New Textual Authentication Method to Resistant Shoulder-Surfing Attack

Islam Abdalla Mohamed Abass[1], Loay F.Hussein[2], Tarak kallel[3], Anis Ben Aissa[4]
Department of Computer Science, Jouf University[1, 2, 4]
Department of Physics, Jouf University[3]

***Abstract*—Using textual passwords suffer from the balance between security and usability. Password policies are usually adopted by system administrators to force users to choose strong passwords. However, users often use a simple password to make it easy to remember, which reduces the password strength and make it vulnerable to information security threats. When users enter their passwords in public places like airports or cafes, they become exposed to shoulder surfing attacks which are considered as a kind of social engineering. With a little effort, an attacker can capture a password by recording the individual's authentication session or by direct observation. To overcome this vulnerability, we propose a new textual-password approach that uses camouflage characters and a virtual keyboard which leads to generating strong and easy to remember passwords. The perspective of usability and security was evaluated by experimental studies conducted with 65 users and then compared with recent studies. The results showed that the proposed technique has the lowest shoulder surfing success rate with just 3.63% with reasonable usability.**

***Keywords*—Shoulder surfing; caesar cipher; virtual keyboard; graphical password; social engineering**

I. Introduction

Current authentication systems have a lot of weaknesses even if the system is secured, an individual's behaviour may cause a security breach. Users usually pick a short or easy password to remember, which makes their accounts vulnerable to attack and easily guessable. On the other hand, longer passwords are harder to memorise and to type correctly [1][2]. To consider a password as strong it must have eight characters or more, contain numbers, special characters mixed with small and capitalize alphabets [3].

By adding the human factor to the equation of security and how easily social engineering can manipulate the user, textual passwords become vulnerable to spyware attacks, keyloggers, dictionary attacks, and shoulder surfing attacks [4]. Most individuals are aware of security threats but they insist to avoid them. A survey reported that 90% of 152 computer users leaked their passwords. In this situation, forcing the user to create a password according to strict policies will not solve this issue [5]. To overcome the limitations of text-based passwords, many techniques such as two-factor authentication and graphical passwords are used [6]. Moreover, using input devices such as the mouse and touch-screen makes graphical authentication techniques possible. Unfortunately, they are unsecured to many attacks such as shoulder-surfing, spyware, Social Engineering and Dictionary attacks.

Shoulder surfing attack is a type of identity theft, it occurs when the attacker looks over someone's shoulder to get passwords, login PINs or other sensitive personal data. This attack can also be done by a small wireless camera that is easy to install. To overcome this problem, a wide range of research efforts have been done on eye-tracking algorithms. Systems login that is based on gazing to select a character from an on-screen keyboard is one of the solutions for shoulder-surfing but it may take a long entry time and lack of input accuracy [7]. Another approach to solve this problem is using a graphical password or integrating both graphical and textual passwords [8][9].

Graphical password has been widely used, especially on smartphones. An Individual can unlock his smartphone after the correct pattern is mapped out on a three-by-three rectangle, as in Fig. 1. As shown in Fig. 2 all the authentication Graphical methods can be grouped into three categories:

1) Recognition-based system: in this method users can login by choosing the correct photo from a list at the signup time [10].

2) Hybrid system: this method combines more than one schema to eliminate their issues and produces a more stable and useful system [11].

3) Recall-Based system: this method asks the user to draw or write something to use it as the Authentication code. There are two types of Recall base systems:

a) The Pure Recall method is relayed on the user to give the right authentication code at the login time [12].

b) Cued Recall method is based on helping the users to login by giving them a hint to remember their passwords [12].

However, most login graphical techniques may suffer from a complicated algorithm or need a special device, which increases the need to develop a new secure login method.

In this paper, we first discuss the shoulder surfing attack as a part of social engineering, then propose a defensive model that can resist shoulder surfing attacks. The defensive model is designed on the concept that the user can enter random camouflage characters by using a virtual keyboard. The character of the virtual keyboard is shifted by using Caesar cipher which is used to encrypt and decrypt the user input. After applying an experimental study to test the defensive model with 65 participants and analyzing the data, the conclusion is presented to summarize the primary outcomes and to determine model usability and efficiency against shoulder surfing attacks.

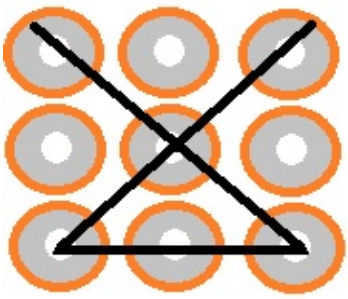

Fig. 1. Touchpoints Pattern to Unlock Smartphone.

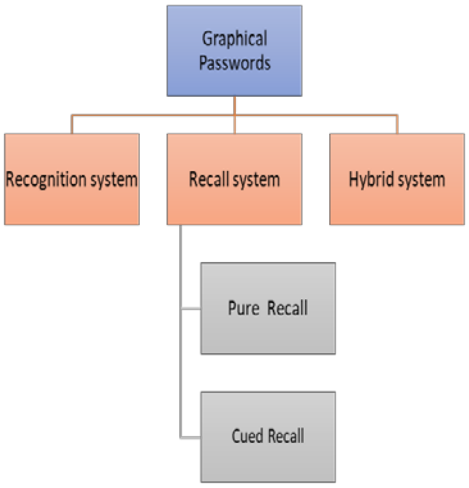

Fig. 2. Categorization of Authentication Methods for the Graphical Password.

II. Related Work

Graphical password authentication systems that depend on recognition based and recall based schema has been adopted in many research to fight against shoulder surfing attacks. In [13], Jiya Gloria Kaka et al. compared 10 graphical authentication methods based on three common attacks and the usability features. Although, most of the authentication systems have acceptable usability only three methods were effective against shoulder surfing attacks.

In [14], Jianwei Lai et al. introduce a unique authentication scheme that resists shoulder-surfing attacks. The scheme is based on textual passwords, so to login, the user will enter part of the password and skip the password character that is marked with 'x'.

Aakansha S. Gokhale et al. developed a new graphical password authentication technique that resists shoulder surfing, brute force and guessing attacks [15]. The authentication technique is based on three questions related to 25 pictures. In the login phase, the user must click on the correct location in the image for every question. The system has a very large password space equal to 8.367939e+34 which can provide a strong secure password.

In [16], Dongmin Choi et al. discussed five model's authentication schemes against shoulder surfing and social engineering attacks. The paper compared defensive types; QWERTY based Secure Keypad, ABC based Secure Keypad, Touch and Slide Secure Keypad, colour-based Secure Keypad and Random Secure Keypad. As a result, the five techniques were weak against shoulder surfing attacks.

Aravinda Thejas Chandra et al. developed an authentication system based on eye-tracking and a smart camera [17]. The gaze-based PIN identification application was tested on a nine-digits keypad by using real-time eye-tracking to login. Although it can be used as a defensive mechanism against shoulder surfing, the paper did not study the medical effect of the system on the user's eyes for a long period of using special if the password is more than 6 characters.

In [18], Anindya Maiti et al. proposed a defensive model based on a random alignment keyboard with twenty-six alphabets created by an augmented reality wearable device. The model involves three different randomization strategies, each one of them can shift the 26 characters to produce a new virtual keyboard. Although the system is effective as a defensive mechanism against side-channel and shoulder surfing attacks, it requires a secured wireless channel and special hardware.

Eiji Hayashi et al. designed a novel secure mechanism for user authentication that can be used with any screen size [19]. In the proposed model the user chooses a set of images as a graphical password. To login, he must choose his distorted images from the set of images. This authentication technique relies on the fact that human perception is influenced by his information. Despite the simplicity of the method used, it is effective against social engineering and shoulder surfing attacks.

Vishal Kolhe et al. introduced an authentication system based on a 3D password [20]. The 3D password is a multi-passwords system that combines a textual password with a graphical password in a virtual environment. Users can move in a virtual environment to create their passwords. Although the model provides secure authentication and user friendly, it has many disadvantages like time, memory requirement and cost. The system provides immunity against brute force attacks and key loggers but is still vulnerable to shoulder surfing attacks.

Hung-Min Sun et al. introduced a graphical authentication system for smartphones called PassMatrix [21]. The system consists of many components:

- Password verification module.
- vertical and Horizontal axis control module.
- Login indicator generator module.
- Image discretization module.
- Communication module.
- Database.

The images which are used to login are divided into horizontal (1-11) and vertical axis (A-G) grids. To login, the user must circle his hand on the screen to get the generated key or listen to an audio that contains the generated key by using earbuds or a Bluetooth headset. The audio is sent from the

server using a secure channel, then the user must shift the character to match the key. This procedure is repeated until the login is finished. The total accuracy of all login trials is 93:33% which means it can be used to defend against smudge attacks and shoulder surfing attacks.

III. Social Engineering and Shoulder Surfing Attacks

Social engineering is an attack that depends on the human factor. It's classified as a non-technical attack in general. However, it can be combined with technical types of attacks like Trojan and spyware, which makes it more effective [22]. Cyence, a cyber security analyst company reported In 2016, that the United States was the most targeted country with social engineering attacks and had the highest attack cost, followed by Japan and Germany. The total cost of these attacks in the US alone was $121.22 billion [23].

Shoulder surfing is a kind of social engineering. It can be performed by using technical and non-technical ways. Although shoulder surfing attack can be noticed by the victim, it could be combined with other types of attacks like spear-phishing and dumpster diving which makes it a powerful attack. A survey was done in the US, Germany, and Egypt concluded that 67.4% of Shoulder surfing occur in public places and 74.1% of the observer were strangers [24]. Depending on the Humans nature people act like that for different reasons such as curiosity, boredom or to get private data. Some companies produce special screens that make it difficult to see the smartphone or computer screen from an angle to keep the privacy [25]. This screen can be useless when the attacker uses a small hidden camera that can capture video and send it directly to the attacker. Although there are multi-solutions to solve the shoulder surfing problem, they are suffering from common issues such as:

1) The most common software and operating system use alphanumerical usernames and passwords for authentication, which makes it difficult to apply random security algorithms.

2) Some graphical password Algorithms used in systems are vulnerable to shoulder surfing and other types of attacks [26].

3) Adding layers of security or complex authentication systems decreases the usability and functionality of the system.

4) The common careless behaviours like writing down a password or using the data autofill technique make security solutions worthless.

IV. Proposed Defense Model

In this study, two different models were designed, a shoulder surfing defensive model and a traditional login system that contains just a password with eight characters and a username. The proposed defensive model is based on camouflage characters and a virtual keyboard with shifted alphabetic as shown in Fig. 3.

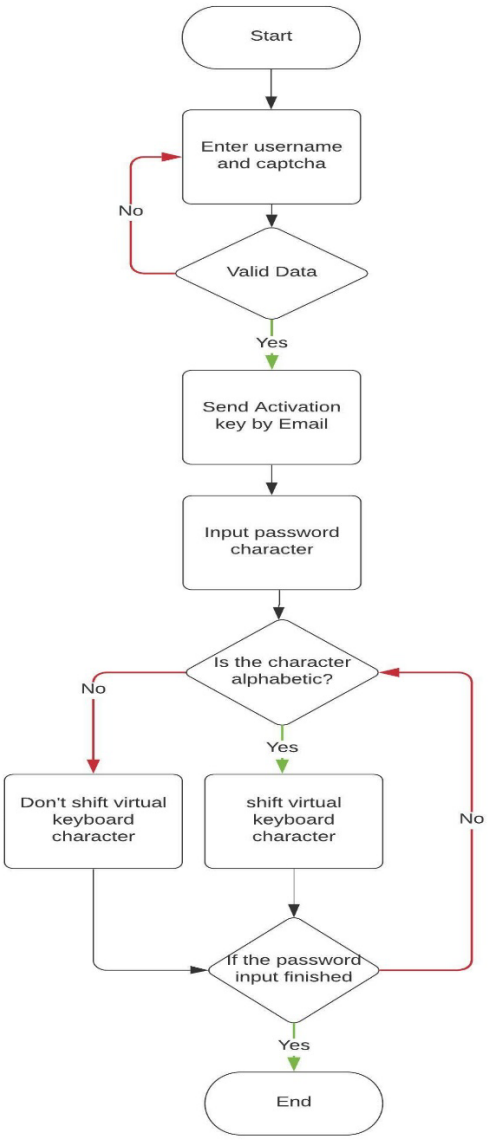

Fig. 3. The General Authentication Mechanism.

The virtual keyboard uses Caesar cipher to shift the 26 alphabetic, while the rest of the keyboard keys which are coloured with blue will be static and will act as normal keys as in Fig. 4. Caesar cipher is a simple substitution cipher that uses the same key for encryption and decryption [27]. Depending on the symmetric key letters are shifted a certain number of places down the alphabet. If the shift exceeds the number of the alphabet, the alphabet will just be rotated to the front. The alphabet in the proposed model is arranged in horizontal lines according to the QWERTY keyboard, so the first alphabet is q and the last is m. The result of Caesar cipher will be according to the QWERTY keyboard not to the normal alphabetic sequence. This system also applies another layer of protection by adding camouflage characters to the real password. The user authentication process is divided into two phases as follows.

Fig. 4. The Virtual QWERTY Keyboard.

A. Registration Phase

1) The user must enter eight characters password, username, and email to register an account as in Fig. 5.

2) The traditional system will just use the password and the username to login as in Fig. 6.

B. Login Phase

1) For authentication, the user must enter his username and captcha character as in Fig. 7. After that, the server will send the activation key to the users' email. The activation key (AK) will be random from 1 to 9 and it mustn't be in the password that has already been entered by the user in the registration phase.

2) In the Caesar encryption algorithm, the encryption key (k) will be chosen randomly from 1 to 10 to shift the character in the virtual keyboard. In the encysting process, x is the character number in the virtual keyboard and k will be fixed in each authentication session as in Eq (1).

$$En(x) = (x-k) \bmod 26 \quad (1)$$

3) Every time the user enters an alphabetic character, the virtual keyboard will shift only the alphabetic character's position according to the Caesar cipher. Note that the virtual keyboard will shift after pressing alphabetic keys and will not shift, if the user enters a number, special symbols or press any other button. The user password must be written by the physical keyboard, but according to the virtual keyboard character. For example, if the first password character is 'x', the user will press 'k' on the physical keyboard as shown in Fig. 8.

4) The user will combine his real password with a camouflage character by using the activation key followed by a character equal to the value of the activation key. For example, if the activation key was 5 and the user password was xAvd4$141 the user could enter 5t!C3wxAvd4$141, xAvd4$1415t!C3w or xAv5t!C3wd4$141 as his password. The sequence 5t!C3w will be used as a camouflage for the password and can be added at any position to the real password.

5) After entering the password the decryption key will equal the number of entered alphabetic multiplied by the encryption key. For example, if the encryption key was 3 and the user entered 5 alphabetic the decryption key would be 15.

6) Finally, when the user submits the system will Decrypt the password by using Caesar decrypt equation as in Eq (2). Note that the password will be decrypted from right to left and the decryption key will be subtracted from the encryption key after decrypting each alphabetic. For example, if the decrypt key is 33 and the password is 'tupert24wertq', the letter 'q' will be decrypted with k equal 33 and 't' with k equal to 30. Then the system will omit the camouflaged character from the password to get the real password.

$$Dn(x) = (x-k) \bmod 26 \quad (2)$$

As a result of this approach, if a person tries to comment shoulder surfing attack, he will not succeed; because the arrangements of the alphabet change after every click and the password is protected by the camouflaged character. Also, this technique is powerful against the keylogger that takes screenshots after each input.

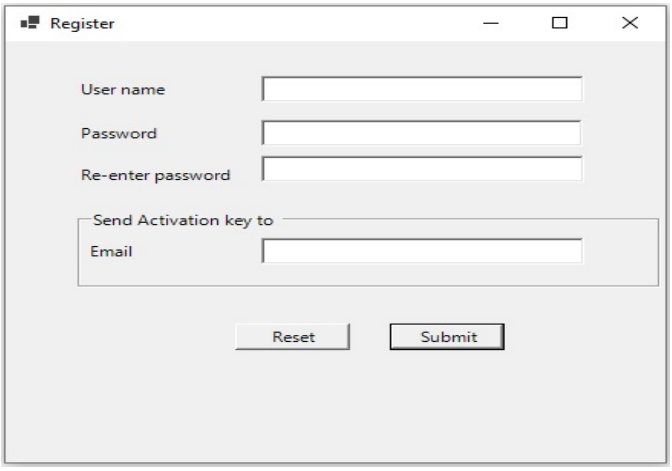

Fig. 5. System Register Screen.

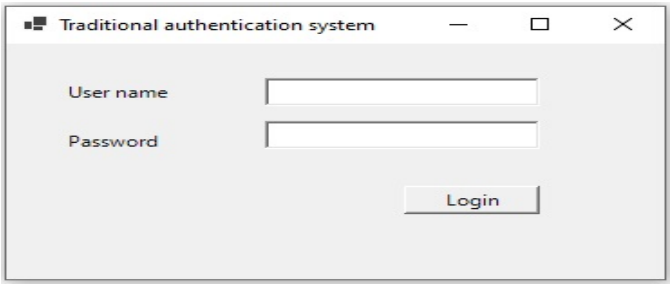

Fig. 6. Traditional System Login Screen.

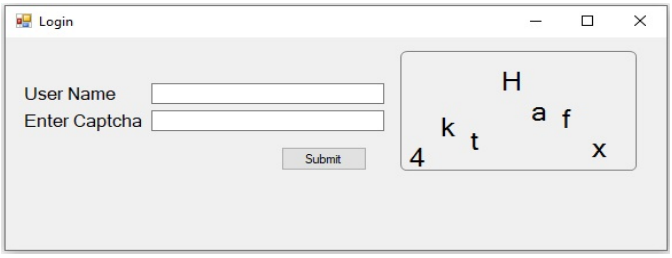

Fig. 7. Defensive Model Login Screen.

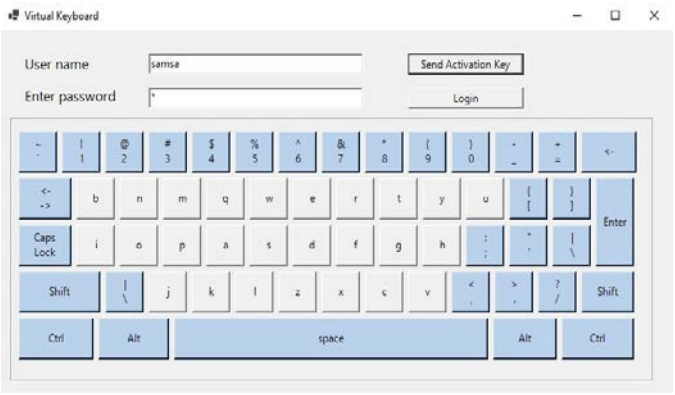

Fig. 8. The Virtual Keyboard when k=3.

V. Experimental Study

The experimental study aims to evaluate the model against shoulder surfing attacks and to measure the usability of the proposed techniques. The following explains the experimental details:

1) Design two applications; the first, with a traditional login system, and the second, is based on the virtual keyboard; to be able to evaluate the proposed defensive techniques against shoulder surfing.

2) The experiment was done in a controlled environment in the lab and all participants entered 8-character passwords in both systems.

3) Experimental study with 65 participants divided into 20 PhD holders and 45 students. fifty-five of the participants will act as ordinary users, and 10 will act as shoulder surfing attackers. The experiment began with a brief explanation of the proposed defensive techniques. To become familiar with the system, the 55 participants are allowed to create their passwords and then login to the system approximately 3 times. Also, the 55 participants were informed that they are just allowed three attempts to login each time with each a count. If the three attempts failed, the account would be locked and the user has to try to login with a new account.

4) Measuring the success rate of the attack will clarify the models' susceptibility to shoulder surfing. To accomplish that, the 55 participants acted as victims, with 5 random students and 5 PhD holders acting as shoulder surfer attackers. The efficiency of the model is determined by analyzing and comparing the shoulder surfing success rate of the experiment with other studies.

VI. Results

To determine the model's usability two factors must be measured, entering time and login success rate. The success rate of the shoulder surfing attack will evaluate the model defensive technique. The result of these factors is used to compare four systems: The suggested traditional system which depends on static username and password memorized by the user, the defence proposed model and two models from other studies. For simplicity, the traditional login system will be represented with M1 and the defensive model with M2. While the M1 password has a fixed number of characters which is 8, the M2 password is between 10 and 18 characters.

A. Entring Time

The average time of the M1 model was 22.78, while M2 was 32.62 seconds as shown in Table I. The min and max time of the M1 system was 19.8 and 27.2 seconds, while in M2 was 30.1 and 36.6 seconds. The standard deviation (SD) in the entring time test of the two models was almost equal. By comparing the result it's clear that the M1 system is easier to use than the M2 model. Although the M1 test was better it has a fixed number of characters which is 8, while M2 has more characters even if the AK equals one. In general, the test result is affected by two factors:

1) The user typing speed.
2) The number of characters of the password.

B. The Success Rate of Login

The login success rate is calculated by dividing the overall success login attempts over the total of all attempts of one participant. All 55 participants have given 3 attempts for login and they repeated this process for 5 different accounts. Table II shows the SD and mean values for M1 and M2 models. By comparing the mean value, M1 is better than M2 by 0.015. However, all participants have used the M1 model before in their life which makes it the most familiar model to them.

C. Success Rate of Shoulder Surfing Attack

The experiment of shoulder-surfing attack was performed by 10 attackers and 55 users represent the victims. To keep the experiment real just 25 of the users were told that they will be watched to capture the login data. The attacker has to get the exact password and guessing is not allowed. The M1 model value was very high with 80.1%, while the defensive model M2 was 3.63% as shown in Table III.

The conducted result compared to the most related studies in terms of resisting shoulder surfing attacks and usability, support the M2 model technique in defending against shoulder surfing attacks as shown in Table IV.

TABLE I. The Results of Entering Time in Seconds

Model	Min	Max	Mean	SD
M1	17.8	25.2	22.78	3.76
M2	30.1	36.6	32.62	3.25

TABLE II. The Results of the Login Success Rate

Model	Mean	SD
M1	0.961	0.39
M2	0.946	0.44

TABLE III. The Results of the Shoulder-surfing Success Rate

Model	shoulder-surfing success rate
M1	80.1%
M2	3.63%

TABLE IV. PROPOSED MODELS RESULT COMPARE TO OTHER STUDIES

Study	Entry Time	Success Rate of login	The success rate of shoulder surfing
Proposed models			
M1	22.78	96.1%	80.1%
M2	32.62	94.6%	3.63%
Other studies			
[28]	23.2	64%	26.4%
[29]	3.66	97%	16%

VII. DISCUSSION

In this section, we analysed the data collected from the 65 participants, 55 acted as normal users and 10 as attackers. The M1 model has a faster entry time and a higher log in success rate than the M2 model; which makes the M1 a more friendly system. However, the M1 system is vulnerable to shoulder-surfing threats by 80.1% while M2 scores just 3.63%. The outcome obtained from the experiment indicates that using a visual keyboard with camouflage characters is a good defensive mechanism against the shoulder-surfing attack. It might be worth mentioning that the delay in M2 entry time is happening because the user must first check his email to get the AK key, then he must enter the password according to the dynamic virtual keyboard. This result is not enough to conclude that the M2 model is the best approach against shoulder-surfing, so it should be evaluated with other models [28][29] that are designed to fight against shoulder surfing. By comparing all models, it's obvious that the defence model M2 is the best defensive model with a success rate of shoulder surfing attack equal to 3.36%. However, it's the worst in entry time As shown in Fig. 9. Note that in the M2 model, the user must enter the password every time and can't use the autofill technique. Also, the model M2 aims to improve protection against shoulder surfing attacks, if it is done with human eyes or electronic devices like cameras. Furthermore, regardless of the defensive technique used users' behaviour is considered as the first line of defence against shoulder surfing attacks.

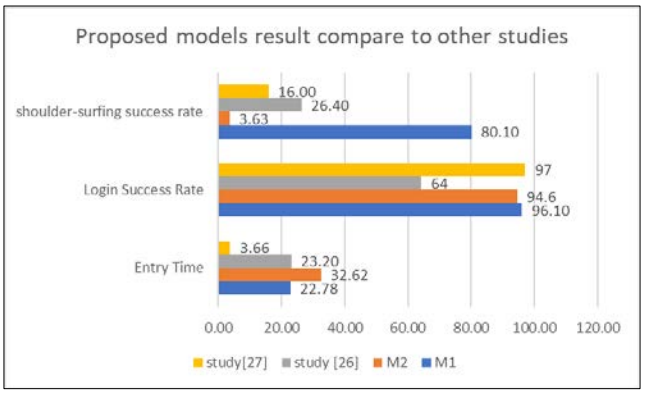

Fig. 9. The Proposed Model Result Compared to other Studies.

VIII. CONCLUSION

In this paper, a new model that relies on camouflage characters and a virtual keyboard combined with the Caesar cipher is proposed as a defence method against shoulder surfing attacks. An experiment with 65 users was conducted to evaluate the proposed defence model against a traditional login model. The evaluation depends on two factors: usability and the shoulder-surfing success rate. The results of the developed model were compared with two other studies that focus on shoulder surfing defence and use the same factors to measure their models. The obtained usability test indicates that the proposed defence model has the highest entry time compared to the other system, but it has the best result in preventing shoulder surfing. Depending on the results, the proposed defence model is recommended as the best solution for shoulder surfing attacks.

REFERENCES

[1] Dinei Florencio, and Cormac Herley, "A large-scale study of web password habits," Proceedings of the 16th international conference on World Wide Web, pp. 657–666, 2007.

[2] J.Yan, A. Blackwell, R. Anderson and A. Grant, "Password memorability and security: empirical results," IEEE Security & Privacy, vol. 2,pp. 25-31, 2004.

[3] Krishnapriyaa Kovalan et al., "A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users," International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, 2021.

[4] Eugene H.Spafford, "OPUS: Preventing weak password choices," Computers & Security, vol. 11, pp. 273-278, 1992.

[5] Ari Kusyanti and Yustiyana April Lia Sari, "Creating and Protecting Password: A User Intention," International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017.

[6] Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle," Comparison of Graphical Password Authentication Techniques," International Journal of Computer Applications, vol. 116, no. 1, 2015.

[7] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing shoulder-surfing by using gaze-based password entry," Proceedings of the 3rd symposium on Usable privacy and security,pp. 13-19, 2007.

[8] Cheryl Hinds and Chinedu Ekwueme, "Increasing security and usability of computer systems with graphical passwords," Proceedings of the 45th annual southeast regional conference, pp. 529–530, 2007.

[9] Huanyu Zhao and Xiaolin Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," 21st International Conference on Advanced Information Networking and Applications Workshops, 2007.

[10] Siddeeq Ameen Yousif and Laith Jasim Saud, "Computing Nodes and Links Apperances on Geodesics in Networks Topologies Using Graph Theory," Iraqi Journal of Computers Communications Control and Systems Engineering, vol. 12, no. 1, 2012.

[11] Salim Istyaq and Khalid Saifullah, "A new hybrid graphical user authentication technique based on drag and drop method," International Journal of Innovative Research in Computer and Communication Engineering, vol. 6, 2016.

[12] Suliman A. Alsuhibany, "Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns," Journal of Ambient Intelligence and Humanized Computing, pp. 1645-1655, 2020.

[13] Jiya Gloria Kaka, Oyefolahan O. Ishaq and Joseph O. Ojeniyi, "Recognition-Based Graphical Password Algorithms: A Survey," IEEE 2nd International Conference on Cyberspac, 2021.

[14] Jianwei Lai and Ernest Arko, "A Shoulder-Surfing Resistant Scheme Embedded in Traditional Passwords," Proceedings of the 54th Hawaii International Conference on System Sciences, p. 7144, 2021.

[15] Aakansha S.Gokhale and Vijaya S.Waghmare," The Shoulder Surfing Resistant Graphical Password Authentication Technique," Procedia Computer Science, vol. 79, pp. 490-498, 2016.

[16] Dongmin Choi, Chang Choi and Xin Su," Invisible Secure Keypad Solution Resilient Against Shoulder Surfing Attacks," 10th International

Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2016.

[17] Aravinda Thejas Chandra, G. Sneha, Srushti Anand and C. Yashaswini developed, "Real Time Eye Blink Password Authentication," International Journal of Research in Engineering Science and Management, vol. 4, no.7, 2021.

[18] Anindya Maiti, Murtuza Jadliwala and Chase Weber," Preventing Shoulder Surfing using Randomized Augmented Reality Keyboards," IEEE International Conference on Pervasive Computing and Communications Workshops, 2017.

[19] Eiji Hayashi, Rachna Dhamija, Nicolas Christin and Adrian Perrig," Use Your Illusion: Secure Authentication Usable Anywhere," Proceedings of the 4th symposium on Usable privacy and security, pp. 35-45, 2008.

[20] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar and Pranjal Rathod, "Secure Authentication with 3D Password," International journal of Engineering Science and Innovative Technology, vol. 2, 2013.

[21] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System," IEEE Transactions on Dependable and Secure Computing, vol. 15, 2016.

[22] Islam Abdalla, "Social Engineering Threat and Defense: A Literature Survey," Journal of Information Security, vol .9, 2018.

[23] Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," Future Internet, 2019.

[24] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann and Florian Alt, "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers," Conference on Human Factors in Computing Systems, pp. 4254-4265, 2017.

[25] Mohamed Khamis, Malin Eiband, Martin Zürn and Heinrich Hussmann, "EyeSpot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing," Multimodal Technologies and Interaction, 2018.

[26] Arash Habibi Lashkari, Samaneh Farmand, Omar Bin Zakaria and Rosli Saleh, "Shoulder Surfing attack in graphical password authentication," International Journal of Computer Science and Information Security, vol. 6, no. 2, pp. 145-154, 2009.

[27] Tonni Limbong and Parasian D.P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab," International Journal of Engineering Research & Technology, vol. 6, 2017.

[28] Suliman A. Alsuhibany, "A Camouflage Text-Based Password Approach for Mobile Devices against Shoulder-Surfing Attack," Security and Communication Networks, 2021.

[29] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow and Heinrich Hussmann, "Swipin: fast and secure pin-entry on smartphones," Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 1403–1406, 2015.