Prevention of Shoulder Surfing with the use of Graphical Password Authentication

Arushi Mittal
NIIT University

Vishal Sahu
NIIT University

Chirag Bhatnagar
NIIT University

Dr. Kumar Nitesh
NIIT University

Shoulder Surfing attacks allow the adversary to gain the user's password by peering over the user's shoulder as he or she types their password into their devices. A typical user's password is particularly vulnerable to shoulder surfing. As a result, prevention of such attacks becomes increasingly necessary. Because the majority of the people are more accustomed to textual passwords than graphical passwords, much research has been conducted to incorporate such a system that has the components of a textual password but is also effective in preventing shoulder surfing to a greater extent. Unfortunately, none of the proposed text-based shoulder surfing prevention graphical passwords is both secure and efficient. In this paper, we will offer an idea that includes elements of both textual password and graphical password approaches by introducing different colour and dial combinations to boost the security and effectiveness of a graphical password system while keeping the familiarity of a textual password.

Keywords: **Shoulder Surfing, Graphical Password**

1 Introduction

When we think of cybercriminals, we usually picture tech-savvy geeks who write malware or get illegal access to remote computer systems to steal sensitive data. However, there is frequently a simpler approach to collecting personal information and passwords. Shoulder surfing is a simple method of spying on unwitting victims to gather passwords and other sensitive information, PINs, and other login information. This attack can be carried out at a close range or a longer range using, for example, binoculars or similar hardware. Attackers do not need any technical expertise to carry out this strategy; simply keeping a close eye on the victims' environment and typing pattern is adequate. Shoulder surfing dates back to the early 1980s when it was done to grab calling card digits near public pay phones and make long-distance calls with them or sell them for less than the original purchaser paid. However, the development of modern-day technologies such as concealed cameras and covert microphones makes shoulder surfing easier and allows the attacker to do long-range shoulder surfing. There are two varieties of shoulder surfing. The first type of attack involves using direct observation to gain data access.. This is when someone stares straight over the victim's shoulder to see what they are doing, such as entering their PIN. The victim's behavior is initially recorded in the second type. Criminals can then thoroughly examine these recordings later on to gather the needed information. Video recordings can now be used to find the PIN for unlocking mobile devices, even if the display cannot be seen in the video. The user's finger motions are sufficient to determine the login data in the case of PINs.

Users have trouble recalling complex information due to long-term memory impairments. Because the memory is not "refreshed," a user who does not use a password on a regular basis is more likely to forget it. When a person has many passwords, he or she may jumble the bits of the different passwords or lose track of which system they pertain to. Password memory concerns are often addressed by lowering the complexity and amount of passwords, which compromises password security. A strong password should be at least eight characters long, random, and include uppercase, lowercase, digits, and special characters. Users ignore password policies in favour of short, simple passwords that are relatively easy to guess using dictionary attacks.To address this problem, graphical password authentication was introduced. In 1996, Blonder was the first person to suggest graphical passwords. An authentication method is through the use of graphical password that lets the user to choose from a collection of graphical vector shown in a graphical user interface in a predefined order (GUI). Because people remember visuals better than text, graphical passwords are easier to remember. Advantages of graphical authentication include its high level of security. You may generate more human-friendly passwords using graphical password schemes. Both dictionary attacks and brute force searches are ineffective. In comparison to text-based passwords, they take up a lot more storage space. The process of creating a password and logging in is far too time-consuming.

2 Literature Review

Lee and Mun-Kyu stated[1] that the authentication in their study article is limited to 4-digit pin-entry, which limits the randomization of the characters in a password. Because the characters are limited to nine numbers, an attacker can easily guess or memorize minute aspects of the password while shoulder surfing. This approach consists of 9 digits, each of which is associated with a distinct symbol. The pin must be entered four times using this method. The first round is to figure out what the session key is for the next three rounds. The user recognizes the symbol under the first digit of his or her pin and pushes "ok" in the first round. For the remaining three rounds, he or she turns the row to couple the symbol and pin's second digit, then pushes "ok."This method takes less time to enter the pin, but it restricts the user to 9 characters. It is clear that if the attacker learns even one digit from the pin, he or she will be able to simply analyze and crack the pin.

IEEE's Taekyoung Kwon and Sooyeon Shin ran an experiment to see how efficient a PIN entering method known as the BW method in the paper [2] in which half of the input keys were colored black and half were colored white, was at preventing shoulder surfing. The user is then prompted to enter the color of the chosen key. This system triangulates the intended key using four-color inputs before registering it as an input. They discovered that using cognitive methods and training, this method may be easily broken in their experiment. They also suggested that the system be improved by employing four colors rather than two to boost the unpredictability and input variations of the PINs.

A Simple Shoulder Surfing Resilient Graphical Password Method by Chen, Yi-Lun, proposed a method[3] that generates the desired password using 64 characters (26 lower case letters (a-z), 26 capital letters (A-Z), 10 numerals (0-9), and symbols). "." and "/" in cyclic order and basic rotations (clockwise and counter-clockwise). Since this method collects characters in a single section of a circle, it can be unstructured in terms of usage.

Cued Recall-Based Technique, Recognition-Based Technique, Recall-Based Technique, and Hybrid Schemes have been addressed and elaborated by Dhanashree Kadu, Shanthi Therese, and Anil Chaturvedi in [4]. Consider the following scenario: (DAS) Draw A Secret is a technique that allows the user to draw a basic picture on a 2D grid of size N * N that is expressed by distinct two - dimensional coordinates (x, y) without the need of a pen. For authentication, the user must redraw the image by drawing strokes in the same order as during the registration phase. Even while some of these strategies are difficult to implement from the user's perspective and others are simple, they have not been able to totally eliminate the problem of shoulder surfing. "It may be concluded that breaking graphical passwords is more challenging than breaking alphanumeric passwords," they added.

Moving on, in Graphical password authentication with the use of hybrid pin keypad Hemamalini, M., and R. Saranya[5] have briefly discussed Hybrid PIN, a method that describes a simple, efficient, and alternate remedy for shoulder surfing attacks. The suggested Hybrid PIN keypad approach uses a digital pattern with 0-9 numbers. When the authorized user initiates the login process and passes the login request to gain access to financial services, the system displays a Hybrid PIN Keypad. It's made in a 4-3 matrix format. The pattern is then re-shuffled when the transaction is done and the screen is logged off. For shoulder surfers, the shuffling method's motto is "no clue." This methodology is now in use and is thus user-friendly, although it does not totally solve the shoulder surfing problem and requires further development.

3 Methodology

In this section, we will go over the methodology we used to create this application. We will describe a simple and effective graphical password scheme based on texts and colors that is resistant to shoulder surfing. The proposed scheme's alphabet contains 70 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and some special characters. The proposed scheme consists of two phases, the registration phase and the login phase, which are as follows.

3.1 The Key

Each key of the keyboard contains two rings i.e an outer ring and an inner ring. This key also consists of 8 sectors which consist of the one color that is selected by the user at the time of registration and 7 decoy colors. The image below showcases the key in detail. Each ring rotates both clockwise and anti-clockwise.

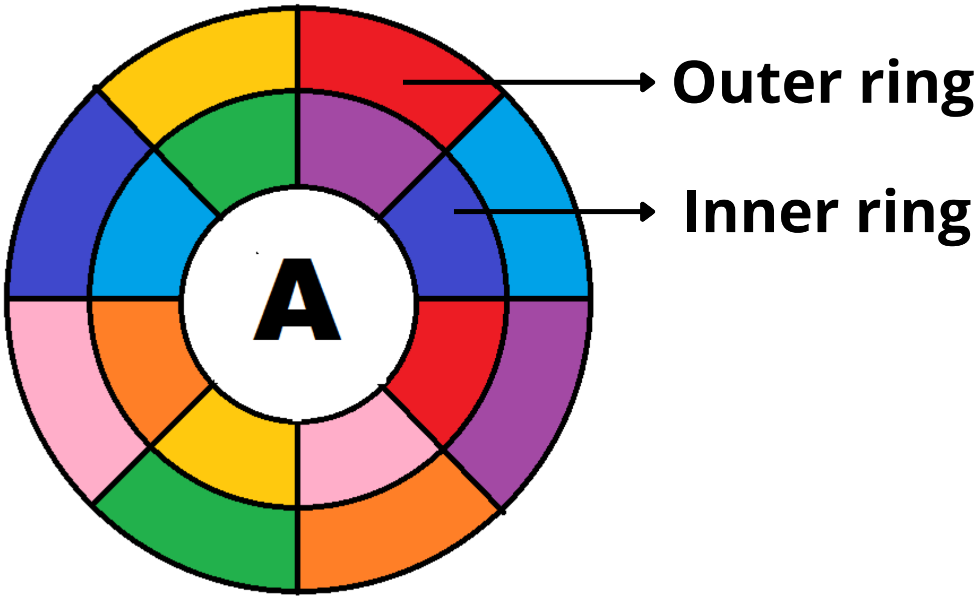
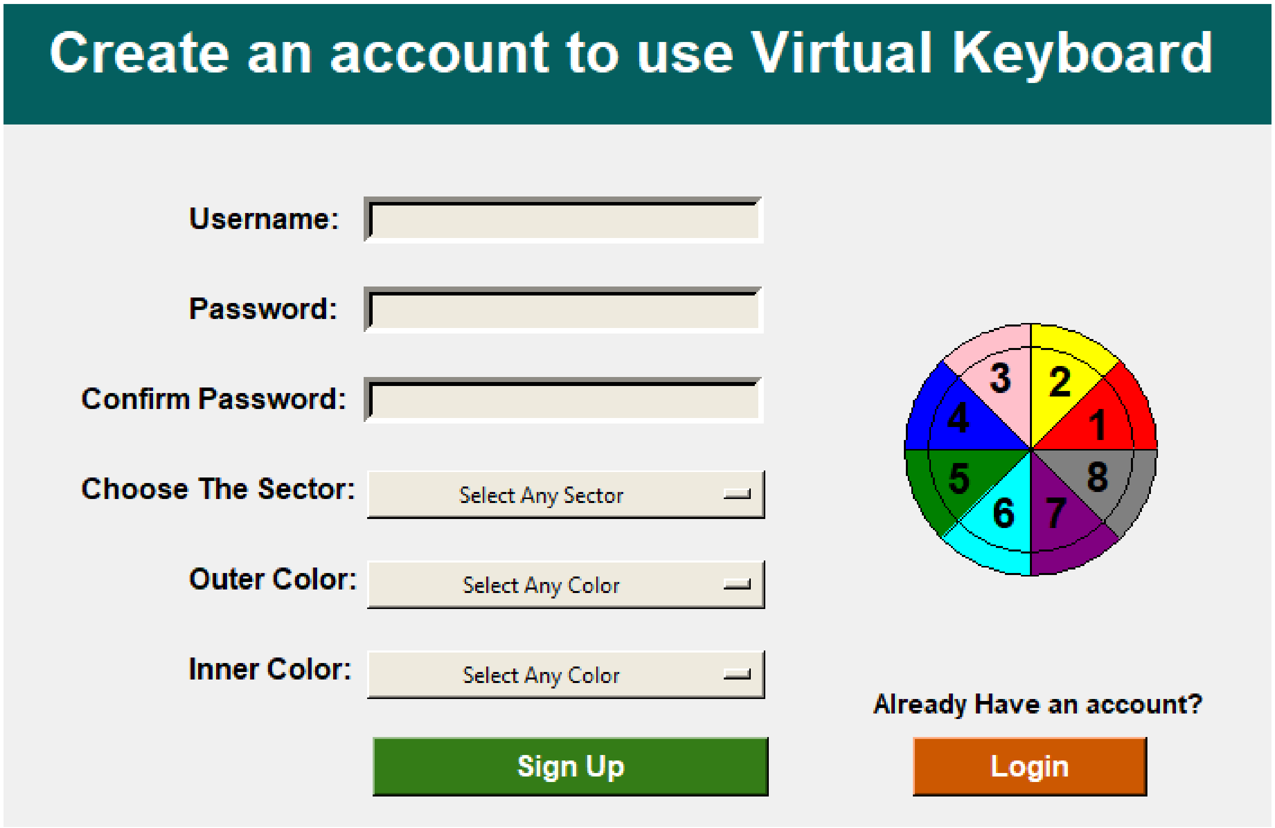


Fig:1 Model of 1 key in our keyboard

3.2 Registration phase

During the registration phase, the user is asked to choose a color from the system's 8 available options for the key's outer circle. The other seven colors that were not chosen will serve as decoys, the same process will follow for the selection of the inner circle's color. Finally, the user must choose one of the eight sectors of the key as the desired sector to complete the combination. To use the proposed keyboard, the user must remember these three factors as well as the string password. It is recommended that the user perform this phase in an environment free of shoulder surfing, as this phase contains critical information about the authentication process. After this, the user can use the keyboard for any form of password authentication.



Create an account to use Virtual Keyboard

Username:

Password:

Confirm Password:

Choose The Sector: Select Any Sector

Outer Color: Select Any Color

Inner Color: Select Any Color

Already Have an account?

Fig:2 Registration Window

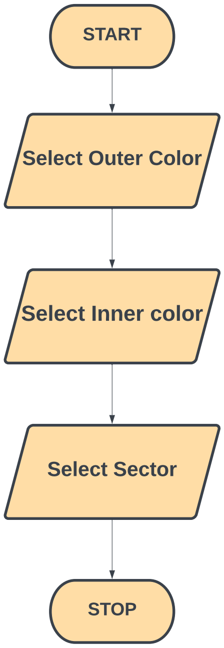


Fig:3 Registration phase

3.3 Login Phase

This phase consists of the following steps to perform the authentication

Step 1: The user must locate the key he or she wishes to enter from the keyboard. This should be a simple task because the keyboard follows the QWERTY system, so the location of a specific key is the same as on a standard keyboard.

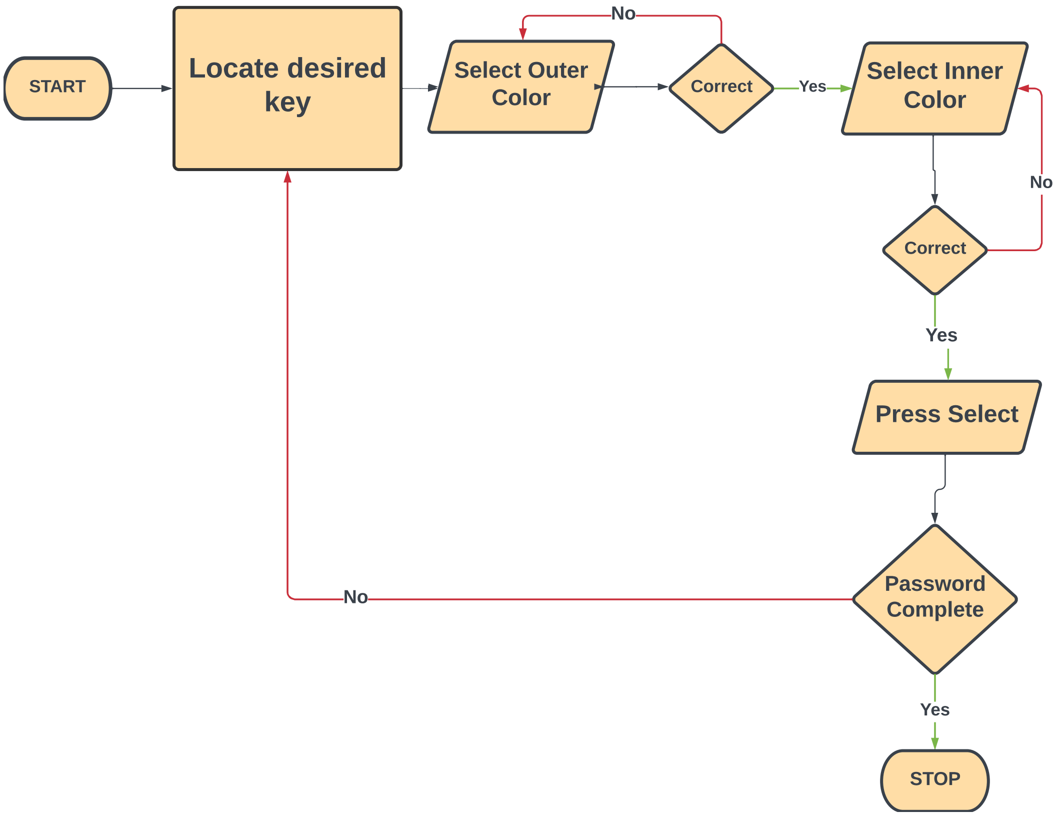


Fig:4 Login Flowchart

Step 2: To bring the specific color to the specific sector of the key, the user must now rotate the outer ring of the desired key. This task can be completed by using the button on the top left of the keyboard (i.e. the left and right keys) labeled with the name of the ring being rotated (an example of which can be seen in the image below). When the desired color matches the sector, the user can move on to the next ring. The procedure for the second ring remains unchanged.

Step 3. The previous two steps must be repeated until the user has entered his/her complete password in the input field, at which the user can click on “Copy to Clipboard” to copy the entered password to use it on the desired platform.

If users wish to use capital letters to enter their password, they can do so by pressing the "Caps Lock" key located at the top left (Just under Rotate Outer Ring Key).

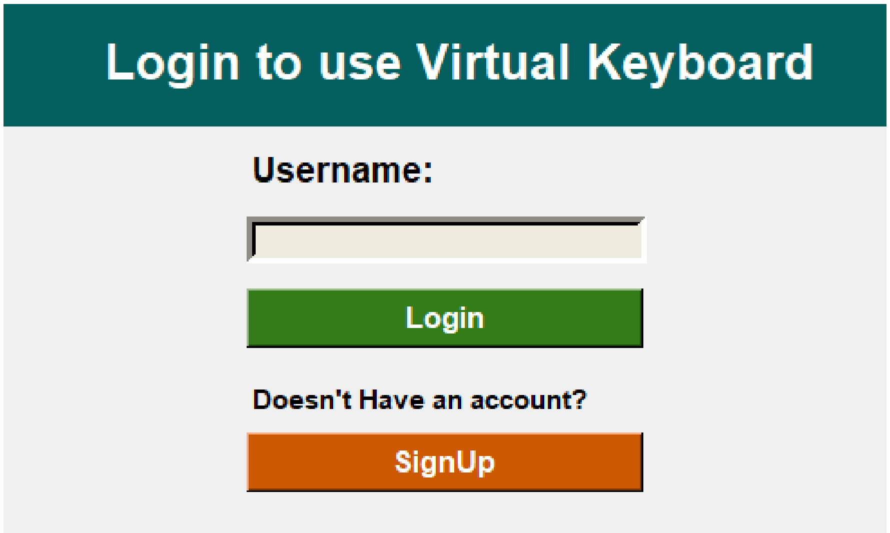


Fig:5 User Login Window

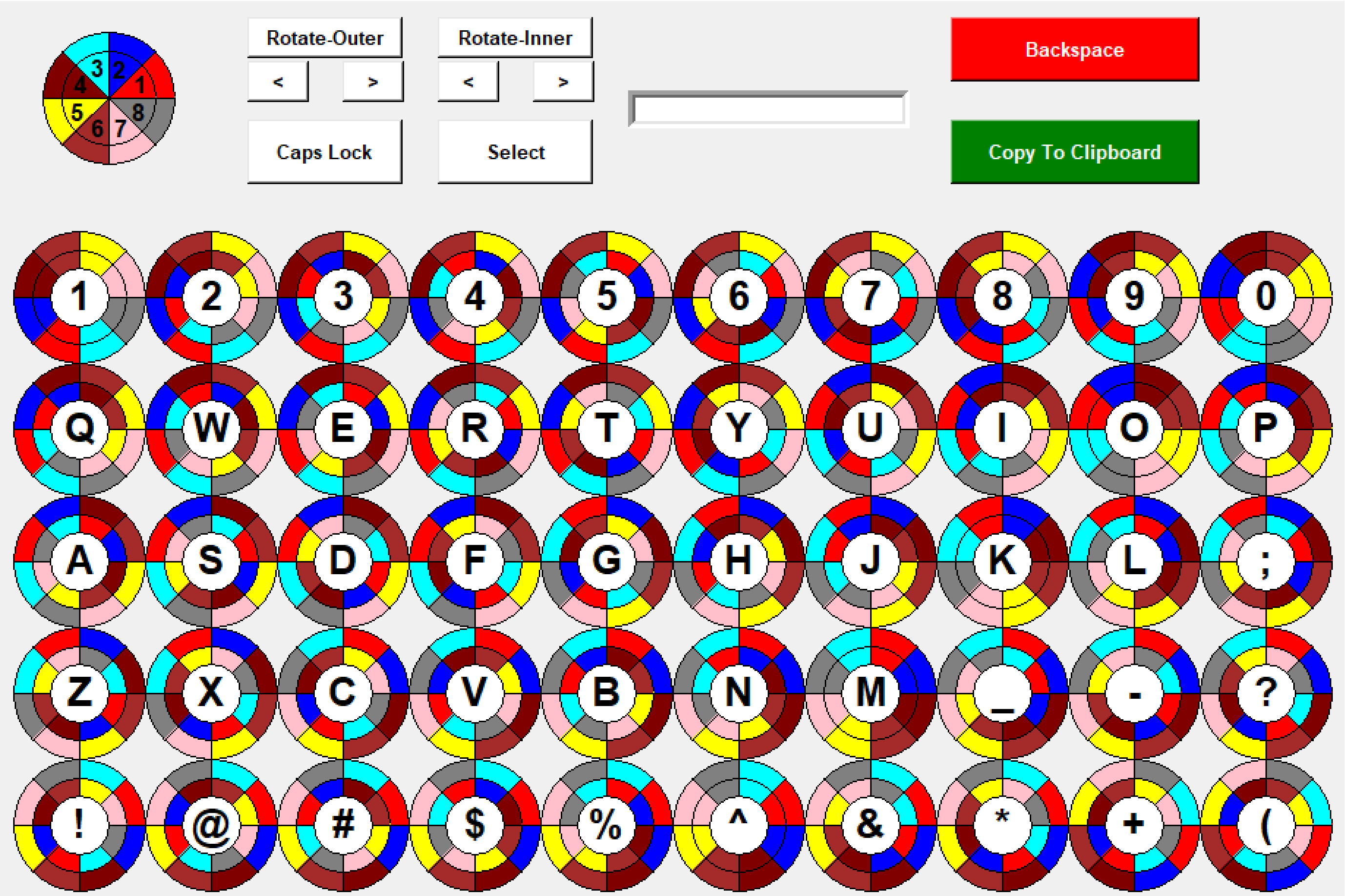


Fig:5 Keyboard Window

3.4 Technology Applied

So what is the technology used in designing the above model? Our proposed model is based on a GUI application built using the famous Python Library, Tkinter. As the scope of Python in the technological world is increasing day by day, we chose Python to develop this virtual keyboard to prevent Shoulder Surfing to some extent.

3.4.1 Python Libraries Used:

- **Tkinter** for designing the graphical user interface in a user-friendly manner. Tkinter is not only the GUI Programming Toolkit for Python but also the most common one because of its easy to code property.

- **Random** library to randomize the choice of colors in the eight sectors of a key. Every time, the user uses the keyboard, the colors are chosen randomly from the list of selected 12 colors.

- **Itertools** module is used to iterate over the list of selected colors to have the permutations of the colors selected for every 50 keys so that no two keys have the same permuted choice of colors.

3.4.2 Python Tools Used:

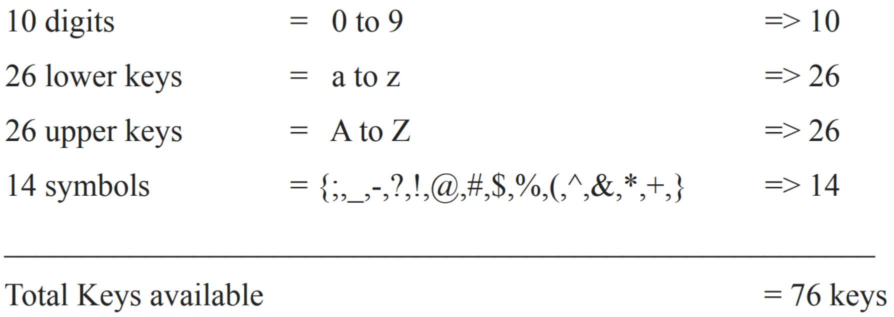
- **PyInstaller:** It is used to bundle the python application with its dependencies into a single package for the user to run the app without installing any python interpreter or module. This tool is used to convert our .py file into an executable file for the user to use our virtual keyboard without setting up the python environment on his/her machine.

- **Visual Studio Code:** The source code editor is used to develop the virtual keyboard and test the model by debugging the code and troubleshooting all the errors occurring while writing the code.

4 Analysis

4.1 PASSWORD SPACE/ COMBINATION:

Since total number of keys are:



10 digits	=	0 to 9	=> 10
26 lower keys	=	a to z	=> 26
26 upper keys	=	A to Z	=> 26
14 symbols	=	{;,_,-,?,!,@,#,$,%,(,^,&,*,+,}	=> 14
Total Keys available			= 76 keys

Since password space is also dependent on sectors and colors so it comprises 12 colors in the outer sector, 12 colors in the inner sectors, and 8 sectors considering the average password length lies between 6 to 15 digits. Therefore,

$$PasswordSpace(S) = \sum_{L=6}^{15} \left(12 * 12 * 8 * (76)^{L}\right) \simeq 1.9028 * 10^{31} \tag{1}$$

As you can see, our method is almost 1000 times better than the existing method proposed by Chen, and Yi-Lun[1] and hence provides a better variety of password options including more combinations.

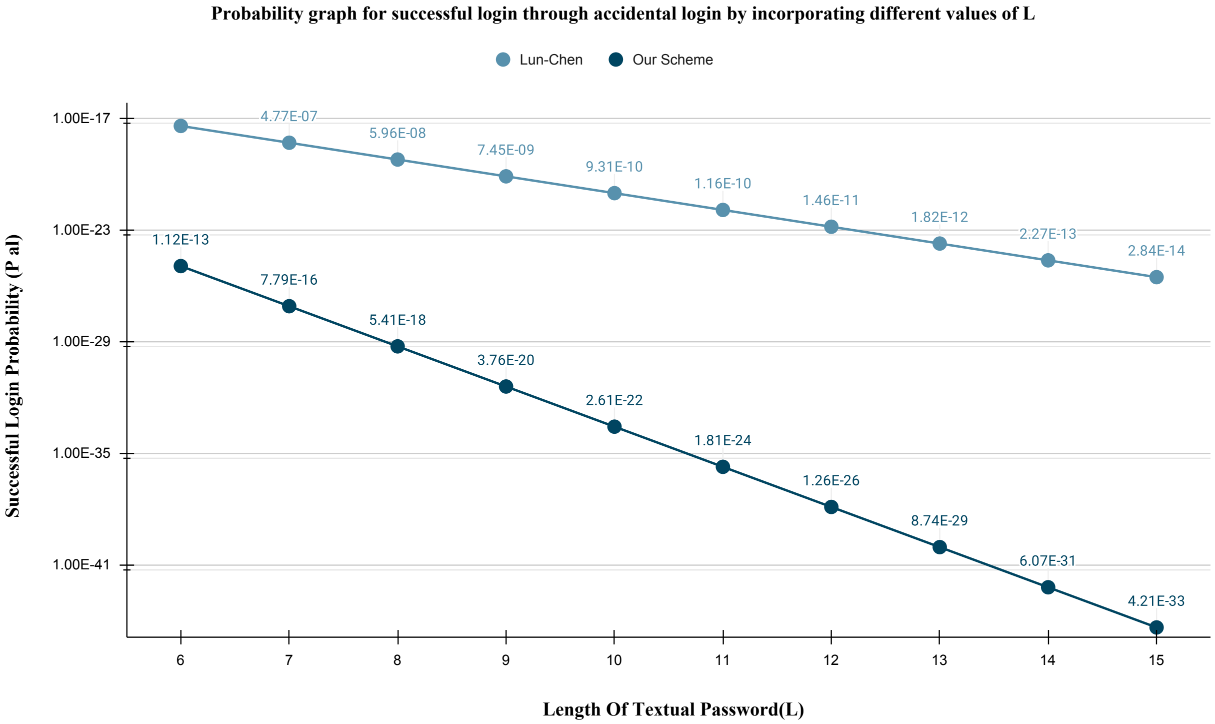
4.2 RESISTANCE TO ACCIDENTAL LOGIN:

Considering that the correct sector is already known by the adversary, then the probability for logging in accidentally for the given password length(L) is Pal(L),

$$P_{al}\left(L\right) = \left(\frac{1}{12} * \frac{1}{12}\right)^{L} = \left(\frac{1}{144}\right)^{L} \tag{2}$$

Assuming length L=10

$$P_{al}\left(10\right) == \left(\frac{1}{144}\right)^{1} {}^{0} = 2.608 * 10^{-31} \tag{3}$$



Password length L→	6	7	8	9	10	11	12	13	14	15
Our Figures	1.12E-13	7.79E-16	5.41E-18	3.76E-20	2.61E-22	1.81E-24	1.26E-26	8.74E-29	6.07E-31	4.21E-33
Lun Chen[1]	3.81469e-6	4.76837158e-7	5.96046448e-8	7.4505806e-9	9.3132257e-10	1.1641532e-10	1.4551915e-11	1.8189894e-12	2.2737368e-13	2.8421709e-14

Fig.6 Graph for Resistance to accidental login

In any case, since the length of the password is confidential, firstly the adversary needs to figure out length of password. As an assumption for even distribution of the lengths of the passwords is accepted uniformly between the range of 6 and 15, the likelihood that the enemy accurately surmises the secret word length is 1/10. Accordingly, the probability of accidental login for the proposed scenario is,

From L=6 to L=15,

$$P_{al} = \frac{1}{10} \sum_{L=6}^{15} P_{al}(L) \tag{4}$$

which on calculation leads to

$$P_{al} = 1.129 * 10^{-14} \tag{5}$$

which in turn is a very very small number for a real-world scenario.

Scenarios and their Summation for accidental login over L=6 to 15	Our Scheme	Lun-Chen's Approach
Sector Compromise	1.129*E-14	4.35*E-7
1 Color Compromise	1.289*E-13	4.35*E-7
2 Colors Compromise	4.359*E-7	Not Applicable
Sector + 1 Color Compromise	3.65*E-8	Direct Password Leak

Moreover, since our keyboard can be used for logging-in in third parties applications also, therefore their Rate-Limiting of passwords will add an extra advantage. Thus, accidental/coincidental login could not be performed efficiently easily .
Now coming to the comparison part, as discussed by Chen, and Yi-Lun[1] in their paper, if we keep on increasing the length of the password, it becomes tougher and tougher with each try as the chance of accidental login according to the password of length L=15 is 2.84E-14 whereas, in our method for the same length, the chances are 4.21E-33 which itself creates a huge difference.

4.3 USABILITY

The client picks conventional text passwords and one sector as his secret phrase in the proposed plot. As most clients know about printed passwords, it is for the most part simpler for the client to track down characters than symbols on the keyboard. And, the activity of the suggested method is straightforward and simple to learn, the client just needs to pivot the colors clockwise or counterclockwise for each key in the password to log in with their password.

4.4 ALGORITHM

```
**Algorithm 1** Graphical Password
$Input(Sector, OuterColor, InnerColor)$
$Submit = 0$
while Submit==0 do
    if $letter\ is\ UpperCase$ then
        Click On CapsLock Button
    end if
    if $SectorOuter = OuterColor\ and\ SectorInner = InnerColor$ then
        Click On Select Button
        Submit=1
    else
        while $SectorOuter \neq OuterColor$ do
            Rotate Outer Circle Clockwise or Anti-clockwise
        end while
        while $SectorInner \neq InnerColor$ do
            Rotate Inner Circle Clockwise or Anti-clockwise
        end while
    end if
end while
Exit
```

Thus, based on our thorough examination of the proposed method, we discovered that, when compared to the existing method of shoulder surfing prevention using graphical passwords, our method significantly reduces the likelihood of successful shoulder surfing attacks.

5 Conclusion

We suggest a simple text-based shoulder surfing resistant graphical password in this research, which allows the user to finish the login procedure fast and conveniently while avoiding shoulder surfing attacks. The operation of the suggested technique is basic and easy to understand for users who are accustomed to textual passwords. Without utilizing a physical keyboard, the user can swiftly and conveniently log into the system. Finally, we looked at how resistant the suggested method is to shoulder surfing. We were able to create a strategy that considerably reduced the possibilities of shoulder surfing when compared to previous methods. A limitation of the method proposed in the paper is that the amount of time required to enter a password increases as a number of steps must be followed while entering the password key. In addition, in order to successfully avoid the attack of shoulder surfing, the user must remember a number of variables in our method.

6 Reference

1) Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry by Lee, Mun-Kyu. "Security notions and advanced method for human shoulder-surfing resistant PIN-entry." IEEE Transactions on Information Forensics and Security 9, no. 4 (2014): 695-708

2) Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected: Kwon, Taekyoung, Sooyeon Shin, and Sarang Na. ("Covert attentional shoulder surfing: Human adversaries are more powerful than expected." IEEE Transactions on Systems, Man, and Cybernetics: Systems 44, no. 6 (2013): 716-727.)

3) A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme by Chen, Yi-Lun, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao. "A simple text-based shoulder surfing resistant graphical password scheme." In 2013 International Symposium on Next-Generation Electronics, pp. 161-164. IEEE, 2013

4) Dhanashree Kadu, Shanthi Therese, and Anil Chaturvedi "Different Graphical Password Authentication Techniques." International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017).

5) Graphical password authentication using hybrid pin keypad Hemamalini, M., and R. Saranya. "Graphical password authentication using hybrid pin keypad." Malaya Journal of Matematik (MJM) 1, 2019 (2019): 554-559

6) https://imgupscaler.com/

7) https://www.privacysense.net/terms/shoulder-surfing/

8) https://www.lifelock.com/learn/identity-theft-resources/what-is-shoulder-surfing

9) L. Sobrado and J. C. Birget, “Graphical passwords,” The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

10) L. Sobrado and J.C. Birget, “Shoulder-surfing resistant graphical passwords,” Draft, 2005.

11) S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.

12) H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, “Design and analysis of a graphical password scheme,” Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.

13) B. Hartanto, B. Santoso, and S. Welly, “The usage of graphical password as a replacement to the alphanumerical password,” Informatika, vol. 7, no. 2, 2006, pp. 91-97.

14) S. Man, D. Hong, and M. Mathews, “A shoulder surfing resistant graphical password scheme,” Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105- 111 .

15) T. Perkovic, M. Cagalj, and N. Rakic, “SSSL: shoulder surfing safe login,” Proc. of the 17th Int. Conf. on Software, Telecommunications Computer Networks, Sept. 2009, pp. 270-275.

16) Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.

17) T. Yamamoto, Y. Kojima, and M. Nishigaki, “A shouldersurfing-resistant image-based authentication system with temporal indirect image selection,” Proc. of the 2009 Int.

18) H. Zhao and X. Li, “S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.

19) B. R. Cheng, W. C. Ku, and W. P. Chen, “An efficient login-recording attack resistant graphical password scheme Sector-Login,” Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.

20) M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. “Authentication schemes for session passwords using color and images,” International Journal of Network Security Its Applications, vol. 3, no. 3, May 2011.

21) S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. “A new shoulder-surfing resistant password for mobile environments,” Proc. of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.

22) Z. Imran and R. Nizami, “Advance secure login,” International Journal of Scientific and Research Publications, vol. 1, Dec. 2011.

23) M. K. Rao and S. Yalamanchili. “Novel shoulder-surfing resistant authentication schemes using text-graphical passwords,” International Journal of Information Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012 .

24) Network Working Group of the IETF, “The Secure Sockets Layer (SSL) Protocol Version 3.0,” RFC 6101, 2011.

25) Network Working Group of the IETF, “The Transport Layer Security (TLS) Protocol Version 1.2,” RFC 5246, 2008

26) Y. Abdrabou, M. Khamis, R. M. Eisa, S. Ismael and A. Elmougy, "Engage: Resisting shoulder surfing using novel gaze gestures authentication", Proc. of the 17th International Conf. on Mobile and Ubiquitous Multimedia, 2018

27) Y. Abdrabou, M. Khamis, R. M. Eisa, S. Ismail and A. Elmougy, "Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication", Proc. of the ACM Symp. on Eye Tracking Research Applications, 2019.

28) L. Bosnjak ˇ and B. Brumen, "Shoulder surfing experiments: A systematic literature review", Computers Security, 2020.

29)F. Brudy, D. Ledo, S. Greenberg and A. Butz, "Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays through Awareness and Protection", Proc. of The International Symposium on Pervasive Displays PerDis ’14, 2014.

30) A. De Luca, E. von Zezschwitz, L. Pichler and H. Hussmann, "Using Fake Cursors to Secure On-Screen Password Entry", Proc. of the SIGCHI Conf. on Human Factors in Computing Systems CHI ’13, 2013.

31)M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers", Proc. of the SIGCHI Conf. on Human Factors in Computing Systems CHI ’17, 2017.