test, the percentage of cracking this password mechanism is almost more than 98 percent because the other user failed to identify the password. This authentication will provide security in the real world.

6.3 Time for OTP generation

The above test was conducted to check the ability to survive this authentication technique against real-world attacks. In this section, we will be delivering the OTP generation time. In this research project, we used two otp. First, binary OTP is used for authentication, and another is integer OTP used for authorization. So in this, we will perform a test that tells us how much time it will take to generate for both the OTP. As a result, the authorization OTP max value is 08 sec, the min value is 04 sec, and the average value is 06 sec. Moreover, for binary OTP, the Max value is 05 sec, the min is 03 sec, and the average is 04 sec. This outcome shows that this mechanism is less time-consuming. It helps the user to get fast authentication and authorization.

OTP Generation	Time in Sec(Max)	Time in Sec(Min)	Time in Sec(Avg)
Binary OTP	05	03	04
Integer OTP	08	04	06

Table 1: OTP Generation Time

6.4 Difficult to identified the password

In the previous research, the attacker can guess the user account password. For example, an attacker can identify the password in graphical-based authentication by referring to

the image pattern. Even in password-based authentication, an attacker can find the password such as date of birth, contact number, social media account details, and so on. This research has implemented the cued click authentication approach by using the image and binary OTP. In this mechanism, an attacker cannot find the password or the authentication key because the image with click region and binary OTP is used in this approach. If the user sees a particular spot or an area on the pictures, an attacker will be failed to log in. For a successful login, an attacker should know the image spot and carry the binary OTP and the logic behind it. So this is the significant difference between this research project and the previous authentication mechanism.

7 Conclusion and Future Work

According to various research carried out on user authentication. The most used authentication is password-based authentication and graphical-based authentication. Firstly, password-based authentication is also known as well secure authentication. Most web applications use password-based authentication by using the combination of characters, symbols, and integers. It provides a strong and secure password, but in some conditions, the password requirements are too complicated that the user forgets the password (Kaur and Mustafa; 2019). Secondly, As taking into consideration issues of password-based authentication. The graphical-based authentication is used. It also gives secure and simple passwords. Such kind of authentication is used in the banking sector, restaurants, and colleges. Some researchers invented a technique where it took more time to authentication. It uses multiple image layers and an authentication layer, which puts the user in trouble. (Golar and Khandelwal; 2021)

Both the password-based authentication and graphical-based authentication provided security against shoulder surfing, eavesdropping, and brute-force attacks. Both techniques have advantages and disadvantages. In the proposed system, the issues faced in the password and image-based authentication are tried to overcome. The techniques used are images, binary OTP, click point (Moraskar et al.; 2014). By using this mechanism, the user will easily complete the authentication successfully and securely. Furthermore, future implementation will require limitations for the image click, and the text password will be combined with the images. The password will hide under the image. As a result, the motive of reaching the security efficiency is reached and full fill the user authentication purpose.

References

- Boonkrong, S. (2020). Password-based authentication, *Authentication and Access Control* .
- Bošnjak, L. and Brumen, B. (2019). Shoulder surfing: From an experimental study to a comparative framework, *International Journal of Human-Computer Studies* **130**: 1–20.
URL: <https://www.sciencedirect.com/science/article/pii/S1071581918305366>
- Golar, P. C. and Khandelwal, B. (2021). Graphical-based authentication system and its applications, *Advances in Systems Analysis, Software Engineering, and High Performance Computing* .

- Jain, A., Khetan, R., Dubey, K. and Rambade, P. H. (2017). Color shuffling password based authentication.
- Jayapriya, P. and Manimegalai, R. (2018). Finger knuckle biometric authentication using texture-based statistical approach, *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)* pp. 170–174.
- Kaur, A. A. and Mustafa, K. K. (2019). A critical appraisal on password based authentication, *International Journal of Computer Network and Information Security* .
- Laghari, A., ur Rehman, W. and Memon, Z. A. (2016). Biometric authentication technique using smartphone sensor, *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* pp. 381–384.
- Mallaiah, S., Sinha, S. and R, P. (2017). An authentication for digital transaction with otp using color code systems (ccs), *International Journal of Computer Sciences and Engineering* **5**: 285–287.
- Mandal, S. K. (2017). An efficient identity based authentication protocol by using password, *CompSciRN: Other Applied Computing (Topic)* .
- Mohamad, Z., Thong, L. Y., Zakaria, A. H. and Awang, W. S. W. (2018). Image based authentication using zero-knowledge protocol, pp. 202–210.
- Moraskar, V., Jaikalyani, S., Saiyyed, M., Gurnani, J. and Pendke, K. (2014). Cued click point technique for graphical password authentication.
- Park, Y., Lee, S., Kim, C. and Park, Y. (2016). Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks, *International Journal of Distributed Sensor Networks* **12**(7): 1550147716658607.
URL: <https://doi.org/10.1177/1550147716658607>
- Pramod (n.d.). Icauth: Image color based authentication system.
URL: <https://www.cs.jhu.edu/~pramod/icauth/paper.pdf>
- Refish, S. H. A. (2018). Pac-rmpn: Password authentication code based rmpn, *2018 International Conference on Advanced Science and Engineering (ICOASE)* pp. 286–289.
- Shah, P. (2013). Image based authentication system.
- Taralekar, A., Chouhan, G., Tangade, R. and Shardoor, N. B. (2017). One touch multi-banking transaction atm system using biometric and gsm authentication, *2017 International Conference on Big Data, IoT and Data Science (BIGDATA)* pp. 60–64.
- Zaki, M. H., Husain, A., Umar, M. S. and Khan, M. H. (2017). Secure pattern-key based password authentication scheme, *2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)* pp. 171–174.
- Zheng, W. and Jia, C. (2017). Combinedpwd: A new password authentication mechanism using separators between keystrokes, pp. 557–560.