National College of Ireland

Implementing Colour Shuffling with OTP as a defence against Shoulder Surfing

MSc Internship
Cyber Security

Swaroop Phatak
Student ID: x17164800

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Mr. Swaroop Satish Phatak		
Student ID:	X17164800		
Programme:	MSc. Cyber Security	**Year:**	2018-2019
Module:	Academic Internship		
Supervisor:	Imran Khan		
Submission Due Date:	12 August 2019		
Project Title:	Implementing Colour Shuffling with OTP as a defence against shoulder surfing		
Word Count:	5232	**Page Count**	17

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: .....

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):	

Implementing Colour Shuffling with OTP as a defence against Shoulder Surfing

Swaroop Phatak
X17164800

Abstract

Shoulder surfing is an attack which has to be exterminated for the betterment of the society. Identity theft and digital piracy are also the branches of shoulder surfing and keylogging. Authentication is the remedy for these attacks as identifying the correct person before giving access to a system is a crucial part. Traditional password systems are vulnerable to visionary attacks like a person standing behind and watching over the user's shoulder and cameras can record the finger movements on the keyboard. To avoid these attacks, the method of graphical password was introduced. This research introduces a graphical method with password, colour and OTP as three factors of authentication. This scheme helps user to authenticate without exposing the password to other entities. The analysis of this scheme is performed and also the user survey has been displayed.

Keywords: Authentication, Shoulder Surfing, Key logging, OTP, Password, AES

1 Introduction

Authentication is the word highly held for the purpose of identifying a person while accessing a resource or performing certain actions. The basic example of authentication is when a person entering a building has to identify himself to the security guard before entering. This method was traditionally used, as machines do the work of security guards in today's digital world using methods like passwords and face or voice recognition. Another example is of the bank in which traditionally a person in need of money would go to a bank employee, tell him account details and withdraw the amount required. Now there are machines called as ATM's (Automated Teller Machine) that work as a bank employee to provide user money when needed. (SearchSecurity, 2019)

The human power required for these jobs has certainly reduced however on the other hand machines can wrongly interpret the input if the data is tampered with and some other person can get unauthorized access to the resource, it may be a residence, a bank account or any other facility. These machines are trustable but the user entering important information in the places like ATM's in a mall or in a crowded place is a dangerous aspect as an attacker can shoulder surf the user's password during the transaction. To avoid these attacks, the traditional password schemes like numeric and textual passwords have to be replaced by graphical passwords which are hard to track even if an attacker can see over a user's

shoulder. Graphical passwords include text or number matching, image selection and arranging numbers or characters. (SearchSecurity, 2019)

This paper proposes a method which includes selecting a colour, from the available list of colours, during the time of registration with a username and password. During the login phase user will receive an OTP on the registered mail which has to be matched with the colour, selected during the registration, in a graphical wheel of 6 sectors. The detailed information about the working model will be explained in the methodology section. By implementing this password scheme at the ATM's in crowded places, the attacks like shoulder surfing can be avoided. Another attack similar to shoulder surfing is the keylogging. This attack is possible where keyboards are used irrespective of its contents like numbers or alphabets. This attack comes in two forms software keylogging and hardware keylogging. The software keylogging operates by placing a software in the operating system and taking the logs of the keys that user uses. While in hardware keylogging, the buttons pressed by the user are recorded and stored in a hardware device. By using touch screen and graphical passwords the attacks like keylogging can be avoided. (Comodo Securebox, 2019)

Research Question

Can shoulder surfing be avoided using graphical passwords like colour shuffling and OTP?

This research paper is organized as follows. Section I contains Introduction which provides the motivation for research and a brief description of the defined model. Section II contains related work also called as literature review which provides a descriptive summary of each and every scientific paper referred during the research. Section III Research Methodology. This section describes in a detail format the way this model has been designed, each and every step taken under consideration during the execution. The tool used for developing the model, the programming language used and the list of other resources are mentioned in this section. Section IV includes all the architecture diagrams used for the research project. The diagrams like UML diagram, state diagram and use case diagram are displayed in this section. Section V lists the implementation stage that is the final stage of the execution. The outputs are discussed in this section. Section VI is the evaluation section, probably the most important section in the research. In this section the model designed is evaluated for its efficiency and accuracy by analysing the output obtained during the execution. Section VII is the conclusion and future work which presents the future work that could be carried out on the defined model and the conclusion of the current project. The last section contains the references used for the research. The reference section includes various website URL's which have been referred for the information gathering.

2 Related Work

The graphical password scheme with text is secure and well established. As a result there are previous similar works in research papers and journals. This section illustrates a critical review of the previous research in this field with an evaluation stating the advantages and

disadvantages. The methodologies used in the previous findings are also detailed for better understanding.

2.1 Authentication using PIN and Passwords

(Wagh and Ambekar, 2015) in their research paper introduce a method of graphical password for authentication which is resistant to shoulder surfing. The method illustrated has two phases, registration phase and login phase. The procedure starts by user registering for the service. In this phase, user has to choose a password between the length 7 and 16. The password may contain any characters either uppercase or lowercase, any numbers between 0 to 9 and special symbols. A sector has to be selected by the user from 1 to 6, which will be used at the login phase. The password is encrypted by using the system key and stored in the password table.

Once the user is registered, login phase comes into picture. In the login phase, a graphical circle is presented in front of the user containing 6 sectors. All the characters, symbols and numbers are distributed evenly between the 6 sectors. There are two buttons namely clockwise and anticlockwise. These buttons are for rotating the sectors in the circle. The password selected at the time of registration will be distributed in all the 6 sectors. User has to bring each character in the designated sector and click confirm button one after the other. When all the characters of the password are confirmed the user will be able to login by clicking on the login button. If the person is not authenticated three times an email will be sent to the user's registered email address through which the password can be reset.

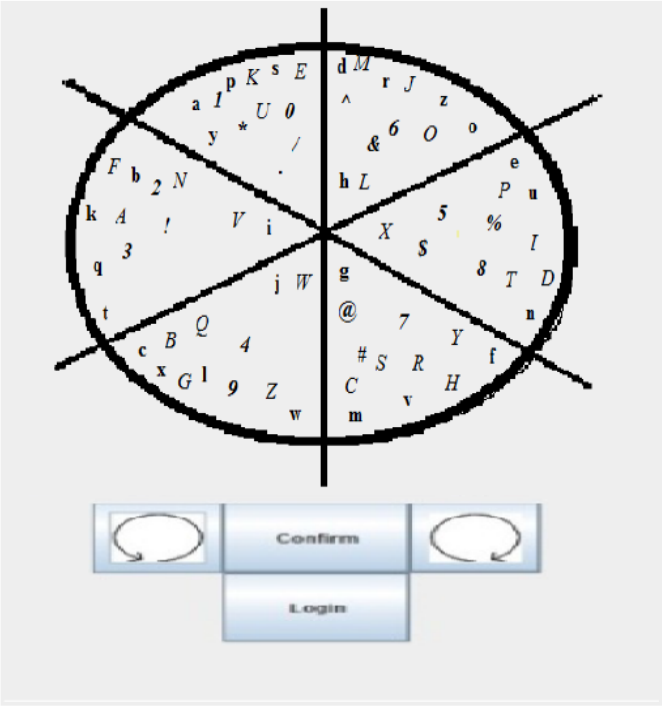

Figure 1. Graphical authentication with sectors

The research paper has only one factor authentication that is the password. Passwords can be cracked using various decryption methods and tools. The two factor authentication scheme is more secure when compared to the one factor authentication.

(Nikam, Bhujbal and Warpe, 2015) introduced an improvement over one factor graphical passwords in their research paper. The proposed system also has two parts, registration part and the login part. The registration part includes selection of username and password with a colour, for example, red, blue, black, orange, green, etc. The choice of the user is saved for future reference. The uppercase letters, lowercase letters, number from 0 to 9 and two symbols "." and "/" can be used for creating the password.

During the login phase user is presented with a graphical circle comprising of 8 sectors. Each sector will represent a different colour and will contain all the letters, numbers and symbols evenly distributed between all the sectors. The user has to remember the colour selected during the registration phase. Each character of the password has to be brought into the selected colour and confirmed. One by one all the characters in the passwords are cross validated and if the password is correct, the user is granted permission to login into the system. The Random Number Generation Algorithm has been used to evenly spread all the characters in the sectors of the circle.

The research paper provides a graphical authentication method with two factors to avoid shoulder surfing. However, the research paper does not specify which encryption is used while storing the password. A simple encryption scheme can give away passwords to cyberattacks which is not safe. If the password is compromised, an unauthorized user can get access by accident.

(Sreelatha et al., 2011) state that textual passwords are vulnerable to many attacks as a result of which graphical passwords based on colour and numbers have to be used. In this research paper, a method named pair-based authentication scheme has been introduced. The password chosen has to be of 8 characters minimum and the total number of characters in password should be even. The uppercase letters and numbers are used to form a grid.

During the login phase, username has to be entered after which a grid of 6 by 6 is displayed which consists of random numbers and letters. The characters in the password have to be selected using the pair based method in the grid. The intersection of the row and the column is one of the many characters of the password.

This method increases security but on the other hand, the time taken to complete the password is long and the selection process is complicated. Common people prefer the process to be fast and secure. Moreover if all the symbols, numbers and letters are used the size of the grid will increase to an extent where the grid is too big to select the required password using this method.

(Zhao and Li, 2007) discuss a method of authentication for avoiding shoulder surfing. A system named S3PAS is used in this research. This system is designed for the authentication between the client and the server. The single set scheme is implemented which provides the user with an image displaying all the characters. The password is hidden between the characters. User will choose the password from all the characters by clicking in

between the invisible triangle. For example consider the password is “AB13”. To complete the password user will have to click in patterns namely “AB1”, “B13”, “13A” and “3AB”.

To choose first three words user will click on any character that lies in the triangle formed by “AB1” and so on till the password is complete. Once the password is accepted by the system, user is allowed to login and do further operations. Furthermore there are 3 more methods defined namely, three-set scheme, rule-based scheme and Enhanced Graphical scheme. Each method increases the size of the grid displayed with the characters on the screen.

The scheme has a disadvantage in the case where the character grid is of a small size. Small size refers to less characters which may lead to accidental logins, resulting in chaos.

(Perkovic, Cagalj and Rakic, 2010) in the research on shoulder surfing safe login define a novel PIN (Personal Identification Number) entering method for safe authentication. User will have PIN to enter into the system but instead of directly entering the numbers, a grid containing numbers from 1 to 9 are displayed on the screen with another set of buttons containing arrows showing all the directions like east, west, north, south, north east and northwest. The numbers in the grid are arranged in such a form that each number has all other numbers within one hop distance.

A challenge is provided to the user with every character of the PIN. For example if the first character of the PIN is 4, then the user will receive a challenge character as 9. There will be a dark box in the grid which user can move using the arrow buttons. Depending on the challenge character, the dark box will be moved to that position which will not reveal the original PIN characters to the attacker.

The method introduced is called SSSL method. The method protects the PIN but the time taken for the user to complete the challenge is the major drawback in this research. Also the arrow movements can be observed by the attacker leading to revealing certain numbers of the PIN.

(Zheng et al., 2009) propose a stroke based authentication method for the users. This research contains two important steps namely the password creation step and the login step. The password creation step includes the process of creating a pattern on a grid of size 5 * 5. The user can choose any shape according to the simplicity and preference. The same shape should be drawn on the grid for pattern password creation. The next step is the login step, which allows user to access the services based on the authentication information provided. An ID is required to be entered before password which is in the form of numbers or characters.

The password grid is presented to the user at the login phase to enter the pattern selected during the password selection phase. User has to enter the pattern in a binary format that contains 1’s and 0’s. The grid will be filled with random 1’s and 0’s from which user types in the pattern of the numbers required in the password field. Any shape can be selected as a password for example, 5, S, N, M and L are some of the most common patterns used by the user.

This scheme is similar to the pattern that is used to unlock mobile phones. However due to some of the most common patterns that user tend to set, the chances of accidental login increases leading to a cyberattack.

2.2 Authentication through Colour and Images

(Wiedenbeck et al., 2006) propose a Convex Hull click scheme. The scheme is introduced to avoid all the observation attacks while user is entering the password. This method eliminates the possibility of electronic capture due to the images used for authentication. The process starts with user selecting the number of images as pass-key defined by the administrator. User should memorize the selected images by practising on a daily basis.

The login phase will display a window with many images to the user. The images selected as the passkey by the user should be selected again from all those images. If all the images selected are correct the user is authorized. The clicking of the images is not direct as user has to click in between a convex hull forming a triangle keeping the pass images as the corner points. In some cases the convex hull can be very narrow, in that case the exact images between the pass-images have to be selected.

The method holds an advantage as the attacker cannot predict which icon user will choose as the password. Even if an attacker is observing the user entering the password, the information is not given out due to convex hull concept. The major drawbacks of this method are the time required for completing the authentication process and remembering the password images.

(Yamamoto, Kojima and Nishigaki, 2009) describe temporal indirect image-based authentication (TI-IBA). The flow starts with selection of the images as password. The number of images will be between 2 and 5. Once the images are selected the choice of the images are saved in the database for further use. There are two phases, registration phase and authentication phase. The first phase includes the selection of images.

The second phase is the process of logging in to the system. User will be presented with presentation slides. Each slide will contain 4 images. The images of the password can be on any slide. The time one slide stays on the screen is about 10 seconds. User has to click on the slide containing the images of the passwords. Even if some other person is observing, image recognition will be complicated due to the slide show.

The time required for login will be more due to the selection of slides. All the images of the password are stored in a single slide which user selects. This selection can be accidentally observed by using the camera and the password can be exposed.

(Gao et al., 2009) in the research of design and analysis of graphical password scheme have devised a new method called ColorLogin. This scheme has four different levels namely low, medium, high, and self-defence. The user is entitled with three stepped operation first is the choosing the level of security needed, second is the choice of colour and third choice is the image selected as the password.

The method of perplexing the attacker is used as the user will click on the dummy icons instead of the original icons of the password. A window will appear on the screen consisting of many images, each and every image will be unique. The colours are distributed within the images in any shape for example in a diagonal or square format. When user clicks on one password line, the images in the line get substituted by locks. This becomes one of the major drawback as the observer can note what are the images on both the lines selected and can use them in future. Also the time taken for selection of security, colour and the images takes a long time which is not suitable for normal users.

(Sobrado and Birget, 2002) in the research of graphical passwords define a scheme which substitutes the alphanumeric passwords introducing the use of images in authenticating a user. The research paper mentions one phase that is the login phase. The time when user tries to login into the system, an image will appear on the screen where user has to select certain points on the image. Those points should match the points selected during the registration phase. If the points match then the user is successfully authenticated. However this method is not secure as a person watching over the user's shoulder can easily remember the points selected by the user and can repeat the process to gain the access to the user's account.

2.3 Defined strategy and Advantages

In the current research of a graphical password a scheme including colours and OTP is introduced. This research overcomes all the limitations that are present in the papers discussed in the first section of the literature review. The time factor required for the login, the accuracy of the authentication and the possibility of accidental logins are discussed in the evaluation section.

3 Research Methodology

The colour shuffling technique introduced by (Nikam, Bhujbal and Warpe, 2015) uses colour with the password for the authentication. The graphical password research by (Wagh and Ambekar, 2015) uses password and section selection in the graphical wheel for user identity confirmation. This research is based on the improvement of the idea stated in the paper by (Nikam, Bhujbal and Warpe, 2015). This research uses a three factor authentication. The three factors being password, colour and OTP.

3.1 Graphical Circle

The research paper by (Nikam, Bhujbal and Warpe, 2015) propose a graphical authentication method using a graphical circle with 8 sectors to match the user's password. However the time taken to match the characters in the sector depends upon the length of the password and the amount of random characters in the circle. This research proposes a method using a

graphical circle with 6 sectors which will contain random lowercase letters and numbers from 0 to 9. This will reduce the login time and the user credentials will also be safeguarded as user does not have to match the actual password.

3.2 One Time Password (OTP)

Previous researches prefer matching the user's password in the designated graphical sectors with the help of colours or sector numbers. User selects these at the time of registration. In this research to safeguard user's password an extra layer of authentication is added known as the One Time Password. The user's password, entered during the registration, is stored in the database by encrypting it with AES. The OTP is sent to the user's registered mail ID at the time of the login process. The OTP sent to the user is of 4 characters including a combination of lowercase letters and numbers. This reduces the time taken by the user to login while keeping the password protected. (Man, Hong and Matthews, 2003)

3.3 Visual Studio and Database

Visual Studio 2019 framework is used for the implementation of this project. The language used is C sharp. Various libraries provided by Microsoft are used in this project. A desktop application for an authentication system is developed. The final implementation is explained in detail in section 5. A database is created to store all the user information entered during the registration phase. This table includes username, mail ID, name, address, phone number and the colour choice made by the user. Table that stores the OTP sent to the user is also included into the database for reference purposes. The colour selected by the user is saved in the database with the help of ID's. For example ID 1 is provided for the colour indigo, ID 2 is provided to the colour red and so on. SQL server provided by the Visual Studio is used to perform operations on the database. (Visual Studio, 2019)

3.4 Pseudo Random Algorithm

Generation of the One Time Password is done by taking into consideration the characters included. For example in this research the OTP is the combination of numbers and lowercase letters which means from all the 36 characters present, any random four characters are chosen and sent to the user for the process of identity confirmation. The random class provided by Microsoft is used to produce a pseudo random OTP.

4 Design Specification

The architecture of the proposed system comprises of various components that contribute in successful working of the scheme. The architecture diagram for this research is displayed below. The scheme contains six primary components namely user, registration phase, login phase, forgot password, OTP and service. Working of each element is explained in the

implementation section. This section illustrates different UML diagrams in relation to the proposed model. For example use case diagram and sequence diagram.

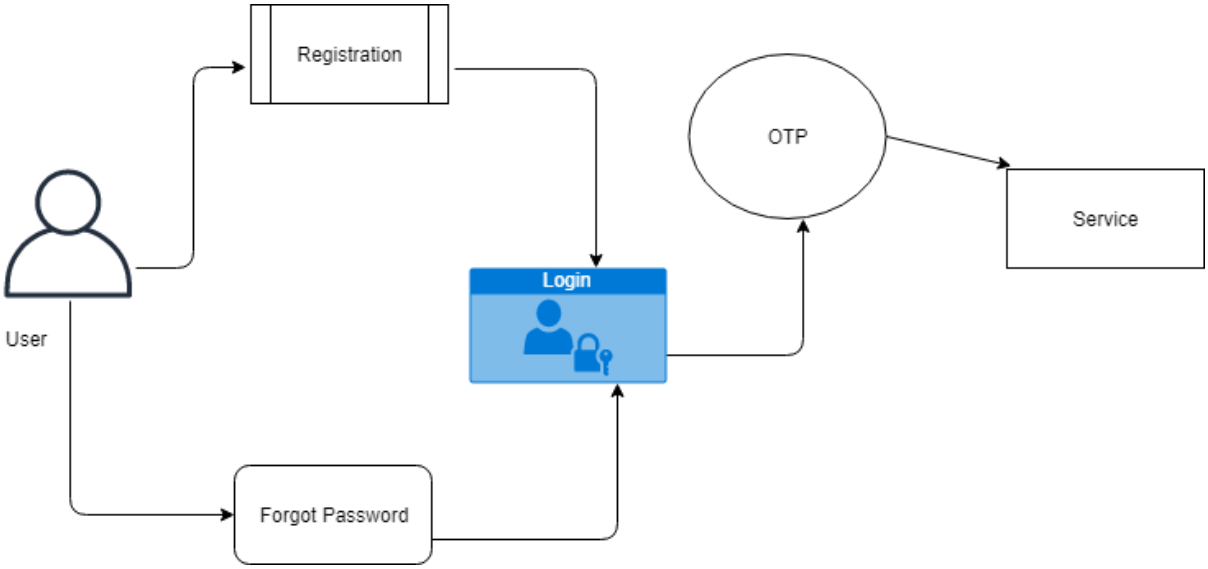

Figure 10. Architecture Diagram

Pseudo random number generator algorithm is used for generating the OTP sent to the user. The OTP is 4 characters long. The combination of numbers and lowercase letters is included in the OTP. The random class provided by C sharp is used for implementing the OTP process.

4.1 UML Diagrams

Sequence Diagram

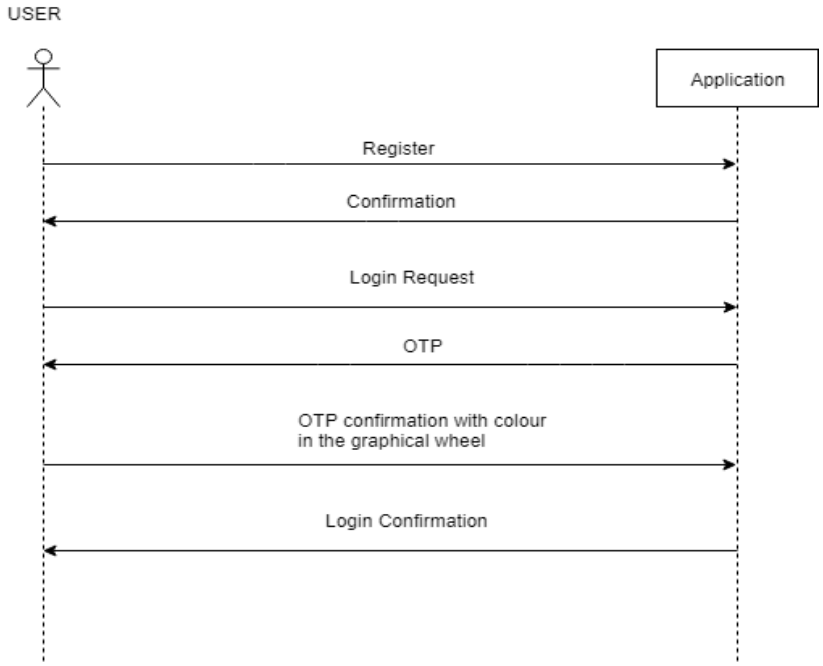

Figure 11. Sequence Diagram

Use Case Diagram

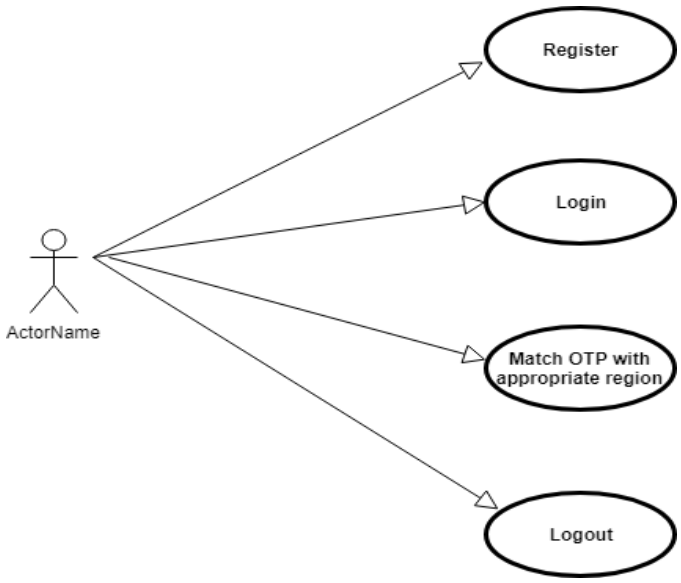

Figure 12. Use Case Diagram

5 Implementation

The research implementation executes in a step by step process. Each step depends on the output of the previous step. Three phases are presented in this section namely registration phase, login phase and forgot password phase.

5.1 Registration Phase

Step 1:- Registration of the User.

The process starts with the user signing up for the service by using the registration form. This step takes the personal information from the user like username, name, address, phone number, mail ID, password and the colour code. The information taken is saved in the database for further reference and cross checking when customers login again. The password is encrypted before saving to the database with AES encryption. It is recommended to input all the information in a shoulder surf free zone.

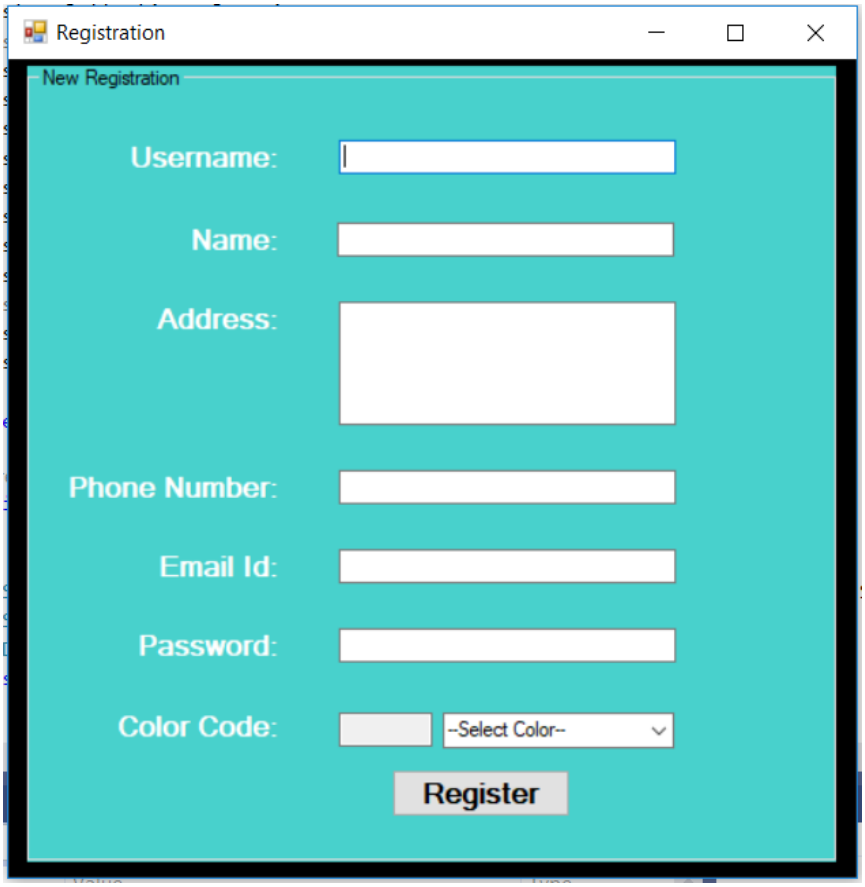

Figure 5. Registration Page

Step 2:- Selection of the colour.

During the registration, the user has to select a colour among the primary colours namely indigo, red, blue, green, orange and violet. The choice of the colour is also saved in the database as it is required for confirming the user identity in the further steps.
The image asking the user to select a colour is as follows.

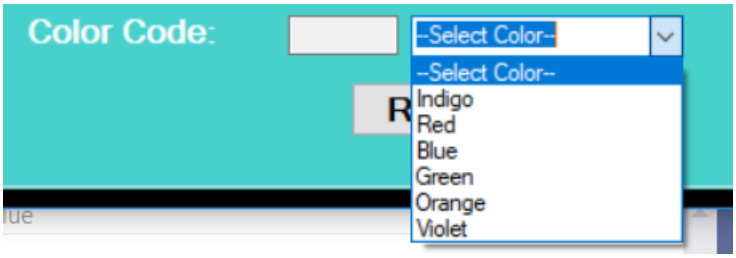

Figure 6. Selection of colour.

5.2 Login Phase

Step 3:- Logging in to the account.

Once the registration is done, the user is officially a member of the service and can login at any time the user wishes. The login screen, user will encounter, is shown in the diagram below. To login user will be asked to enter the username and password given at the

time of registration. If the entered username and password matches the one in the database, an OTP will be sent to the mail ID of the user given at the time of registration which will consist of 4 to 5 characters which will include numbers and letters. The length of the OTP is kept short to decrease the time required for the authentication.

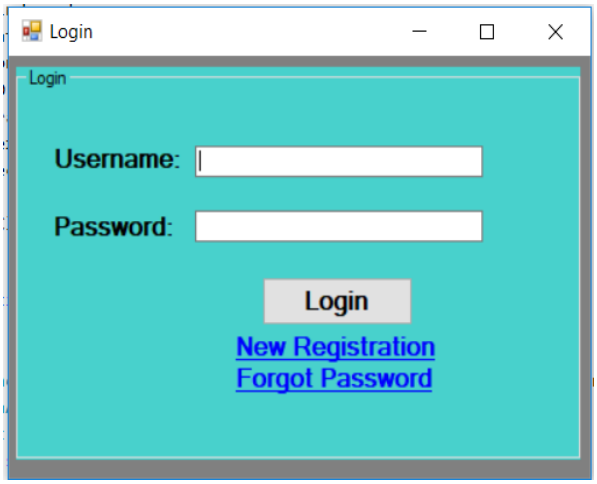

Figure 7. Login Page

Step 4:- Matching the OTP with the colour in the graphical wheel.

The graphical password in this implementation is a wheel containing of 6 sectors. Each sector contains random characters and numbers. All the numbers and characters in the OTP will be present in the wheel. An image as an example is displayed below.

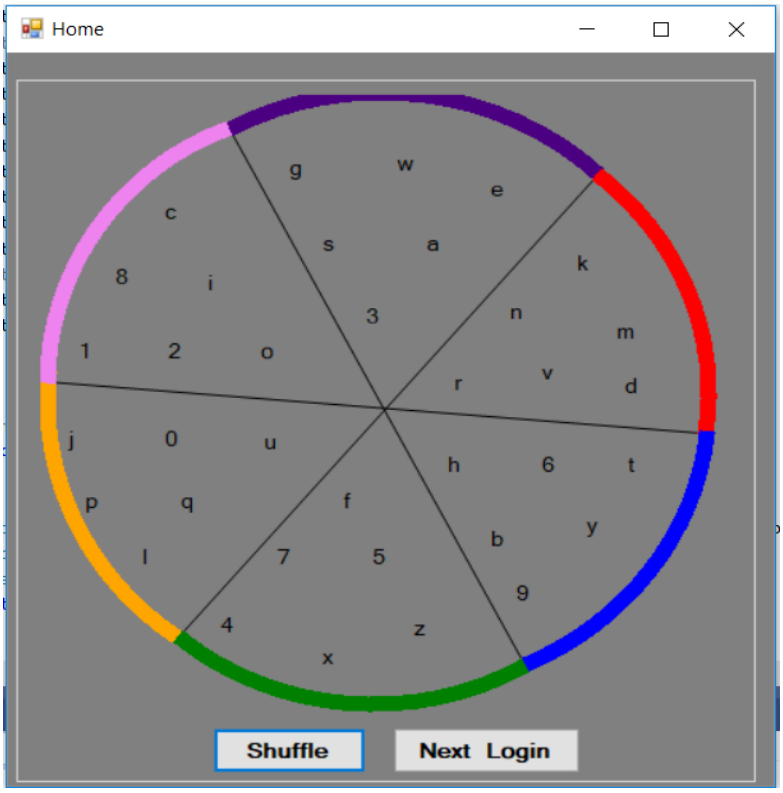

Figure 8. Graphical Password Wheel.

The image shown above displays a circle with different colours on the parameter. The user has to identify the colour selected during the registration phase and then shuffle the sectors to bring the numbers and letters into the right colour.

Step 5:- Bringing numbers and letters into the right colour.

There are two buttons present below the graphical wheel namely, Shuffle and Next Login. User has to shuffle the wheel bring the 1st character of the OTP in the appropriate colour and press next login button. Once the 1st character is confirmed, the second character which is in another sector than the first character is brought into the correct colour and the next login button is pressed which then confirms the second character of the OTP. Accordingly all the characters in the OTP have to be shuffled and brought into the correct colour individually after which if the OTP is correct the system will let the person login. An array is designed such where the characters confirmed are matched with the characters in the OTP.

5.3 Forgot Password Section

The user is recommended to remember the username and the password. However people forget their credentials as there are many accounts on the social media and the internet. In that case there is an option called forgot password. This function operates as any other forgot password function. If the user cannot recall the password created at the time of registration and needs to login, clicking the forgot password link by entering the username will send an email to the registered mail ID and can use that password to login into the service.

6 Evaluation

The developed application is based on authentication. Only proposing a method is not enough as there should be some proof that the method is going to work and is strong enough to withstand cyberattacks. The analysis of this project is done with respect to the strength of password, the time user's take to login into the system and the possibility of accidental login.

6.1 Passwords Space

The user enters a password during the registration phase of 8 to 15 characters i.e. the length of the password can be anywhere between 8 and 15 ($8<L<15$). The password must contain at least one uppercase letter, one lowercase letter, one special symbol and one number. These are the basic requirements user should meet for the system to accept the password. Hence the total characters used for this research is 80 characters including all the special symbols. Depending on the length provided for the password, the possible combinations of the passwords are calculated as follows. (Wagh and Ambekar, 2015)

Formula –

$$\sum 8 * 80^{L} = 8.5899 * 10^{28}$$

The value of L on the L.H.S of the equation varies from 8 to 15. However for the calculation, the value of L is considered to be minimum as 8. The final value we get is a large value in which concludes that the password space for the research is very large.

6.2 Accidental Login

The login process comes into the picture after the registration step. During the login, user will receive an OTP on the user's mail address which will be used for matching in the graphical wheel according to the colour chosen. However at times if a person is trying to access another user's account, the chances of that person to successfully infiltrate the account are addressed here. (Nikam, Bhujbal and Warpe, 2015)

The available password characters are 80 and the minimum password length is 8. This implies that user has to enter a minimum 8 character password. According to this data the probability of accidental login is given below.

Probability – Minimum Password / Total password characters

8/80 = 1/10 = 0.1.

The above value implies that there is a 0.1 chance that an accidental login can happen.

6.3 User Survey

The login process takes certain time as the OTP sent to the mail ID has to be matched in the graphical wheel with 6 sectors. A survey is performed with 10 users to check the login times required for each user. The results are displayed below.

The graph shown below has two axes, X axis and Y axis. The X axis represents the users like user 1, user 2 and user 3 etc. The Y axis represents the time taken by every user to login into the system. The average time taken by the users to login into the system is from 15 to 20 seconds.

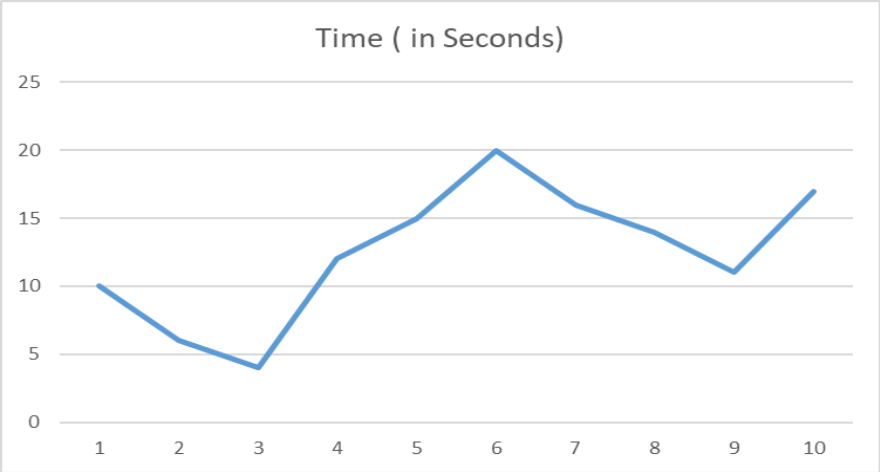

Figure 9. User Survey

6.4 Discussion

The research on a method of authentication has been performed. The evaluation section shows various results depending on the performance of the application. The results like the password space, probability of accidental login and user survey provide higher efficiency than the previous works on this research. The formulas from the reference papers are being used for obtaining the results. Also the user survey was conducted with the people working with computers in their daily lives.

7 Conclusion and Future Work

Authentication, as a crucial process, has to be secure. A method called graphical password is used to implement a process to authenticate users into the system. The scheme proposes three factors for authentication namely colour, password and OTP. The efficiency of the proposed method is high as compared to the previous works. As the efficiency increases, the security of the system also increases which results in less accidental logins and system failures. The project has been developed by using the C sharp language in the Visual Studio framework. The system requirements for this desktop application are minimum which makes it easier to be implemented in various offices and institutions.

Three factors were compared during the evaluation namely password space, the possibility of accidental logins and the time required for the login process. All the factors produced highly effective results that are discussed in the evaluation section.

The only factor obstructing the implementation of this method is the time taken by the user to logon into the system. In future the time constraint can be taken into account while researching the topic as it will save many people from cyberattacks.

References

Wagh, S. and Ambekar, A. (2015). Shoulder Surfing Resistant Text-based Graphical Password Scheme. *International Conference on Computer Technology*.

Nikam, A., Bhujbal, T. and Warpe, S. (2015). A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme. *International Journal of Advance Foundation and Research in Computer*, Volume 2(2348 - 4853).

Sobrado, L. and Birget, J. (2002). Graphical passwords. 4, p.7.

Yamamoto, T., Kojima, Y. and Nishigaki, M. (2009). A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection. *Centre for Research and Evidence on Security Threats*, p.7.

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. and Manoj Kumar, V. (2011). Authentication Schemes for Session Passwords Using Color and Images. *International Journal of Network Security & Its Applications*, 3(3), pp.111-119.

Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J. (2006). Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. *Proceedings of the National Academy of Sciences*, p.8.

Gao, H., Liu, X., Wang, S., Liu, H. and Dai, R. (2009). Design and Analysis of a Graphical Password Scheme. *2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*.

Zhao, H. and Li, X. (2007). S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme. *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, 2.

Zheng, Z., Liu, X., Yin, L. and Liu, Z. (2009). A Stroke-Based Textual Password Authentication Scheme. *2009 First International Workshop on Education Technology and Computer Science*, p.6.

Man, S., Hong, D. and Matthews, M. (2003). A Shoulder-Surng Resistant Graphical Password Scheme - WIW. p.6.

Perkovic, T., Cagalj, M. and Rakic, N. (2010). SSSL: Shoulder Surfing Safe Login. *JOURNAL OF COMMUNICATIONS SOFTWARE AND SYSTEMS*, 6(2), pp.65-73.

SearchSecurity. (2019). *What is shoulder surfing? - Definition from WhatIs.com*. [online] Available at: https://searchsecurity.techtarget.com/definition/shoulder-surfing [Accessed 3 Aug. 2019].

Comodo Securebox. (2019). *What is Key Logging and Keystroke Logger? | How Comodo Helps*. [online] Available at: https://securebox.comodo.com/key-logging/ [Accessed 5 Aug. 2019].

Visual Studio. (2019). *Visual Studio 2019 | Download for free*. [online] Available at: https://visualstudio.microsoft.com/vs/ [Accessed 7 Jun. 2019].

SearchSecurity. (2019). *What is Authentication? - Definition from WhatIs.com*. [online] Available at: https://searchsecurity.techtarget.com/definition/authentication [Accessed 5 Jul. 2019].