Usable Authentication Methods for Seniors

Jaspreet Singh, Yvonne Hwei-Syn Kam

Abstract*: Standard authentication methods require user to remember long texts or random numbers when authenticating. The elderly face problems of remembering these passwords maybe due to cognitive decline or simply because they are unfamiliar with current technological devices. This paper compares available authentication methods that are more usable for the elderly and summarises the effectiveness of these systems.

Keywords—authentication, passwords, usable authentication, elderly, seniors

I. INTRODUCTION AND BACKGROUND

The number of people aged 65 and above in 2017 is a total of 7.769% of the total population [1]. The proportion of this age group (also known as senior citizens) is expected to increase in years to come.

Online authentication is part of the online experience whether it may be for social networking, e-commerce or utilizing electronic mail services. Textual passwords are the universally accepted means of online authentication. As services, healthcare and products become more online based, the elderly are expected be familiar with online authentication. Based on statistics from the Norwegian Centre of Information Security, a person has a minimum of 17 passwords for personal use and an average of 8.5 passwords for work [2].Even for the technology adept Generation Z, remembering all 17 passwords is a challenge. As for the senior citizens who are not used to technology, it proves to be a monumental task. The design of modern day authentication systems does not take the problems of senior citizens into consideration. In a paper titled "Designing Authentication with seniors in mind" by Renaud et al. [3], the problems that seniors face when using authentication systems is vividly imagined with 3 fictional characters. The problems they face are for example, trouble typing in passwords, due to arthritis, early stage dementia, failing vision and etc. Renaud et al. also mentioned that a big part of why senior citizens have trouble with authentication systems is because they did not use computers during their working lives, thus they have no mental model to match the interfaces when they have to use the latest technology.

As people age normally, they experience a decline in cognitive abilities. Mental functions such as verbal ability, some numerical abilities and general knowledge are least affected by the ageing process. Whereas, aspects of the brain including memory, processing speed, executive functions and reasoning will have gradually decreasing capabilities from middle age onwards.[4], [5]. This would make the technology inept senior citizens have a harder time remembering passwords for their internet accounts. The method in which information is stored can be best explained by the Atkinson & Shiffrin [6] memory model. In the model, memory is described as a passing of information through 3 checkpoints which are the sensory organ, short term memory (STM) and long term memory (LTM). A stimuli is detected by the sensory organ and passed into the STM where it is stored for a limited time. If not rehearsed repetitively this information will be discarded. Linking the information with something meaningful may allow better encoding so that information can be stored effectively in (LTM) (Fig. 1).

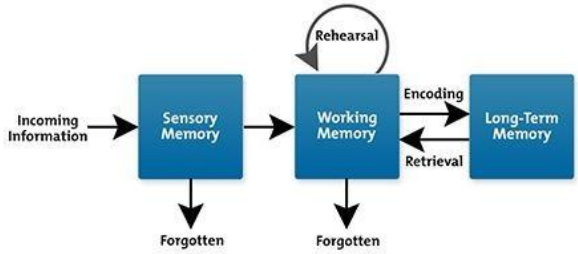

Figure 1: Cognitive Memory model [6]

In a study done by Vu and Hill [7], they find that older adults are more susceptible to forgetting their textual passwords. Biometric authentication is not a viable solution to this problem as shown by the study done by Khan et al. [8]. In the study, young (average age is 22 (range is 18–29) and older adults (average age is 67 (range is 50–84) were given 4 types of authentication ie. PIN, pattern, cued-click points(CCP) and biometric. Results were broken down into configuration time, authentication time and authentication errors where time is a measured variable. Biometric authentication recorded the highest configuration time, highest authentication time and the most number of errors for older adults. Table I displays the results.

The motive behind developing a graphical password is to provide a solution towards the usability problems of textual passwords. Both textual and graphical password systems rely on knowledge based authentication mechanism where the user provides a shared secret that only he and the system knows. But instead of using alphanumeric characters, graphical passwords use media such as images that stimulate the memory. Graphical passwords work on the theory that human memory works better when remembering images compared to remembering strings of characters. Tullis, Tedesco and McCaffrey [10] have shown that humans are able to remember their target images through a 6 year separation. Gehring et al. [11] discovered that visual information was remarkably easier to recall in short and long term memory. This would help ease the memory load of older adults when trying to remember their passwords.

Revised Manuscript Received on August 18, 2019

Jaspreet Singh, Graduate, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.
Yvonne Hwei-Syn Kam, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.

Table 1 : The average configuration and authentication times in seconds [8]

	Young	Older
Conf. time		
PIN	16	30
Pattern	19	42
Fingerprint	52	65
CCP	46	81
Auth. Time		
PIN	3.7	7.7
Pattern	3	4.5
Fingerprint	18.7	38
CCP	5.7	8.5
Auth. Err		
PIN	0.3	0.47
Pattern	1.3	0.53
Fingerprint	4	7.2
CCP	0.3	0.5

II. SURVEY ON AUTHENTICATION SYSTEMS

Often there is question on the effectiveness of graphical authentication systems and whether it is really necessary when traditional authentication systems such as PINs and passwords are working fine. This view does not take into account the problems faced by senior citizens who struggle with memory as they age. A graphical authentication system intends to fix the areas that are not considered by the design of traditional authentication systems. Traditional authentication methods require user to select passwords that may include uppercase letters and special characters which are hard to remember. On top of that, web browsers nowadays provide an autofill functionality that keeps passwords so we do not have to remember them. Memories that are not rehearsed will be forgotten. Graphical authentication aims to alleviate the problem of memorability. This is most helpful for the people who will be most affected by this problem, the elderly. In this section we briefly survey traditional authentication systems (Part A) and then some available graphical authentication systems that are in general more usable for seniors (Part B) and make a comparison of them (Table III) to find some common areas on what makes a graphical authentication system usable for seniors.

A. Traditional Authentication Systems

Personal Identification Number

Personal Identification numbers (PIN) is a commonly used method for authentication. PINs involve only numeric characters and are usually limited to 4 or 6 password spaces. From a security point of view, PINs are less vulnerable to shoulder surfing compared to graphical authentication systems because they can be hidden on screen (with asterisks, for example). When compared to pattern, fingerprint and CCP authentication the configuration time for a PIN password is found to be the fastest, while coming in a close second to Pattern Lock for login time [8]. Speed and security are the main reasons why PIN and textual passwords have become universally accepted. However according to Khan et al. [8], usability ratings by senior citizens show that unlike their young counterparts they do not rate speed very highly, instead they prefer an authentication method that is easy to remember.

Textual Password

Compared to PINs which are restricted to digits, textual passwords can contain alphanumeric and special symbols. Text passwords therefore have a larger password space, making it more resistant to brute force attacks. The only security liability that arises when a text password is used is from the user himself. Users tend to either use common words as their password which risks a dictionary attack or use personal information which risks a social engineering attack. Nevertheless, the textual password is still preferred by many. An authentication preference study to evaluate the type of preferred authentication system by patients to access their PHR (Patient Health Records) found that most of the test subjects preferred text passwords compared to pattern and voice recognition [12]. It should be noted however, that the same study found that when patients were asked as to why they preferred text passwords over the other two, the common response was that they could save the password on the login page which saved the test subjects from typing in their password every time they logged in. Nevertheless, this will more likely cause them to forget their password or write them down somewhere.

B. Graphical Authentication Methods Which Are More Suitable For Senior Citizens

Pattern Lock

The Pattern Lock [13] (Fig. 2) authentication allows users to draw recognizable pattern within the limits of a 3×3 grid. It is a widely used authentication on Android lock screens as an alternative to PIN. In an experiment involving older adults, Khan et al. [8] found that Pattern Lock authentication takes the least amount of time during a login process when compared to PIN, fingerprint and CCP. Compared to young adults, significantly fewer older adults felt that Pattern lock (and also PIN) was time consuming but significantly more felt that Pattern lock (and also PIN) was tiring. The most liked option after PIN was Pattern lock which was a very close second. One of the main reasons was that Pattern lock was easy to remember. A few unique dislikes were reported by a few older adults: dexterity was required for Pattern Lock and Pattern Lock and CCP were difficult to note down for safe keeping unlike their other passwords.

Unlike other graphical authentication, Pattern Lock requires the user to have physical contact on the screen to create a pattern. This leaves an oily residue or smudges on the screen and can be considered as an information leakage. Aviv et al. [14] reported that it is possible for an attacker to use smudges on a screen to gain access to a device.

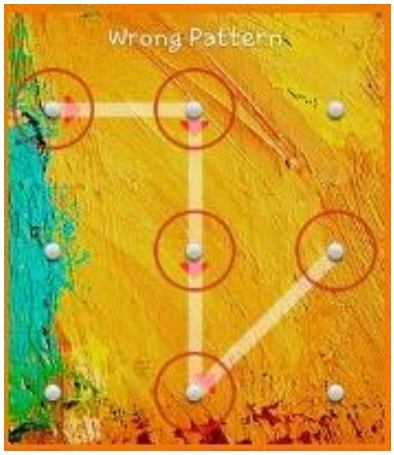

Figure 2: Android Pattern Lock [13]

Doodles/Handwriting

Doodles or handwriting authentication systems are recall based. The first such system is the Draw-a-secret (DAS) (Fig. 3) scheme developed by Ian Jermyn et al. [15]. DAS allowed users to draw a simple picture on a grid consisting of one pen stroke or several pen strokes depending on user preference. To log in, user has to redraw the same picture in the given grid either with the use of a pen or a stylus. The reason for using doodles as an authentication method is because it is a form of handwriting. When an alphabet is written, it is done so without any conscious thought of how it is formed [16]. Longcamp et al. [17] argues that there is a specific part of the brain that controls the processes of writing letters and numerals allowing us not only to recognize our own handwriting but reproduce it.

Sreeramareddy et al. [18] reported from their study that the mouse gesture-based password method could prove to be a viable authentication solution for seniors as they could reenter their passwords with higher accuracy than the young people. Familiarity of gestures also plays a part in accuracy with familiar gestures being performed more accurately by seniors [19].

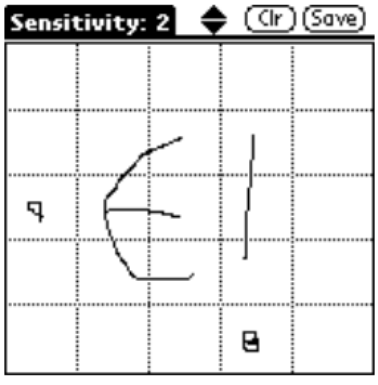

Figure 3: Draw-a-secret [15]

HandWing [20], is a recognition based authentication system, in which the images used are doodles. The password images are doodles which were drawn by the user prior. The authors reported that it increased memorability and usability. However, the authors acknowledged that it was weaker than traditional passwords and had a proportion of authentication errors.

Face-Based Authentication System

A face based authentication system is an authentication system that uses faces as a unique verification system. An example of a face based authentication system is Passfaces [21]. During registration, Passfaces provides the user with 3 random faces and the user is asked to remember the faces. Whenever the user tries to login, he will be provided with the face that he was asked to memorize along with other randomized faces. By selecting the pictures belonging to his password, the user will successfully login. Passfaces uses the fact that human are able to remember the faces of people better than text. According to Valentine [22],[23], the short term memory and long term memory for Passfaces were better than when using traditional passwords.

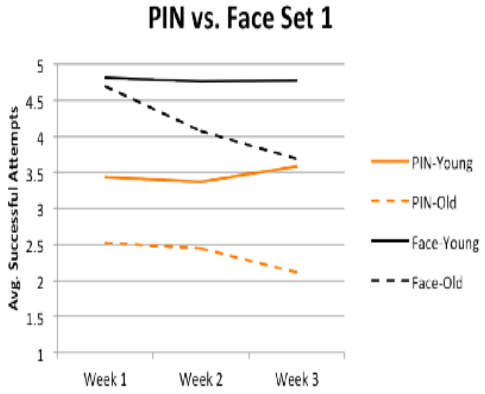

Figure 4: Accuracy of younger and older participants with PIN and Faces [24]

It is suggested that Face based authentication is used rather than textual passwords for senior citizens because it will be easier for them to remember. Nicholson et al. [24] conducted an experiment to measure the performance of young adults and older adults in memorizing textual passwords and face based passwords. The experiment was broken down into 2 sets which are SET1 (shown in Fig. 4) and SET2 (shown in Fig. 5). SET1 had a frequency of testing of once per week for 3 weeks whereas SET2 had a frequency of testing of once per week for 2 weeks, ie. skipping the first week. The results can be seen in the Figs. 4 and 5. It is clear that older adults benefited massively from face based authentication where they performed with higher accuracy than with PIN.

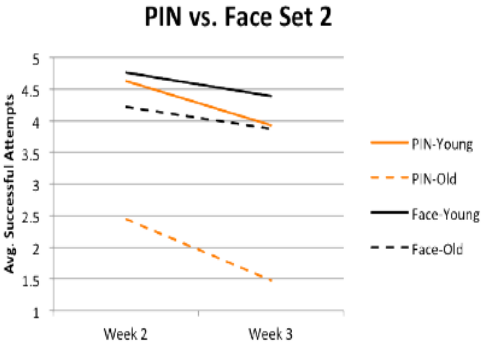

Figure 5: Accuracy of younger and older particicpants with PIN and faces SET2 [24]

Music-Based Authentication System

Musipass is a music based authentication system developed by Renaud et. al [25] which uses music to authenticate users. During enrollment (shown in Fig. 6), the system shows users a number of musical icons on the screen. User will have to move the mouse cursor over the icon to hear the music playing. The user chooses the music he or she prefers as their password and moves on to the next stage. There are four stages, each displaying 9 different sound clips. After enrollment is the training stage (shown in Fig. 7), where users are given a chance to listen to the password clips again and are asked to enter some text describing it. This stage allows users to listen to the sound clips again and become accustomed to them, thus reinforcing memory.

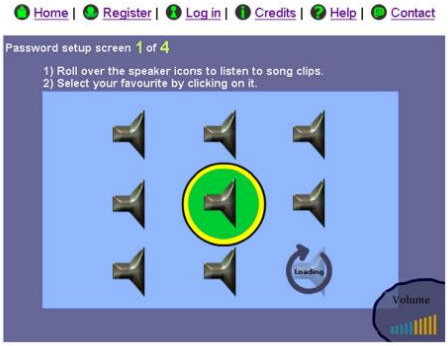

Figure 6: Enrollment with Musipass [25]

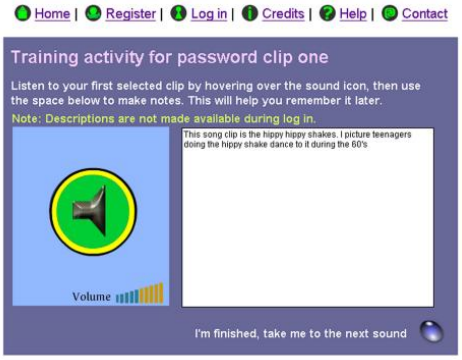

Figure 7: Training with Musipass [25]

Following the completion of enrollment and training, users can authenticate themselves using this system. For authentication, users input their email address and are taken through the four stages. The concept of a music based authentication is based on the fact that music is a part of our everyday lives and we love it [26]. It was also suggested by Peretz et al. [27] that humans are hardwired to process stimuli in the form of music.

Renaud et al. [25] did a comparison study to evaluate Musipass against traditional textual passwords. The factors that were manipulated in the study include age and musical experience. The study concluded that participants irrespective of age, found that recalling the Musipass password was tremendously easier compared to traditional passwords. It was also found that those with musical experience tended to be better at remembering their Musipass passwords than those without. Table II shows the results from the study. Musipass success percentage is observed to be clearly better than the traditional textual password. It can also be observed that the success percentage is high across all age groups tested.

Table 2 : Musipass Authentication Results [24]

Musical experience	Age	No. Participants	Musipass success %	Traditional success %
None	Under 25	1	100	0
	25-35	0	0	0
	36-45	1	0	100
	46-55	2	100	100
Listen frequently	Under 25	3	100	66.67
	25-35	8	87.5	37.5
	36-45	3	100	0
	46-55	3	100	66.67
Play instrument	Under 25	4	100	50
	25-35	6	100	66.67
	36-45	4	75	25
	46-55	1	100	100
Professional Musician	Under 25	4	100	75
	25-35	3	100	100
	36-45	3	100	50
	46-55	2	100	100

Cued Recognition

Cued Recognition or CuedR by Al-Ameen et al. [28] aims at making system-assigned passwords more memorable through multiple cues. Al-Ameen et. al argues that coming up with a password should not be the responsibility of the user due to security concerns, instead it should be the burden of the system. CuedR will help the user memorize the system assigned password. CuedR works by assigning 6 random keywords to the user. Each keyword would be from a different portfolio such as countries or animals. An example of a keyword is “Cheetah”. Each keyword would have an image, number and phrase related to it. Fig. 8 illustrates the components of a keyword.

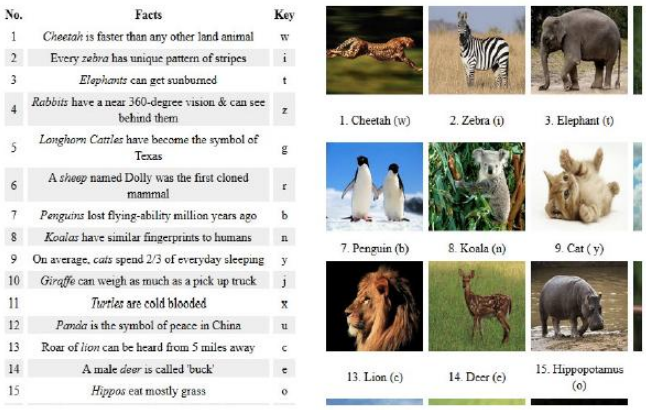

Figure 8: Login Screen of CuedR recognition system[28]

Whenever the user attempts to login, he will be provided with a login screen as shown in Fig. 8. Each of the keywords is assigned a key, this key will be different every time to provide a variant response property [9]. The user has to select one of the keywords that he has previously selected

during registration. After selecting a keyword by inputting the key, he will be redirected to the next screen where the same procedure occurs for each of the memorized keywords. An experiment was done by Al-Ameen et al. to evaluate the success rate of CuedR. The experiment was done in 2 sessions where the second session is held a week after the first to test participant's memory of their password. Participants comprised of young university educated students. Results from the experiment for both login sessions showed CuedR having a 100% success rate. Fig. 9 shows the results of participants' personal opinion on which cue helped them the most. It can be seen that the participants felt that image cues were the most helpful.

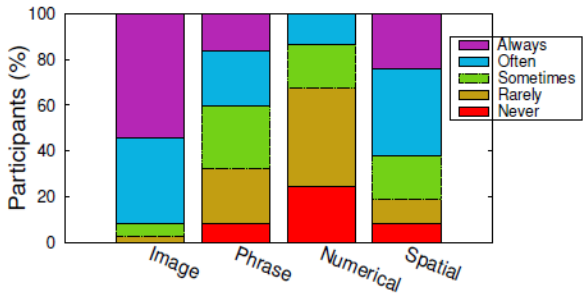

Figure 9: Participants' feedback on most helpful cues [28]

III. SUMMARY OF AUTHENTICATION METHODS

Table III displays a table comparing the advantages and drawbacks of the systems discussed. Studies done [8], [24], [25] show that graphical authentication systems do help the elderly. From a usability point of view, the elderly are more open and acceptable to using graphical authentication systems compared to young adults who find them annoying and time consuming [8], [12], [20].

Faces stood out as being highly memorable to the elderly. Recall based methods such as Pattern Lock were able to be performed with speed and accuracy by seniors but some felt that Pattern Lock was tiring. Recognition of own doodle images was also deemed acceptable by the seniors though it had a proportion of authentication errors. Music was highly memorable across different age groups. Thus it can be concluded that graphical authentication systems aimed towards seniors could incorporate any or some of these elements.

The focus of design when creating a graphical authentication is not only security but also usability. If it does not make authentication easy enough for the user then it will not be effective. However, there will be a trade-off in terms of security as graphical authentications are vulnerable to attacks such as shoulder surfing. Thus there is a need to balance between security and usability especially for older users as not all sites and transactions have the need of such

Table 3 : Comparing Authentication Systems

Authentication System Type	Devices/Softwares Implemented	Advantages	Drawbacks
Pattern Lock	•Android Screen Unlock [13]	•Patterns are easier to remember compared to PINs •Login process is fast	•Susceptible to "smudge attacks" •Only practical on touch screen phones •Tiring for seniors
PIN and Textual Passwords	•Implemented in most electronic devices	•Comparatively resistant to shoulder surfing attacks •Universally accepted •Login process is fast	•Difficult to remember •Tiring for seniors
Faces	•Passfaces [21]	•Ease of recognition by users, especially older adults •Recognition ability reduces when face portrayed is different from user in terms of age, ethnicity, gender	•Susceptible to shoulder surfing •Login process is time consuming
General Images	•GPI (Graphical Password with Icon) •Photographic Authentication System	•Ease of recognition by users	•Susceptible to shoulder surfing •Login process is time consuming
Images of user's own handwriting	HandWing [20]	•Ease of recognition by users	•Susceptible to shoulder surfing •Login process is time consuming •Higher error rate
Doodles/Handwriting	•DAS (Draw-a-secret) [15]	•Able to personalize password •Seniors can have relatively high accuracy	•Susceptible to shoulder surfing •Login process is time Consuming •Susceptible to shoulder surfing
Music	•Musipass [25]	•Humans are wired to process music. Can be recognized easily	•Require headphones during authentication to avoid shoulder surfing •Login process is time consuming
Graphical Authentication with Cues	•CuedR [28]	•Multiple cues to stimulate the users memory •High login success rate	•Susceptible to shoulder surfing •Login process is time consuming

high security. As Renaud et al. [20] noted "Developers should consider using purpose-tailored identification and authentication mechanisms, both in terms of site content and target user group."

IV. FUTURE RECOMMENDATIONS

The current graphical systems that are available are effective to a certain extent, but they can be better. One of the ways that graphical authentication systems can be improved is by implementing a hybrid graphical authentication system. This would involve making a system rely on not one but two types of media to help users recall their password. The types of media can be music and images or music and faces. That multiple cues help recall have been shown by Al-Ameen et al. [28] In particular, image media should be included. Music has also been shown to be a vastly memorable media (Renaud et al. [25]). Thus a combination would probably render the system even more memorable for the elderly. Another area of the graphical authentication system that can be improved is security. For graphical authentication systems involving music, a detection software can be added to the system to remind the user to put on headphones before starting authentication. Whereas for authentication with images, the image selected by the user can be concealed by requiring user to select the target image via keyboard [28]. Once user selects the target image, there should be no indication on the screen regarding which image is selected by the user. Instead the system moves on to the next portfolio of images. This would effectively prevent any attacker from shoulder surfing, even if the login screen is being watched.

V. CONCLUSION

In this paper we presented the problems faced by senior citizens when using standard authentication methods. We also compared the available methods for authentication and the differences between authentication systems' usability for seniors.

ACKNOWLEDGMENT

Financial support from the Ministry of Higher Education, Malaysia, under the Fundamental Research Grant Scheme with grant number FRGS/1/2015/SG07/MMU/02/1 is gratefully acknowledged.

REFERENCES

1. "The World Bank," The World Bank Group, [Online]. Available: https://data.worldbank.org/indicator/SP.POP.65UP.MA.ZS. [Accessed 22 August 2018].
2. Norsis,2012"Passordvett".[Online].Available: passwords12.at.ifi.uio.no/NorSIS/NorSIS_Passwords12.pdf.
3. K. Renaud, K. S. Brown and A. Szymkowiak, "Designing Authentication With Seniors In Mind," Abertay University, Dundee, UK, 2018.
4. T. Hedden and J. Gabrieli, "Insights into the ageing mind: a view from cognitive neuroscience," Nat Rev Neurosci 5, pp. 87-96, 2004.
5. P. DC and R. -L. P, "The adaptive brain: aging and neurocognitive scaffolding," Annu Rev Psychol, no. 60, pp. 173-196, 2009.
6. C. Atkinson and M. Shiffrin, "Human Memory: A proposed system and its control processes. IN K.W. Spence & J.T. Spence(eds), Advances in the psychology of learning and motivation," in New York academic press, New York, 1968.
7. K.-P. L. Vu and M. M. Hills, "The influence of password restrictions and mnemonics on the memory for passwords of older adults," In Human Interface and the Management of Information. Springer, 2013.
8. H. Khan, K. Grindrod, U. Hengarter and D. Vogel, "Evaluating Smartphone Authentication Schemes with Older Adults," in 12th Symposium on Usable Privacy and Security (SOUPS 2016), Denver CO, 2016.
9. R. Biddle, S. Chiasson and P. & Van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," ACM Computing Surveys, vol. 44, no. 4, 2012.
10. T. Tullis, D. Tedesco and K. & McCaffrey, "Can Users Remember their Pictorial Passwords Six Years Later," in Extended Abstracts on Human Factors in Computing Systems, Vancouver, BC, Canada, 2011.
11. R. Gehring, M. Toglia and &. K. G.A., "Recognition Memory for Words and Pictures at Short and Long Retention Intervals," *Memory & Recognition*, vol. 4, no. 3, pp. 256-260, 1976.
12. A. Fruhling, D. Ramachandran, T. Bernard, R. Schuetzler and J. Windle, "Patient Preference for Authentication and Security: A Comparison Study of Younger and Older Patients," in SIGMIS-CPR'18, Buffalo-Niagara Falls, NY, USA, 2018.
13. "How to reset pattern lock in Samsung Smartphone?," Samsung, 8 June 2018. [Online]. Available: https://www.samsung.com/in/support/mobile-devices/how-to-reset-pattern-lock-in-samsung-smartphones/. [Accessed 25 August 2018].
14. A. J.Aviv, K. Gibson, E. Mossop, M. Blaze and J. M.Smith, "Smudge Attacks on Smartphone Touch Screen," in USENIX 4th Workshop on Offensive Technologies, 2010.
15. I. Jeremyn, A. Mayer, F. Monroe, M.Reiter and A. Rubin, "The design and analysis of graphical passwords," in 8th USENIX Security Symposium, August 1999.
16. W. W. Ph.D, Diagrams Of The Unconscious, New York: Grune & Stratton, 1944.
17. Longcamp, M., Anton, J. L., Roth, M. & Velay, J. L. 2003, Visual Presentation of single letters activates a premotor area involved in writing, Neuroimage 19(4), 1492-500
18. L. Sreeramareddy, P. Mulbah and J.H. Feng, , "Investigating the use of gesture-based passwords by the seniors." In International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer, Cham, 2015, pp. 107-118.
19. C. Stoßel, "Familiarity as a factor in designing finger gestures for elderly users", In Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI '09, ACM (New York, NY, USA), 2009, 78:1–78:2.
20. K. Renaud and J. Ramsay, "Now what was that password again? A more flexible way of identifying and authenticating our seniors." Behaviour & Information Technology 26, no. 4, 2007, pp. 309-322.
21. "Passfaces," Passfaces Corporation, 2005-2018. [Online]. Available: http://www.realuser.com/. [Accessed 11 08 2018].
22. T. Valentine, "An evaluation of the Passface personal authentication system," Goldsmiths College University of London, London, 1998.
23. T. Valentine, "Memory for Passfaces after a long delay," Goldsmiths College University of London, London, 1999.
24. J. Nicholson, L. Coventry and P. Briggs, "Age-Related Performance Issues for PIN and Face-Based Authentication System," April 2013.
25. K. Renaud, M. Gibson, M. Conrad and C. Maple, "Musipass: Authenticating Me Softly with "My" Song," Workshop onNew Security paradigms workshop,ACM, pp. 85-100, 2009.
26. P. J. Rentfrow and S. D. Gosling, "The do re mi's of everyday life: The structure and personality correlates of music preference," Journal of Personality and Social Pschology, vol. 84, no. 6, pp. 1236-1256, 2003.
27. I. Peretz, A. J. Blood, V. Penhune and R. Zatorre, "Cortical deafness to dissonance," Brain, vol. 124, pp. 928-940, 2001.
28. M. N. Al-Ameen, M. Wright and S. Scielzo, "Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues", CHI, 2015.
29. M. E. Manaa and M. K. Al-Rikaby, "Robust Authentication Approach Based on Keyboard Graphical Password," *Journal of Engineering and Applied Sciences*, vol. 12, no. 7, pp. 1738-1745, 2017.

AUTHORS PROFILE

Jaspreet Singh Graduated with a degree in Electronics Engineering majoring in Computer (Hons) from Multimedia University, Malaysia.

Yvonne Kam has a first class Bachelor of Engineering (Hons) Electronics Majoring in Multimedia degree and a Masters in Engineering Science (MEngSc) in the topic of Image processing, from Multimedia University (MMU). She is a researcher and lecturer in the Faculty of Engineering in MMU and is currently pursuing her PhD in Computer Science in University of Malaya on the topic of graphical passwords. As part of her PhD, she has developed and implemented applications for security authentication.