National College of Ireland

Identity Verification with Integrated Protected Graphical and Text Password

MSc Research Project
CyberSecurity

Anushka Ingale
Student ID: x20125020

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Anushka Ingale
Student ID:	x20125020
Programme:	CyberSecurity
Year:	2021
Module:	MSc Research Project
Supervisor:	Niall Heffernan
Submission Due Date:	23/09/2021
Project Title:	Identity Verification with Integrated Protected Graphical and Text Password
Word Count:	5839
Page Count:	18

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:	22nd September 2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
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.	☐

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):	

Identity Verification with Integrated Protected Graphical and Text Password

Anushka Ingale
x20125020

Abstract

The authentication system is a program that enables users to access the system without having to provide a valid password. There are a variety of techniques available, the majority of which were eliminated following the bot attack, with a few remaining. In other words, as a single characteristic, all existing passwords may be erased. Static passwords are used by users to gain access to standard security schemes, but it is well recognized that static passwords are very straightforward to crack. For users to authenticate their identities, passwords are a necessary method of identification. Text-based passwords are difficult to remember and are subject to keystrokes logging, shoulder surfing, and motion detection threats. Rubic is a system that protects against these attacks by combining textual and graphical password. As a result, the goal of this project is to provide end users with a high level of security. Text passwords, such as passphrase, and graphical passwords are included in this project, which decrease the danger of bots or password cracking. A study of existing password authentication techniques was done in order to create this safe solution. In the development of the technology, use of novel and non-traditional approach was preferred. Because many users considered the most common text-based password schemes to be friendly, the system built here has a simple user interface and provides users with the greatest potential comfort in a password solution, making the system simple with the inclusion of graphical password.

1 Introduction

The logging technique is a means of getting access to a computer system or other device by creating and authenticating themselves using user credentials, which are often a "username" and "password" combination. Recognition systems include question-answering systems that use a combination of pictures as the solution image. Other aspects like as click frequency, object selection over a picture, and so on are taken into account by several research. Some authentication methods support the user's picture or utilize a device-generated random image. This paper analyzes previous work on password, advice and focuses on an observational study that was done to see how effective existing password recommendations are when applied to conventional password policy regulations. Graphical passwords are an alternative to text-based passwords. While graphical passwords are more user-friendly, they have downsides for both the system and the user. Graphical passwords are still susceptible to attacks like shoulder surfing, keyboard logging, and video recording, and so are insufficient authentication methodsSadeghi et al. (2021).

The major issue is that both textual and graphical passwords have flaws and are susceptible to keyboard tracking, video recordings, and shoulder surfing. To provide a safe and quick login procedure, we present a method for a login system that includes both graphical and textual passwords. The merits and disadvantages of existing authentication techniques will be examined and discussed in this paper, as well as our suggested implementation of a secure authentication system. This paper also looked into the usability and durability of the Cued Click Points graphical password authentication method. In the cued click point approach, the user chooses a point on the image he chose at registration, then enters a text password, which if right, successfully logs him into his account. However, with a cued click point, the threat element is that if a person predicts the point based on random selection, the first stage is eventually compromised, which is not secure. As a result, we chose colors that are the easiest to recall factor during authentication. Because there are no buttons added directly to the user interface like previous projects, this method requires the user to use particular keys to rotate the color they pick and choose text password.

As a result, the possibilities of shoulder surfing are reduced even further. While developing this interface, we avoided and contemplated risk like integrating graphical pictures directly, which may be a simple guess to estimate points, as well as solely utilizing text-based passwords and other risks. Apart from just inquiring why they should choose excellent passwords or limiting their possibilities with standard password policy restrictions, it is more convenient to educate people how to create better passwords in simple and engaging methods. Many organizations and systems now recognize the insecurity of passwords, yet the practice of entering in text-based passwords is still extensively utilized to obtain access to sensitive and secret data. We've looked into the various graphical and textual password models that are currently available and how they may be enhanced.

Background and Motivation

The "password dilemma" refers to the present scenario in which many passwords are either weak and easily remembered or safe yet difficult to remember. The problem, according to experts, is not with the security systems themselves, but rather with users who are unwilling or unable to follow security procedures. Human issues such as reliability, memorability, memory interference, and predictability of user demand have not been

addressed in technical solutions to password problems. The shift to functional security and the incorporation of human aspects into device architecture is significant and has a direct impact on the security of the system.

The study is comprised of interrelated tasks in which the prior works are discussed as well as the gaps between the proposed system and the previously implemented works. The literature review part will show how the analysis for the next project was done, while the research methodology and specifications section will go into the procedure in detail. Finally, future work connected to this study is discussed, including how this project may be carried to the next level, enhancing security and overcoming the shortcomings of the existing system.

1.1 RESEARCH QUESTION

The research looks at a variety of attack strategies and evaluates them for client use using security criteria and the most recent attack tactics. To protect against attacks like shoulder surfing, guessing, and brute-forcing, new password-security techniques must be created. This study enhanced the various password method for password security against eavesdropping and shoulder surfing. In this approach, one plan is used to improve the character of another.

Question What effect does the implementation of a dynamic rotation of a password input image for text-based passwords have on the system's login security?

The password is an image-based interface that allows the user to verify their identity by selecting a picture rather than a password. The graphical password includes many interfaces, including one with simply an image and another with several pictures. It can also be cued clicked, in which the user clicks on several or a single point by following entering a text password. Despite the fact that cued click points is a combination of graphical and text-based passwords, brute forcing remains a concernFAZLI (n.d.). The approach suggested in this paper is a hybrid of graphical and text passwords, but with a user-friendly interface and a challenging but simple password entry mechanism that lowers the potential threat seen in prior implementations.

1.2 Research Objectives

Obj1: Instead of alphanumeric passwords, use images as pass-codes to improve memorability.

Obj2: Choose a graphical design that employs the disguising approach to increase learnability.

Obj3: Reduce the time required to log in.

Obj4: Provide protection against shoulder surfing.

The structure of the paper is written in the following format Section 2presents the literature review on the previous algorithm, Section 3 deals with methodology approach in Generation of GUI till delivering service to user. Section 5deals with Design Specification Implementation, Evaluation and results obtained after analysis. Section 7Confirms the results obtained with the objectives mentioned and insights are drawn and also the future work based on the topic is discussed.

2 Related Work

2.1 Importance of password security

After conducting extensive research on the security of textual passwords to demonstrate the importance of password security this study was proposed with an improved authentication system. The authors state that passwords are a necessity in our daily lives, but "passwords frequently remain below the level of active." Most people don't think about how to make their passwords safer. One of the top ten computer vulnerabilities in households and companies is weak or nonexistent passwords.Abuzaraida and Zeki (n.d.) The length of a password and the number of potential characters that must be evaluated are closely connected to its strength. However, it's worth noting that length doesn't automatically imply a stronger password, since it also relies on how the password was generated. An 8-character password that is an easily known dictionary term, for example, is far less safe than an 8-character lengthy password with random letters. While a dictionary attack must search through all potential words in a dictionary, it is still less computationally demanding than a brute force technique, which must examine all possible combinations of letters of a certain length. Several techniques have been developed to assist users in creating difficult-to-crack passwords. A "password phrase" is a phrase made up of letters and digits. It has been demonstrated that mnemonic passwords improve the security of the original password. Other safe techniques, such as two-factor authentication and biometrics, have also been proposed to improve the authentication process's security. While these approaches increase security, "their cost and complexity of implementation continue to be obstacles to adoption. They basically use more resources to implement than standard textual passwords and are far more difficult to make ubiquitous. Text-based passwords will continue to be the most common method of authentication until these disadvantages are reduced to an acceptable level or eliminated altogether. Strong text passwords are less vulnerable to dictionary and brute-force attacks, but they are still vulnerable to more sophisticated attacks like shoulder surfing, video recording, and keyboard logging.

2.2 Revisiting Password Rules

It's tough to come up with a textual password that's both strong and easy to remember. While the "password phrase" technique stated above is a good start, there are a few more criteria to follow in order to create a strong textual password.Veras et al. (2021) Password length must be at least eight characters, words must be unique, password storage must be secure, passwords must be changed on a regular basis, system generated passwords are encouraged, and distinct passwords must be used for different systems. Users who follow these guidelines when creating a strong password are more likely to generate one that is difficult to remember. Passwords will not be able to survive shoulder surfing attack even if they are strong textual passwords. "If a peeper is present when a user enters their password in a public place, it will be compromised." Video recording is a more sophisticated approach that includes attackers capturing the user's password using video equipment. The user's punched keys, as well as the positions of mouse clicks, may be captured in this recording. A malicious keystroke logging device can be implanted into

the hardware of a keyboard in a keystroke logging attack. Keystrokes on the keyboard can be recorded and timestamp with this device. The attackers can check the log for passwords used during authentication after retrieving the device. Strong text passwords protect users from dictionary and brute force attacks, but they are readily forgotten and decrypted by more sophisticated methods such shoulder surfing, video recording, and keystroke logging.Ocko (2021) The experiment's findings demonstrate that password cracking techniques and technology have advanced more faster than password security standards, and that entropy in the form of length is the most secure way of password protection.

2.3 Evaluation of attack resistance

While the Internet benefits us in a variety of ways, it also comes at the cost of reduced privacy. As a result, every company, social network, and other platform is attempting to improve security in order to improve privacy. Authentication techniques that are commonly used are vulnerable to a number of attacks.Jiya et al. (2021) Because certain systems are ideal for stand-alone solutions while others are good for online environments, users should apply the security and authentication technique according to the circumstance.

Recognition Based Algorithm	Resistance	Non-Resistance
Pass Face	Brute Force, Guessing, Shoulder Surfing	Dictionary, Social Engineering
Dejavu	Brute Force, Guessing, Shoulder Surfing	Dictionary, Social Engineering
Triangle	Brute Force, Guessing,	Dictionary, Shoulder Surging Social Engineering

Figure 1: Examination of attacks in recognition based techniques

Pure Recall-Based Algorithm	Resistance	Non-Resistance
Blonder	Brute Force, Guessing, Shoulder Surfing	Dictionary, Spyware, Social Engineering
Passpoint	Brute Force, Guessing, Shoulder Surfing	Dictionary, Spyware, Social Engineering
Background DAS	Guessing,	Brute Force

Figure 2: Examination of attacks in recall based techniques

Cued Recall-Based Algorithm	Resistance	Non-Resistance
Passdoodle	Dictionary	Brute Force
DAS	Dictionary, Guessing, Shoulder Surfing	Brute Force, Spyware, Social Engineering

Figure 3: Attack resistance in techniques based on cued-recall

According to research, graphical password methods are more secure than traditional textual passwords also are more precise and trustworthy than textual passwords. DAS is the most practical and user-friendly of the methods investigated, but it is not safe owing to its limited password space.Figure 1 Figure 2Figure 3 Is adopted in this study for an attack-resistant algorithm. Although the grid selection approach solves the problem of DAS's limited password space, it is not user-friendly relative to its complexity. In terms of Déjà vu, the login and registration phases get tiresome as more pictures are handled. Passpoint and grid selection methods are more secure and dependable, although Passpoint has the drawback of not providing resistance to Spyware attacks. The proposed registration approach intends to deliver an effective and user-friendly login experience, as well as a simple and quick graphical password. This is about establishing security for system authentication and validation as efficiently as possible in order to minimize shoulder surfing. The major goal is to create a safe and effective validation that is also resistant to surfing. When compared to findings for pure recognition, pure recall, and cued recall based, the core problem of shoulder surfing remains unsolved, with the increasing frequency of a Brute Force attack.Subangan and Senthooran (2019) This technique's strength is that it changes position of numbers each time an authentication session occurs. The significant advantage of utilizing graphical passwords is that they're easier to remember than passwords based on text. It will also be used to log in using these recalled passwords as a criteria. In short, the issue of shoulder surfing and brute force attacks are minimized and certain security improvements are achieved. This eliminates the risk.

2.4 Multiple password interference in text passwords and click-based graphical passwords

We have looked for the security of graphical passwords in order to find safer password authentication mechanisms. "Graphical techniques are intuitive and offer greater password possibility than text-based solutions," states the author. This makes it easier for attackers to recall and devise graphical passwords. Two kinds of visual password systems exist: systems based on recognition and on retrievalGokhale and Waghmare (2016). Password based on icons are used in recognition-based systems to help users remember and identify their passwords, whereas retraction-based systems let users to execute authentication actions. During authentication, recognition systems displayed randomly generated symbols on a screen and required users to select them in a predetermined sequence. Similar approaches were found in which users chose a chart and consecutive points on the graph. Users had pre-selected regions in a series of systems during authentication, whereas in

some systems users had written phrases or picturesChiasson et al. (2007). Furthermore, some systems required users to draw a picture on a touchpad with the proper pressure before repeating the accurate authentication technique. During login, users organize it on the same screen. The difficulty was that it retained the password drawn, leaving it vulnerable to threats, and there was also the possibility that the user might forget itBhand et al. (2015). And, regardless of how accurate the turns and shape are, if the information given is inappropriate while using the matrix form, the authentication will be rejected, resulting in login failure. Furthermore, restricting oneself to only a subset of the available symbols can drastically reduce the strength of the passwordHafiz et al. (2008).

Another attempt by Vaibhav Godbole to protect the login system with a graphical password while making it more difficult to use using the methods outlined belowBehl et al. (2014). The bigger image is shown in a 9*9 grid, which also incorporates the smaller images. The user can write a textual character from within the pass-square region rather than using the mouse. These are the characters that make up the session-pass-characters. As a consequence, the last input might be a mix of session pass characters and clicks. The initial click is in the midst of the k1, k2, k3, and k4 pass-square. The second click takes place within the pass-square formed by the digits 2, 3, 4, and 5. The third click is in the center of the k3, k4, k5, and k1 pass-square. The fourth click is located in the center of the pass-square formed by the digits 4, 5, 1, and 2. The fifth click is located in the central part of the pass-square formed by k5, k1, k2, and k3. The proposed approach employs a visual login methodology that takes into account the strengths and limits of most devices while still providing a robust method of user authentication. It also emphasizes appealing features of a trustworthy authentication system, such as resistance to shoulder-surfing, hidden-camera, and malware attacks. Although this technique provides multilayer authentication, it cannot be considered effective because validating each combination takes a lengthy time, despite being reliable. Attackers would have a higher chance of clicking within the right regions if the size of each pass-square area is too large. 2014, Behl et al.

Given the aforementioned authentication mechanisms, the approach could undoubtedly be improved. Shoulder surfing is not totally safe when using buttons on the screen since attackers can easily see or record the password being entered. Even if an attacker does not know a user's password or color, he or she can videotape the login process and successfully log in as the user by pressing the exact same buttons as those shown in the video. Also the placement of the letters and digits should not remain constant during each login attempt for the system to be vulnerable to keystroke logging. Furthermore, the procedure of rotating the wheel and selecting letters or numbers with a mouse and a button on the graphical interface should be avoided to make the system less vulnerable to shoulder surfing attacks.

We carefully weighed the merits and downsides of different techniques and algorithms before opting to adopt this methodology using Python, which looks to be successful and secure, after reviewing all of the preceding articles and evaluating their thoughts and comments.

3 Methodology

Figure 4: Methodology for the system

Passwords continue to be a significant type of authentication due to considerations such as accessibility and security. People with a limited capacity to recall complex passwords are more likely to pick simple passwords that can be rapidly guessed, making the adoption of password composition guidelines necessary. Even with increasing password length and complexity, many attacks remain unaffected. It is essential to improve user acquisition because this technique will be utilized by individuals login into their accounts. This is a critical parameter for improving human-computer interaction so that the system is not only convenient for the user but also sophisticated in design, making it user-friendly. Below is a thorough explanation of Figure 4.

Strong password research and analysis:

The necessity of passwords, certain components of password security and vulnerabilities, are frequently overlooked. Tests were conducted to assess the resistance of passwords of various strength to brute force attacks, as well as studies that show a strong link between the difficulty in guessing and the password quality. The study is carried out in order to comprehend an adaptive and effective assessment of password strength, which is also mentioned. This study helps to reduce the harm caused by individuals looking to disclose sensitive digital informationSalem et al. (2016). It offers ways to make password cracking more difficult as well as persuade people to change their passwords.As a result, a thorough examination of passwords was conducted in order to offer users with secure passwords.

User's feasibility consideration in task:

Because the system will be used by individuals, it is important to take into account the convenience and memorability of the system. It is quite easy to construct a long and difficult password containing unusual characters, but the chances of everyone recalling the password are very lowTam et al. (2010). Instead, passwords should be designed those are easy to remember and recall, such as a user's favorite sport, activity, or color. In light of this, the suggested solutions centered on the creation of a user interface that required the user to select his favorite color.

Design and implementation of GUI:

In the study conducted here, activities in a GUI are accomplished by directly altering the graphical components. We utilize the Tkinter GUI library because it offers benefits such as the ability to execute applications written in Tkinter on Windows, Mac OS X, and Linux. We need python installed before we can use tkinter, therefore python 3.8 was used for this experiment.Tkinter was used to construct a basic layout window. The

form was created by experimenting with the various widgets available in the Tkinter toolkitChaudhary (2013). Once that, place function was utilized to add various widgets to the application window, and then constructed a pop-up window to show the results after the submit button was pushed. The functionality of the program entails running suitable callback routines in response to a certain type of event.

GUI testing:

Individuals employed the system, and the results were estimated based on factors such as usability, security, failure rate, login time, and brute force attack protection.After reviewing previous results, testing becomes required since the adjustments made in earlier experiments did not entirely resolve the concerns, therefore the system is tested to ensure efficiency.

Delivering service to user:

After successful and favorable test results, the system is then delivered to the user for implementation.

Tools: 1. Pycharm Edition 2020.2.2

Programming Language: Python 3

Algorithm for Secure Authentication

Step 1: User credentials, such as username and password, are entered by the user.

Step 2: The user is logged in to the system if the user name and password submitted are correct.

Step 3: The system now has more security than earlier systems, where the color of the sector rotated but the character stayed fixed, while now the location of letters and symbols changes with each login.

Step 4: If user enter the wrong username or password, user will get an error message and a pop-up box with invalid login credentials message.

Limitations

The model's constraint is the use of restricted colors, words, and numbers, as well as the exclusion of a special symbol, which can be considered in future implementations.

Strength

When the user rotates the color, it is difficult to tell which color is rotating because all colors move in the same order. The letters and digits in the wheel also change positions after each login, adding to the system's security.

4 Design Specification

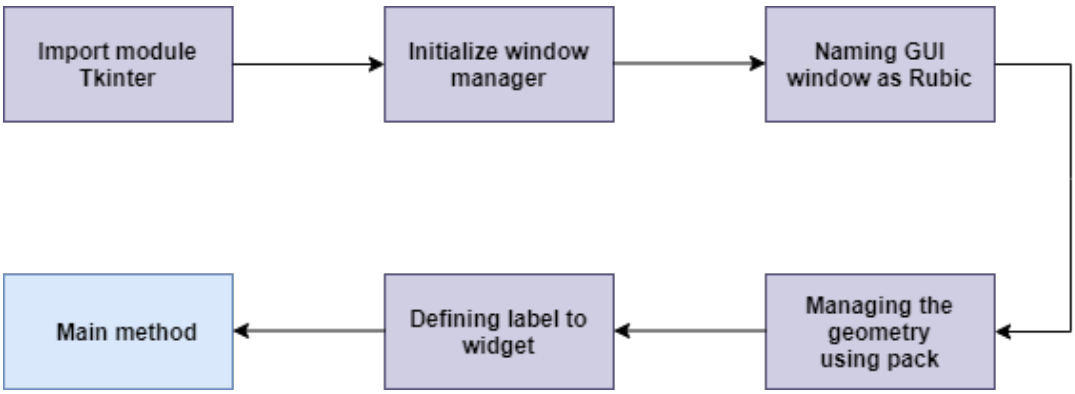

Figure 5: Structure of design

Rubic is a Python program that uses Python's graphical user interface toolkit, Tkinter. In earlier systems, the user rotated the wheel and selected numbers or letters by pressing buttons. This system employs the keyboard characters "c", "a", "i", "o" to give a more distinct login procedure. Logging in has become much faster since the usage of a mouse has been eliminated. Figure 5 depicts the project's overall designLin and Zhou (2018).

Keypress handling for when user selects keys for inner or outer area of sector, slice class and wheel class:

1. The method additionally randomizes the letter, number, and color positions on the wheel, removing any indication of a pattern. As a result, effective shoulder surfing attacks are less likely. Python is an object-oriented programming language, so the routing between three separate modules and windows is controlled by the Main class. Each of these "windows" is also a separate class with its own set of methods that define the activities to be taken on that particular page. The Register module is where a user establishes an account and chooses a username, password, and color. This module saves each user's credentials to a text file and checks for duplicate usernames. Log In module has methods for dealing with keyboard input.

2. The crucial and difficult task was to color the sector of the wheel, along with list of two characters on the wheel, for which classes were created: slice and wheel.

3. A slice list, the preset colors and the characters to be assigned for each section is included in the Wheel class. It has features that called the draw functions for every slice and updated the wheel after every rotation. The entire wheel is replicated in the Wheel class.

5 Implementation

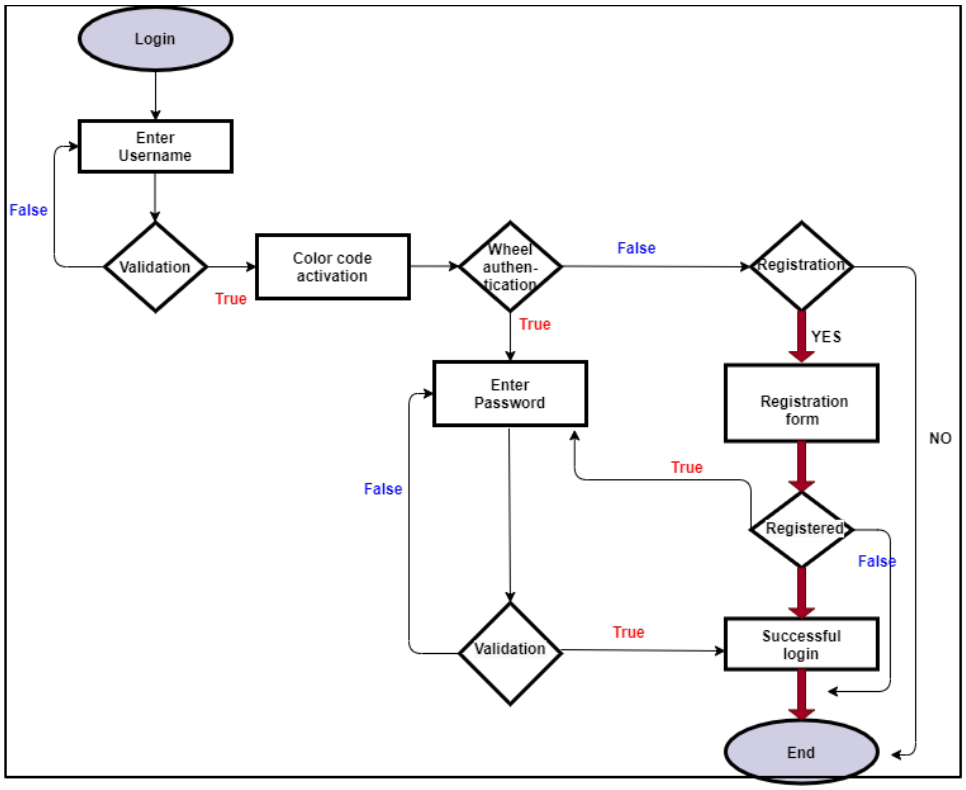

Figure 6: Flow of implementation

This study proposes a password technique that combines text and pictures to avoid shoulder surfing.The flow of the password authentication mechanism in this study is depicted in the diagram Figure 6. There are two essential elements to consider when creating an authentication mechanism: the first is security, and the second is simplicity of use. During the registration process, users create a password based on a predetermined range of letters and numbers, exactly as they do with this authentication technique. A color can alternatively be selected from a menu of options displayed on a wheel of colors, number, and letters. Inner and outer circles are used to display the numbers and letters. The colors of the wheel spin together while text is constant. Depending on the location of their initial letter or number, the user punches the "inner orbit" or "outer orbit" special keys. The letter and number of the user's password are obtained by spinning the wheel using the color they choose at registration, thus we discuss the implementation method and flow of the suggested system in this part. We require Python version 3.x to do this and illustrate the actions and results at each stage.

LOGIN

1. After completing the registration process, the user may log in. This is the first stage of authentication, where the user enters their username and password, which are then verified with the credentials entered at registration. The user interface of the rubic system's login page is depicted in the image below.

2. In the login procedure, the user must use the same user id as when registering, and he should utilize special keys for his password. This is the hardest bit, when the user must employ the color of his choice to enter the password he supplied at registration.

3. The user must select the appropriate shade in order to rotate the sector in the proper order to access the password's beginning and subsequent letters.

4. The spinning of the wheel is unrestricted. The wheel can be rotated in any direction by the user.

5. To input a password, the user must use the special keys "c" and "a" to rotate the wheel, which displays the color, numbers, and characters. The letter "c" rotates the wheel clockwise, whereas the letter "a" rotates the wheel anticlockwise as per Figure 7.

Keys that have been used:

i) c = for clockwise rotation of the wheel
ii) a = anticlockwise rotation of the wheel
iii) i= for selecting a letter/number from the inner sector
iv) o = for selecting a letter/number from the outer sector

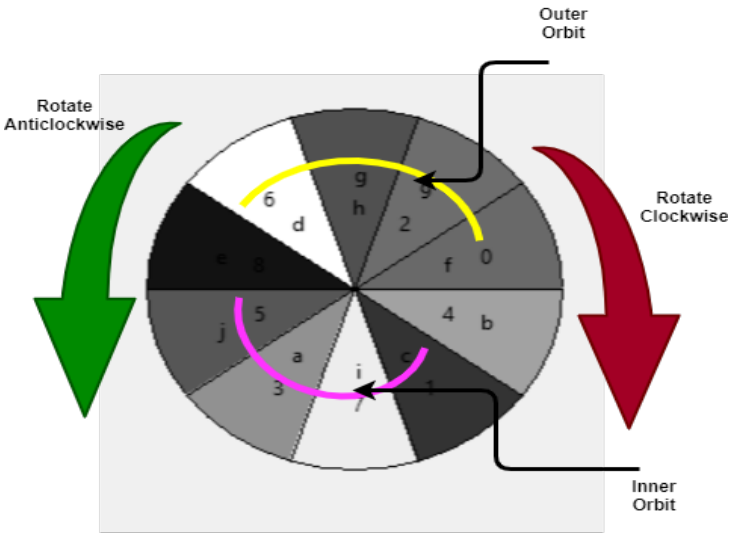

Figure 7: Use of special keys

6. To get to the first letter or number of his or her password, the user must spin the selected color. Carry on with the following set of numbers and letters in the same manner.

7. After reaching the digit or letter, the user should use the special keys "i" and "o" to choose digits or numbers from the sector depending on their position.

8. The key "i" indicates the sector's inner portion, whereas "o" represents the sector's outer part. As a result, the user inputs the password letter by letter, word by word, using these specified keys.

9. Since all of the words or characters typed are displayed with a "*", the password is not visible after it has been entered, ensuring security.

Entering the relevant user id and password and striking the submit button will either result an another pop-up window displaying as shown in Figure 8, informing the user if they were successful or unsuccessful in their login.

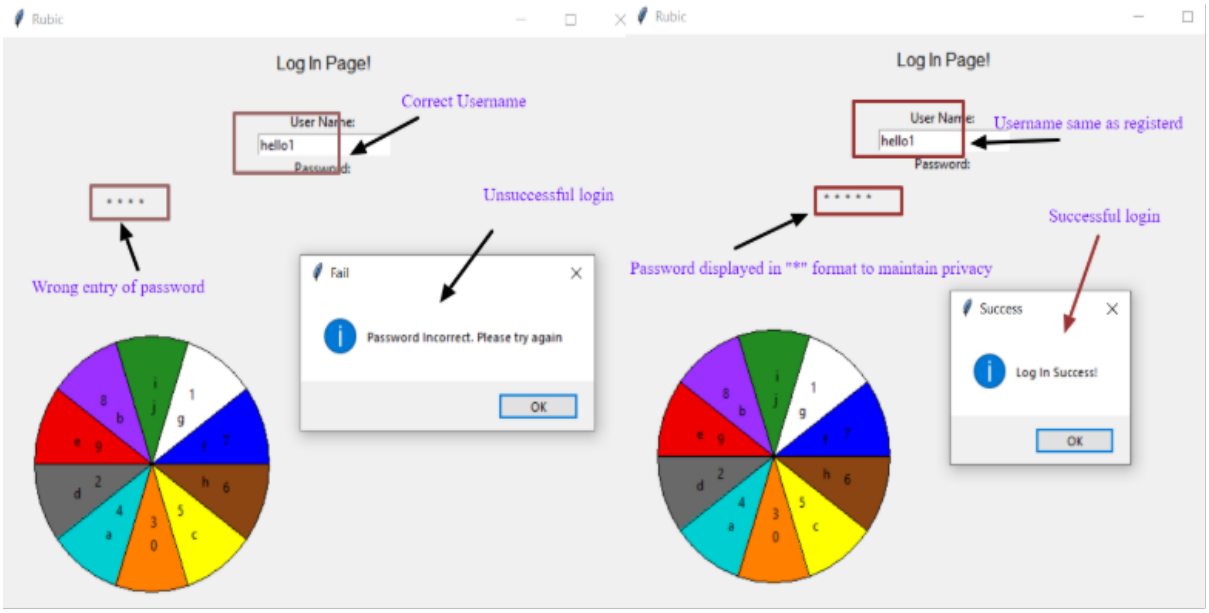

Figure 8: Successful login and Unsuccessful login

REGISTRATION

1. For the first stage, the user must provide his or her user id and password.

2. During the registration process, the user's password options are limited to numbers and letters(digits 0-9 and characters a-j.). The user must select a unique user-id as well as a color from a drop-down menu.

3. After selecting a color, the user must generate a password, complete the registration form, and then submit the form.

4. The password must be remembered for the next time the user logs in.

5. When an user clicks the register button, they become eligible to access the web application services.

6 Evaluation

The findings are compared and recorded down to assess the performance of the suggested approach against the alternatives. The proposed approach ensured a safe login simply changing the location of the number and letters, as well as the color of the sector, after each login, rendering all parameters untraceable.

Even though the system limits the number of characters and digits that may be used in a password, the approach it is utilized in the password process makes it difficult for an attacker to guess it.

1) Login and Registration test (Authentication speed)

We executed a second test with the same 16 participants, this time as users, to see how efficient our system is. They were required to log in to the system in order to see how long it took them to log inEveritt et al. (2009). The analysis is mentioned using the login timings of the previous attempt and the present one in Figure 9 and Figure 10. This analysis is crucial because fast authentication provides another layer of security to the system. This layer of security protects the system against a shoulder surfing attack. Participants used six-character usernames and passwords, such as "creat1" and "corv42," and even chose their preferred colors. The time it took participants to log into the system was recorded in order to check the findings.

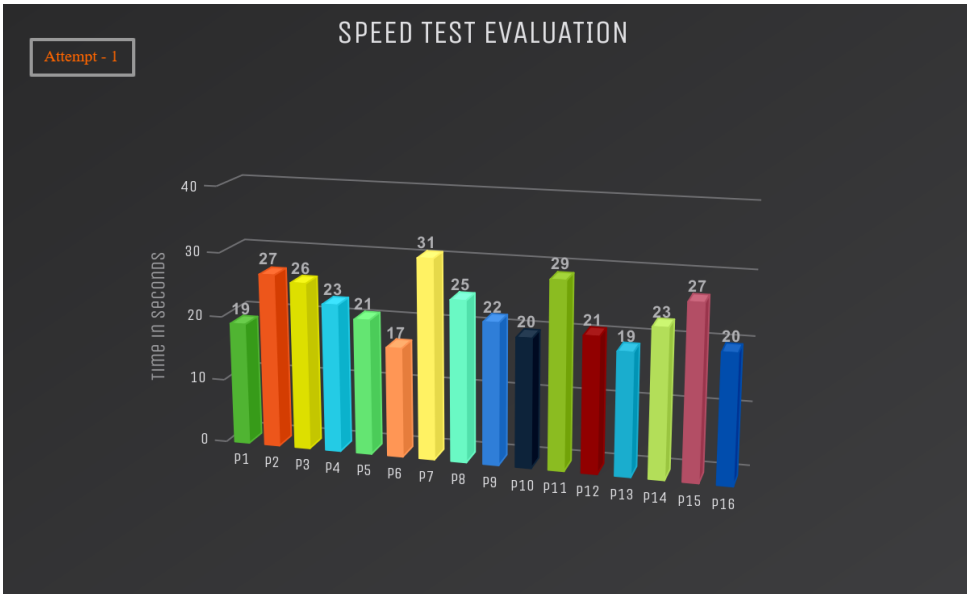

Figure 9: Speed test evaluation for first time login attempt

Users must re-register or login because the system does not provide an erase option. Participants took about 19 seconds, 26 seconds, and 21 seconds on their first try, and 16 seconds, 27 seconds, and 19 seconds in their second attempt. Based on the above mentioned research, it can be concluded that if users utilize this login process repeatedly, the time it takes to log in will drop, making the system more efficient.

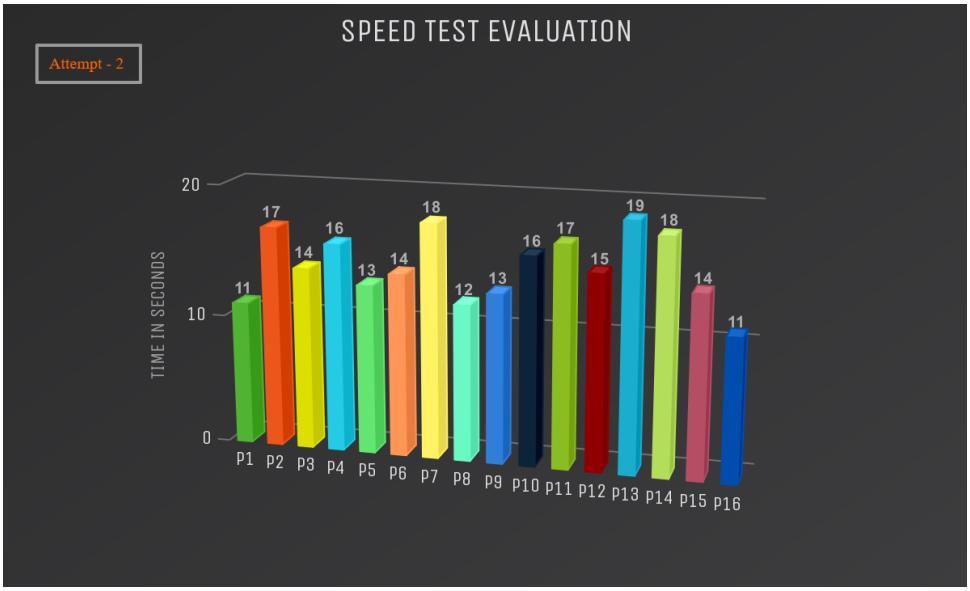

Figure 10: Speed test evaluation for second time login attempt

Because the system's login method is tricky, it's also protected from keystroke login. It's called complicated because the colors, characters, and numbers change positions after each login, making each login have a distinct traceable root for the same login and password.

2) System security check

We had 8 people login to the system to test the security of our password, while the other 16 people watched them while they followed the login procedure. In order to crack the password, spectators not only observed but also recorded the login procedure. People who were witnessing the procedure in real time were unable to crack the password; in fact, none of the 16 people who were there were able to crack the password. After watching the video several times, one of the participants was able to crack the password. However, the chances of breaking it are next to none. There are a total of 10 * 20n (let's call this number X) permutations of passwords and colors that a user may generate with a password of length n and our system supporting 10 colors and 20 characters. This implies that a user's password is one of X options. In the worst-case scenario, attackers would have to try 32000000 passwords for a password length of 5Everitt et al. (2009). Based on our study of 16 people, this likelihood shows that our method is 95.24 percent safe, because attackers find it hard to guess a password without computer power via shoulder surfing and video capture.

6.1 Discussion

Learning python-based GUI programming was challenging at first. The time it took to grasp the approach was more than the time it took to put it into action. The second job was to create logic to place the numbers and characters in the rubic until the logic was created, at which point they were inserted by brute force. However, logic was ultimately established, and two classes were created: a slice class with tkinter functionality and a

wheel class. Different tests were carried out using various parameters to evaluate the output and check the reliability. A user survey was performed with persons who use computers on a daily basis.It was difficult for users to remember the technique, thus it took longer to log into the system. However, after a few trials, the system appeared to be user-friendly, and the login time was dramatically decreased. To improve security even more, the system may be extended by allowing users to generate passwords with more than 8 characters. However, the proposed technique is an effective way for safe authentication that can be utilized to improve system security.

As can be seen in the table below in Figure 11, the proposed approach worked effectively, with a "easy to use" factor percentage of around 76 percent and a "easy to recall" factor percentage of about 69 percent. The specified goals have been accomplished, and the models are producing the intended results.

		Satisfaction during registration		
Features	**Passpoint**	**DAS**	**Passdoodle**	**Proposed method**
Easy to create	54 %	34%	32%	56%
Easy to remember	64 %	60%	43%	67%
Easy to execute	63%	32%	66%	69%
Fast execution	63%	35%	50%	65%
		Satisfaction during login		
Easy to use	73%	75%	65%	76%
Easy to memorize	43%	40%	59%	49%
Easy to execute	80%	60%	71%	76%
Fast execute	60%	35%	63%	65%
		Effectiveness		
Reliability	40%	40%	30%%	32%
		Efficiency		
Security	33%	22%	47%	50%
Usability	57%	50%	51%	67%

Figure 11: Discussion and Comparison of algorithms with the existing algorithms

7 Conclusion and Future Work

No traditional authentication system has been able to match the security and applicability of the username password combination. Despite the fact that several graphical-based password authentication systems have been developed to improve the security of the authentication process, these schemes have flaws or are difficult to use. By integrating text and graphical based authentication strategies, the suggested system was designed to provide a simple interface as well as protection from shoulder surfing, video recording, and keystroke logging. A proper evaluation might, in turn, logically support an increase in the value of proof of relevant records and documents.A user must remember a textual

username, textual password, and a color in the proposed system. The user may then use this information to browse the graphical interface and input their passwords. The system delivers a 95.24 percent security rate, and it takes an average of 14.875 seconds to log into the system on a second try, according to 16 participants' analysis findings. Furthermore, because the system is integrated in one step, the user does not need to go through several authentication steps; all that is necessary is for the user to make the proper option in order to log in successfully.

This approach, according to our data, is more resistant to multiple password breaches than text passwords. We show that participants were able to memorize graphical passwords faster than numerous text passwords. Because the number of letters that can be used in this system is restricted, it could be stretched in the future, but this would result in a larger user interface, which is not a good practice. Instead, the limited number of shades could be widened with more shades, which would make the system more complex. Furthermore, while the login mechanism provides password security, we have not provided protection to the location where the database is recorded, which may be included in future development. As a result, the experiment potentially fulfill the stated goal of assessing making system more efficient.

References

Abuzaraida, M. A. and Zeki, A. M. (n.d.). Awareness and security issues in password management among libyan universities staff members.

Behl, U., Bhat, D., Ubhaykar, N., Godbole, V. and Kulkarni, S. (2014). Multi-level scalable textual-graphical password authentication scheme for web based applications, *REV Journal on Electronics and Communications* **3**(3-4).

Bhand, A., Desale, V., Shirke, S. and Shirke, S. P. (2015). Enhancement of password authentication system using graphical images, *2015 International Conference on Information Processing (ICIP)*, IEEE, pp. 217–219.

Chaudhary, B. (2013). *Tkinter GUI application development hotshot*, Packt Publishing.

Chiasson, S., Van Oorschot, P. C. and Biddle, R. (2007). Graphical password authentication using cued click points, *European Symposium on Research in Computer Security*, Springer, pp. 359–374.

Everitt, K. M., Bragin, T., Fogarty, J. and Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords, *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 889–898.

FAZLI, N. A. B. M. (n.d.). Graphical password authentication using cued click point technique.

Gokhale, M. A. S. and Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique, *Procedia Computer Science* **79**: 490–498.

Hafiz, M. D., Abdullah, A. H., Ithnin, N. and Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique, *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, IEEE, pp. 396–403.

Jiya, G. K., Oyefolahan, I. O. and Ojeniyi, J. O. (2021). Recognition based graphical password algorithms: A survey.

Lin, J. and Zhou, A. (2018). Pydraw: a gui drawing generator based on tkinter and its design concept, *arXiv preprint arXiv:1808.09094* .

Ocko, A. (2021). *The influence of graphical representations of password strength on the behaviour of potential victims of cybercrime*, B.S. thesis, University of Twente.

Sadeghi, S., Manochehri, K. and Jahanshahi, M. (2021). Use of digital image watermarking to enhance the security of graphical password authentication, *Journal of Algorithms and Computation* **53**(1): 165–180.

Salem, A., Zaidan, D., Swidan, A. and Saifan, R. (2016). Analysis of strong password using keystroke dynamics authentication in touch screen devices, *2016 Cybersecurity and Cyberforensics Conference (CCC)*, IEEE, pp. 15–21.

Subangan, S. and Senthooran, V. (2019). Secure authentication mechanism for resistance to password attacks, *2019 19th International Conference on Advances in ICT for Emerging Regions (ICTer)*, Vol. 250, IEEE, pp. 1–7.

Tam, L., Glassman, M. and Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience, *Behaviour & Information Technology* **29**(3): 233–244.

Veras, R., Collins, C. and Thorpe, J. (2021). A large-scale analysis of the semantic password model and linguistic patterns in passwords, *ACM Transactions on Privacy and Security (TOPS)* **24**(3): 1–21.