Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://akademiabaru.com/submit/index.php/arca/index
ISSN: 2462-1927

Legibility Environment Factor for Shoulder-Surfing Resistant Authentication Scheme using Visual Perception of Graphical-based Authentication

Juliana Mohamed[1*], Mohd Farhan Md Fudzee[2], Muhamad Hanif Jofri[1]

[1] Department of Information Technology, Centre for Diploma Studies (CeDS), Universiti Tun Hussein Onn Malaysia, KM 1, Jalan Panchor, Muar, 84600, Malaysia
[2] Faculty of Information Technology and Computer Science (FSKTM), Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, Malaysia

ARTICLE INFO

Article history:
Received 21 June 2024
Received in revised form 21 July 2024
Accepted 18 August 2024
Available online 18 September 2024

Keywords:
Soulder surfer; authentication; legibility; enviroment factor; viewing angle; algorithm; legibility impact factor

ABSTRACT

Shoulder surfer is among the factors that make authentication unsecure. The physical transaction processes at automated teller machines (ATM) are the most likely to be vulnerable to shoulder surfer attacks. In addition, using an app through smartphone gives insecure situation to the user during any authentication activities. Legibility environment factors are one of the factors that affect legibility from the shoulder-surfer's viewing angle. The research focuses on Shoulder-Surfing Resistant Authentication Scheme using Visual Perception of Graphical-based authentication. The research is carried out by developing the algorithm of the authentication process. The research allows for auto-hiding or auto-glaring techniques to the algorithm and experiment so that a shoulder-surfer cannot be seen during authentication activities. The outcome satisfies the objective and is in accordance with the legibility impact factor. Based on the results, the research concludes that the strategy successfully reduces shoulder surfers' legibility outside of the safe zone to a crucial level.

1. Introduction

Authentication plays a pivotal role in information systems, especially in transactions involving current and personal accounts, necessitating heightened security measures. Ensuring high security and privacy requires a strong authentication system [6,17]. User authentication is the process in which individuals authenticate themselves in order to use online banking facilities. The identity of a user attempting to access an online system is confirmed through the use of user authentication techniques. There are several types of authentications; basically numerical-based authentication and graphical-based authentication [8]. These two are mainly used during authentication activities for its purpose and highly to be secured in digital environment. Authentication is crucially due to the potential for attackers to compromise vast amounts of personal data although there it is stored very securely [6,15,22]. Furthermore, the conventional use of automated teller machines (ATMs) presents

* *Corresponding author.*
E-mail address: julianaju@utm.edu.my (Juliana Mohamed)

https://doi.org/10.37934/arca.36.1.1019

vulnerabilities for attackers and data thieves. Thus, mobile online method gives impact to the user by its accessibility and security purpose.

1.1 Graphical-based Authentication

Normally, authentication involves numeric data to-be key in before any activities i.e. transaction or login apps being success. This activity gives more security and occurs practically to user. Although it provides more security to the user, it also tends to be lacking in its usability to user [14]. The existing authentication using numerical based frequently seen as lot of limitation in terms of capability and accessibility [7]. According to Kovalan *et al.*, [8], numerical-based authentication tends to be frustrated to the user by keying several numbers within sixteen seconds. Due to its limitation, attackers take it as an advantage for them to steal the information. Therefore, a solution of graphical-based authentication has been discovered to overcome the common problem.

Graphical-based authentication using Ishihara chart is seen as way to overcome the attacker especially shoulder-surfing attack. This solution not only works to protect against the attacker but it also gives an added value to the user by its usability. This works by the same method by keying the one-time password (OTP) of six numbers but representation in visually of a graphic to the authentication. The authentication will be repeated after sixteen seconds if the user can't catch up the time while keying the OTP. This idea at least will satisfy the user by the invention of key in the OTP rather than the conventional way.

1.2 Shoulder-surfing Attack

Attackers possess the capability to acquire user identification information and bypass authentication through various types. Attackers include those who use brute-force or guessing techniques, shoulder-surfing techniques, dictionary or password guessing techniques, malware or spyware techniques, and social engineering techniques. [10]. The actual user can be attacked using brute-force or guesswork in offline mode, such as when a smartphone's lock password is compromised. User IDs and passwords used to log into websites are examples of dictionary attacks or password guessing that target users online. Attacks using malware or spyware that target users using technological monitoring and social engineering user by illusion of recordability [16].

Shoulder surfing is a form of surveillance attack that occurs when authenticating with a mobile device. It is a type of observation attack in which an attacker tries to see a victim's authenticator as it is typed into the device [19]. One of the most frequently reported concerns of smartphone unlocking techniques is the shoulder surfing attack [13]. The physical transaction actions at the ATM are most vulnerable to shoulder surfing attacks [11].

Shoulder surfers will attack an authorized user who is being observed by a person via camera or video and will reveal the legal user's password. Furthermore, an authorized user is being watched over his or her shoulder for the password. A shoulder-surfing assault also employs an electromagnetic pulse scanner to monitor the keyboard or mouse on computers or cellphones. Meanwhile, it is possible that an individual's authentication session is being recorded by the shoulder surfer [2].

This research addresses the issue by presenting a suggested technique for an authentication process termed auto glare/auto hide. Environmental and display factors are the two categories of criteria that the study looks into when determining legibility. For this study, the result focuses on the environment factor which included include ambient brightness, viewing angle and distance.

2. Proposed Method and Algorithm

The research proposes a technique called Usable Access (UAce) that is consistent with authentication protocols [18]. UAce standard taking into account the features and qualities from the user authentication [21]. This method was appropriately adapted by USec (Usable Privacy and Security), which complies with ISO 9241-220 authentication standards [5,20]. Figure 1 depicts an illustration for UAce.

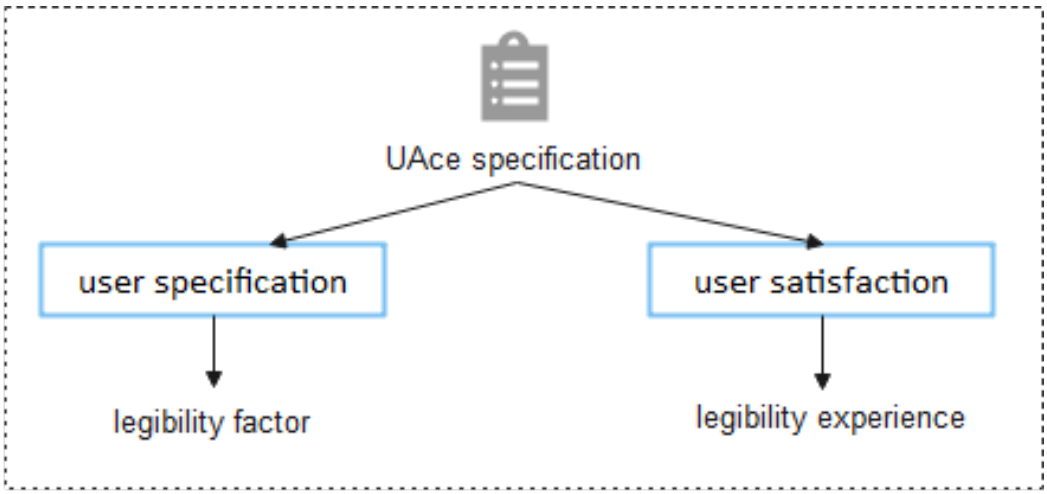

Fig. 1. UAce method

UAce specification includes two major factors: user specification and factor satisfaction. The user specification factor will be investigated with the legibility environment element. Next, the user happiness factor will be investigated, as well as the readability experience and legibility effect factor for the user and shoulder surfer. Consequently, a method has been presented throughout the authentication process. This technique is used in authentication procedures that need two factors of legibility. Figure 2 depicts the auto-glare or auto-hide configuration pseudocode. Table 1 also includes a collection of regularly used notations.

Algorithm 1: Auto glare/auto hide setting algorithm

INPUT: B, α, α_x, $\emptyset$, E, s
OUTPUT: β, S_i
BEGIN
1: B ◄—α
2: $\alpha_0 = 5\ \alpha\frac{0.86}{x}$ //brightness value based on ambient brightness;
3: **FOR** α_0 **DO**
4: **IF** max $\emptyset$ **THEN** //maximum viewing distance;
5: $\alpha = \alpha_x + \frac{\max\emptyset}{\emptyset}$. (α_0 - α_x) //calculate the optimal brightness at current distance;
6: **ELSE**
7: request E from s
8: Authentication successful (β, S_i, $\emptyset$)
9: accepted by s
10: **END IF**
11: **END FOR**
END

Fig. 2. Auto glare/auto hide setting algorithm

Figure 2 illustrates the settings for auto glare/auto hiding during the authentication operations. The operation began with the input quantity of inbound requests, which were then sorted based on the ambiance luminance task. Later, the server will load and broadcast the offer after the brightness value is initiated depending on the ambient brightness. This process assumed that the provider's system, which handled the incoming tasks, had access to this information. Each activity will have its ideal brightness computed at the present distance. The number of jobs that can be completed within the claimed wait time may be approximated using the current server load. This indicates that the surgery will be successful. Table 1 presented the abbreviation for Algorithm 1.

Table 1
List of Frequently Used Notation

Notation	Descriptions
α	Ambience luminance
αx	Ambience luminance task
ø	View distance
β	Targeted screen brightness
s	Server load
B	Request
E	Estimated time
Si	Authentication settlement

3. Result and Discussions

This section goes into further detail on the experiments that were undertaken. The research chose to replace the present authentication mechanism with the Ishihara Test chart, which uses six-digit numbers. The Ishihara Test chart is used for authentication during online transaction operations.

The investigation began with the precision of viewing angle and screen brightness. The complimentary colours used in experiment activities demonstrate the efficiency of the viewing angle. Following that, the experiment was conducted with low-backlit LCD or LED screens to prevent a shoulder-surfer assault. For multiscale and parallel views, the manipulation approaches use an adaptive illumination estimator to separate the picture intensity into an illumination layer and a reflectance layer. To balance out the illumination layer while also improving the reflectance layer, the suggested approach makes use of the available backlight level and our determined image-backlight relationship.

The protective system's purpose is to limit shoulder surfer legibility to a critical level while keeping as much of the user's experience as possible [3,4]. The actual user and the shoulder surfer both see the identical content on the screen, but they differ in two key factors that allow the goal to be achieved: viewing angle and viewing distance.

3.1 Legibility Environment Factors Experiment Setup

There are two major types of elements that impact legibility: the environment factor and the display factor [12]. Ambient brightness, viewing angle, and distance are examples of environmental factors that directly affect how legible something seems to the user. Among them, the size of the visual picture of an item that forms in the viewer's eye is influenced by the viewing distance. The user's eyesight has a direct correlation with ambient brightness. Furthermore, geometrical optics states that the brightness that is seen by the viewer's eyes is determined by the viewing angle and distance. Not to mention, screen brightness, color scheme, and resolution are crucial display factors

that impact legibility [9]. The concept of this study is categorized using the impact factor for legibility, which explains in Eq. (1),

$$\sum \tau o \ell \mathcal{F} = \left(\sum \alpha \ell + \gamma + \vartheta\right) + \left(\sum \mathcal{r} + \delta + \beta\right) \tag{1}$$

where environment factor and display factor consist of (ambience luminance + viewing angle + distance) + (resolution + colour scheme + screen brightness). The legibility environment factor consists of ambience luminance describes by,

$$\alpha \ell = 5\left(\mathcal{L}_b^{0.86}\right) \tag{2}$$

where, $\alpha \ell$ = target screen brightness and $\mathcal{L}_b$ = ambient luminance. The viewing angle γ describes by,

$$\gamma = \gamma\left(\tan\theta = \frac{\sin\theta}{\cos\theta}\right) \tag{3}$$

where, $\tan\theta$ refers to,

$$\tan\theta = \frac{1^\circ}{60} \tag{4}$$

The viewing distance ϑ describes by,

$$\vartheta = \frac{\rho_{\mathfrak{r}} \times \mathfrak{j}_{\mathfrak{r}}}{\rho_{\mathfrak{d}}} \tag{5}$$

where $\rho_{\mathfrak{r}}$ is a reference pixel binocular, $\mathfrak{j}_{\mathfrak{r}}$ is image (meter) and $\rho_{\mathfrak{d}}$ is a real-time binocular pixel distance. The legibility environment factor consists of resolution describes,

$$d\text{^}2 = w\text{^}2 + h\text{^}2 \tag{6}$$

where the *d* is diagonal size includes *w* width and *h* height. Next, the colour scheme, which consist of image quality, describes by,

$$\delta = \left|\mathcal{L}_{\mathfrak{f}} - \mathcal{L}_{\mathfrak{b}}\right| \tag{7}$$

where, δ is default quality, $\mathcal{L}_{\mathfrak{f}}$ for luminance of foreground and $\mathcal{L}_{\mathfrak{b}}$is luminance background respectively. The optimal screen brightness $\mathcal{B}$ at the actual viewing distance ϑ represents by,

$$\mathcal{B} = \mathcal{L}_{\mathfrak{b}} + \left(\frac{\nu\vartheta}{\vartheta}\right)^2 \times \left(5 \times \left(\mathcal{L}_b^{0.86} - \mathcal{L}_b\right)\right) \tag{8}$$

where, $\upsilon\vartheta$ refers to the maximum viewing distance will be reaches. There is some data connected to the study that is interrelated.

3.2 Experiment Result

The experiment starts with the setting up for shoulder surfer's view angle and actual user's view angle. Figure 3 shows the illustration for the configuring.

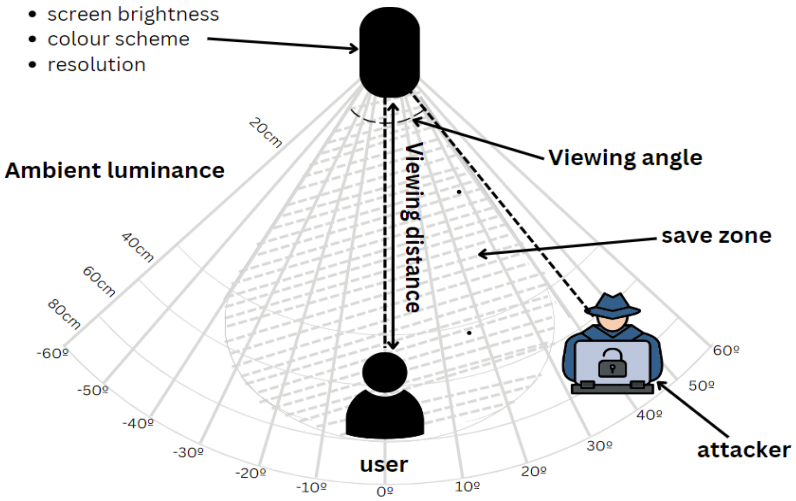

Fig. 3. Configuring for the view angle of the shoulder surfer and the actual user

The experiment setup illustration is shown in Figure 3. A smartphone with a wide viewing angle and programmable brightness settings was used for the experiment. After that, the smartphone is configured to have a modest brightness level, and a photometer is used to measure the brightness. Subsequently, the smartphone is positioned in a brightly lighted space, with its back to the table or other surface where the user intends to use it. An experiment participant group, in which half were "attackers" and the other half were "users". The instructions for the users are to set their phones on tables or other surfaces and use them for a certain amount of time, while the attackers are to stand behind the users and try to see what is on their screens.

An application called the *iSmart* simulator application has been built, and early tests have been conducted, to assess the relevance of parameters. The amount of time that passes between the start of a word and choosing the appropriate response has been noted throughout trials. The variable-controlling approach has been used to examine the impact of variables under control without altering the environment for legibility [1].

Figure 4 illustrates the trend of contrast impact on human eyesight. From this, it was discovered that users' experiences with readability were better when the contrast value was ϒ, improving legibility by 80%; however, when the contrast value was χ, the improvements were only 50%, severely reducing legibility. Normally, users would find it difficult to observe, but from the perspective of the shoulder surfer, this is a helpful warning to prevent them from seeing the real user's login activity. The concept of this pilot testing will be applied to the experiment by real users and shoulder surfers as contributions to the research project.

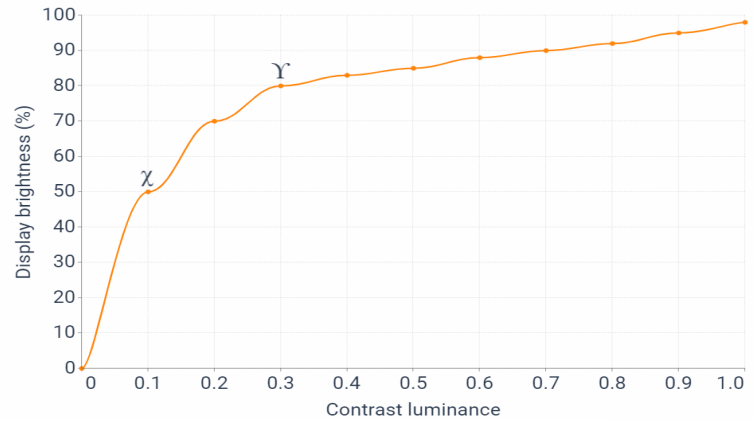

Fig. 4. Display brightness to contrast luminance

A few effects of resolution on viewing angle are shown in Figure 5. While the attacker was given a variable viewing angle by beginning at 10°, 20°, 30°, 40°, 50°, and 60°, users were using i-Smart applications at 0° position. The viewing distance beginning will be changed to 20 cm, 30 cm, 40 cm, 50 cm, 60 cm, and 70 cm in order to test the attacker.

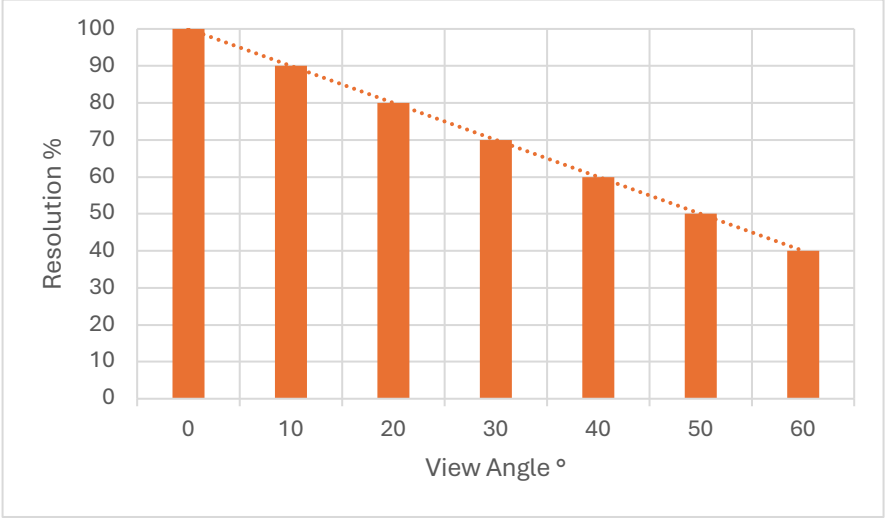

Fig. 5. Pilot testing result for the environment factor's ambient luminance

Table 2 then displays the test's initial view angle, which was 0º. Three more varieties of view angles were used in this experiment. The user was requested to grasp their smartphone from various viewing angles. While standing at the same distance, another volunteer shoulder surfer had a different point of view. At the beginning of the trial, some content was shown, and shoulder-surfers were asked to read it before the real users. Both the exam and its outcomes were documented.

Table 2
Setup for environment's experiment

View Angle (º)	Distance (cm)	Ambient Brightness
0	20	100
10	30	150
20	40	200
30	50	250
40	60	300
50	70	350
60	80	400

An experiment on viewing angle by authorized users and shoulder-surfers was analyzed by the suggested algorithm. Furthermore, the research examined how well-suited the current models were for two other types of constraints: display factor and environment factor. While the display factor was assessed based on smartphone resolution, the environment factor was assessed based on view angle. The findings are displayed in the subsequent figures found in Figure 6. Figure 6 shows the optimum brightness at the current distance. The simulation generated the brightness value based on ambient brightness based on the algorithm 1 and calculated maximum viewing distance.

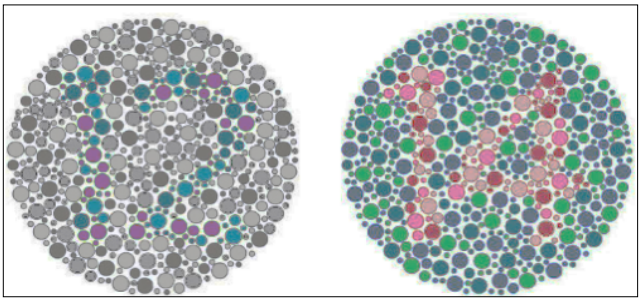

Fig. 6. Optimum brightness resolution

The effect of low ambient brightness on shoulder surfers' resolution vision during authentication operations is depicted in Figure 7. Nearly 90% of the resolution is attained at a direct view angle. This implies that shoulder surfers right behind the user may still make out information pretty well in low light. The resolution drastically decreases to less than 20% when the view angle extends to 60°. This suggests that while viewing from a broader angle, the darkness greatly impairs shoulder surfers' ability to see the information on the screen clearly. When the prospective observer is not immediately behind the user, authentication processes may be safer against shoulder surfing, as seen by the sharp drop in resolution that occurs with increased view angle in dark ambient brightness.

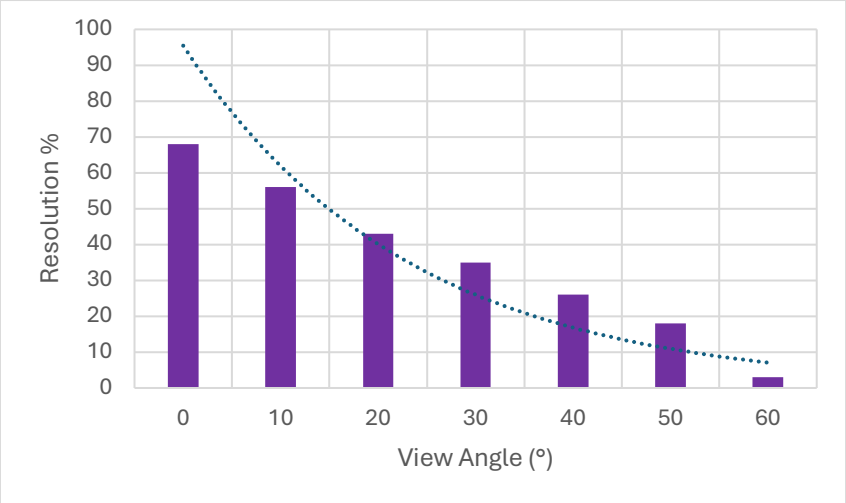

Fig. 7. Findings from experimental result for dark ambient luminance of environment factor

The investigation draws a conclusion on the design of safe authentication settings, highlighting the significance of managing ambient illumination and possible observers' posture. In order to improve privacy and lower the possibility of information leaking during authentication procedures, several elements must be taken into account. This implies the possibility of creating a private area, i.e., when real users are in a secure setting, readability is satisfactory, and the resolution value

exceeds the necessary minimum of 50%. When the shoulder-surfer is outside of the safety zone, their legibility will be severely impaired, and they might not even be able to read at all. It should also be emphasized that this security zone is a temporary installation. As long as the user's furthest viewing distance is 50 cm, a safe zone is created.

4. Conclusions

Shoulder surfer is one of the causes vulnerable to the authentication. Most vulnerable of shoulder surfer attack to the physical transaction activities at automated teller machine (ATM). This paper investigates factors that affect legibility that can be divided into two categories: environmental factors and display factors. This research focusing to the legibility environment factor from shoulder-surfer's viewing angle. The research brings along the algorithm of authentication procedure, enables auto hide or auto glare which shoulder-surfer cannot be seen. The auto glare/auto hide setting gives the most impact to the legibility from shoulder surfer's view. The outcome satisfies the objective and is in accordance with the legibility impact factor. Based on the results, the research concludes that the strategy successfully reduces shoulder surfers' legibility outside of the safe zone to a crucial level.

Acknowledgement
The author would like to thank the Center for Diploma Studies and the Faculty of Information Technology and Computer Science for all the commitment they gave in terms of time and efficient management to the author during her PhD studies and the completion of this paper.

Conflict of Interest
Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution
The authors confirm contribution to the paper as follows: **study conception and design:** Mohd Farhan Md Fudzee; **data collection:** Juliana Mohamed; **analysis and interpretation of results:** Muhamad Hanif Jofri; **draft manuscript preparation:** Juliana Mohamed and Muhamad Hanif Jofri. All authors reviewed the results and approved the final version of the manuscript.

References
[1] Bâce, Mihai, Alia Saad, Mohamed Khamis, Stefan Schneegass, and Andreas Bulling. "PrivacyScout: Assessing vulnerability to shoulder surfing on mobile devices." *Proceedings on Privacy Enhancing Technologies* (2022). https://doi.org/10.56553/popets-2022-0090

[2] Bošnjak, Leon, and Boštjan Brumen. "Shoulder surfing experiments: A systematic literature review." *Computers & Security* 99 (2020): 102023. https://doi.org/10.1016/j.cose.2020.102023

[3] Briones-Villafuerte, Gabriela, Alberto Naula-Bone, Mónica Vaca-Cardenas, and Leticia Vaca-Cardenas. "User Interfaces Promoting Appropriate HCI: Systematic Literature Review." *Revista Ibérica de Sistemas e Tecnologias de Informação* E47 (2022): 61-76.

[4] Distler, Verena. "The Experience of Security in Human-Computer Interactions: Understanding Security Perceptions Through the Concept of User Experience." (2021).

[5] Giaccardi, E., and J. Redström. "Technology and more-than-human design. *Des Issues* 36 (4): 33–44." (2020). https://doi.org/10.1162/desi_a_00612

[6] Karim, Nader Abdel, Zarina Shukur, and AbedElkarim M. AL-banna. "UIPA: User authentication method based on user interface preferences for account recovery process." *Journal of Information Security and Applications* 52 (2020): 102466. https://doi.org/10.1016/j.jisa.2020.102466

[7] Kiljan, Sven, Harald Vranken, and Marko van Eekelen. "Evaluation of transaction authentication methods for online banking." *Future Generation Computer Systems* 80 (2018): 430-447. https://doi.org/10.1016/j.future.2016.05.024

[8] Kovalan, Krishnapriyaa, Siti Zobidah Omar, Lian Tang, Jusang Bolong, Rusli Abdullah, Akmar Hayati Ahmad Ghazali, and Muhammad Adnan Pitchan. "A systematic literature review of the types of authentication safety practices among internet users." *International Journal of Advanced Computer Science and Applications* 12, no. 7 (2021). https://doi.org/10.14569/IJACSA.2021.0120792

[9] Lu, Yongsheng, Hui Li, Nan Chen, and Yujie Shi. "Improving smartphone reading experience for middle-aged and elderly users: the effect of font size, line spacing and stroke weight." In *International Conference on Human-Computer Interaction*, pp. 353-375. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-06050-2_26

[10] Mare, Shrirang, Mary Baker, and Jeremy Gummeson. "A study of authentication in daily life." In *Twelfth symposium on usable privacy and security* (SOUPS 2016), pp. 189-206. 2016.

[11] Markert, Philipp, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. "On the security of smartphone unlock pins." *ACM Transactions on Privacy and Security (TOPS)* 24, no. 4 (2021): 1-36. https://doi.org/10.1145/3473040

[12] Rahman, Md Abdur, and Jaehee You. "Human visual sensitivity based optimal local backlight dimming methodologies under different viewing conditions." *Displays* 76 (2023): 102338. https://doi.org/10.1016/j.displa.2022.102338

[13] Roy, Indrani, Ajmerry Hossain, and Sarker T. Ahmed Rumee. "Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations." *International Journal of Information Technology and Applied Sciences (IJITAS)* 3, no. 4 (2021): 180-183. https://doi.org/10.52502/ijitas.v3i4.201

[14] Suru, H. Umar, and Pietro Murano. "Security and user interface usability of graphical authentication systems–A review." *International Journal of Engineering Trends and Technology (IJERT)* 67 (2019): 17-36. https://doi.org/10.14445/22312803/IJCTT-V67I2P104

[15] The Association Bank of Malaysia, (2024, January 24) More than RM350 million in fraudulent transactions blocked during the first ten months of 2023

[16] The Stars (2024, January 17) Actress shocked to discover RM29,000 missing from bank account.

[17] Tirfe, Dereje, and Vivek Kumar Anand. "A survey on trends of two-factor authentication." In Contemporary Issues in Communication, Cloud and Big Data Analytics: *Proceedings of CCB* 2020, pp. 285-296. Springer Singapore, 2022. https://doi.org/10.1007/978-981-16-4244-9_23

[18] Valarmathi, K., S. Hemalatha, P. Perumal, D. Puthilibai, and M. Abirami. "Shoulder surfing attack trusted verification–a survey." *ECS Transactions* 107, no. 1 (2022): 16041. https://doi.org/10.1149/10701.16041ecst

[19] Zaidi, Ahmad Zairi, Chun Yong Chong, Zhe Jin, Rajendran Parthiban, and Ali Safaa Sadiq. "Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities." *Journal of Network and Computer Applications* 191 (2021): 103162. https://doi.org/10.1016/j.jnca.2021.103162

[20] Zewdie, Temechu G. "Usable Security Case of Remote Web Access." In *HCI International 2020–Late Breaking Posters: 22nd International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part I 22*, pp. 491-501. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-60700-5_62

[21] Zhang, Songheng, Dong Ma, and Yong Wang. "Don't Peek at My Chart: Privacy-preserving Visualization for Mobile Devices." In *Computer Graphics Forum*, vol. 42, no. 3, pp. 137-148. 2023. https://doi.org/10.1111/cgf.14818

[22] Zolkepli, F. (2024, March 4). RM3.8bil taken abroad since 2021.