Pure Recall-Based Graphical User Authentication Schemes: Perspectives from a Closer Look

Adama, Victor, Ndako
Department of Computer Science,
School of ICT Federal University of
Technology Minna, Nigeria
vnadama@futminna.edu.ng

Oyefolahan, Ishaq, Oyebisi
Department of Information
Technology, School of ICT Federal
University of Technology Minna,
Nigeria
o.ishaq@futminna.edu.ng

Ndunagu, J, N
Department of Computer Science,
National Open University of Nigeria,
Abuja, Nigeria,
jdunagu@noun.edu.ng

ABSTRACT

In an era of mobile, embedded and ubiquitous computing, activities of hackers and cybercriminals has metamorphosed into a global pandemic. Resulting effects cuts across most sectors of human endeavor given the high penetration level of technology. Successful unauthorized access leading to information and identity theft, system infiltration, intellectual property theft, financial crimes, extortion, carding and much more are on the increase, consequently making user authentication an important process, ensuring systems and services are accessed by their intended users. Text passwords are the most widely deployed user authentication scheme today. However, are hardly human-friendly for the vast majority, leaving humans with a memorability problem and consequently a security problem. Graphical User Authentication (GUA) schemes, on the other hand, are proven by state-of-the-art research with compelling evidence to perform better in memorability and potentially by implication security. However currently available GUA schemes provide theoretical entropy levels far from that offered by text password scheme. Thus the research community constantly is seeking to improve GUAs to position them as possible alternatives to Text passwords. This study is a first of two planned studies. It seeks to take a closer look at Pure Recall-based GUAs with emphasis on a user authentication design factor contextual parameter. The study aims at a better understanding of Pure Recall-based GUAs developed between the first 20 years (1996 to 2016), then others in a later study in an attempt to better position Pure Recall-based GUAs as alternatives to text passwords.

CCS CONCEPTS

• **Graphical User Authentication (GUA)**; • **Pure Recall Scheme**; • **Security**;

KEYWORDS

User Authentication, Graphical, Password, Pure-Recall, Dynamic

ACM Reference Format:
Adama, Victor, Ndako, Oyefolahan, Ishaq, Oyebisi, and Ndunagu, J, N. 2021. Pure Recall-Based Graphical User Authentication Schemes: Perspectives from a Closer Look. In *3rd African Human-Computer Interaction Conference (AfriCHI 2021), March 08–12, 2021, Maputo, Mozambique.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3448696.3448721

1 INTRODUCTION

Authentication is a word derived from the Greek word "αὐθεντικς", meaning real or genuine. Basically, authentication is a process of ensuring the person attempting to gain access to a service or system is who they claim to be [1]. Unauthorized access could in most cases prove fatal, thereby positioning authentication not only as a key factor, but one of the most important security characteristics given today's globalized digital lifestyle [2]. The need to prevent unauthorized users from accessing sensitive information cannot be overemphasised [3].

Graphical User Authentication (GUA) schemes, have proven by state-of-the-art research with compelling evidence to perform better in memorability and potentially by implication security, than the most deployed scheme today, text passwords. However GUAs are yet to match the security level currently offered by text passwords. Attempting to expand the boundaries of graphical user authentication research, this paper seeks to take a closer look at Pure Recall-based GAU schemes developed between the first 20 years (1996 to 2016), and others in a latter study to establish if findings from this study are consistent with other recent schemes beyond this time frame. A closer look will yield a better understanding of Pure Recall-based GUAs and will offer an opportunity to better position such as alternatives to text passwords. The paper is organized as follows. Section 2 gives an overview of categories of GUA schemes and explains what user authentication entails. Section 3 elaborates on the concept of contextual parameters and their importance in user authentication research and design. Section 4 takes a closer look at pure recall based GUA and makes observations. Section 5 concludes this initial study.

2 GRAPHICAL USER AUTHENTICATION

Graphical User Authentication (GUA) schemes have proven via state-of-the-art research to outperform text passwords in terms of memorability and possibly by implication security [2]. Also proven over time by research is that the usability of an authentication scheme is equally as important as the security it offers [2]. This has positioned usability research as a crucial area in security research. This has also motivated research aimed at exploring for more user

AfriCHI 2021, March 08–12, 2021, Maputo, Mozambique
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8869-6/21/03…$15.00
https://doi.org/10.1145/3448696.3448721

authentication paradigms such as Graphical user authentication (GUA) schemes, to create the right balance between security and usability. The most widely deployed authentication scheme today still remains text password [4]. However, strict security policies associated with text passwords ultimately poses a memorability problem to users [5]. GUA schemes leverage on "Picture Superiority effect", positioning GUAs as better fit password in terms of usability. GUA schemes have broadly been classified based on the cognitive tasks employed by users to retrieve login credentials. Monrose and Reiter in 2005 categorized GUA schemes into three main categories: image recognition, tapping or drawing and image [6]. Whereas, Suo, Zhu and Owen in 2006 categorized GUA schemes into two categories: Recognition-based and Recall-based schemes [7]. Wiedenbeck et al., on the other hand in 2005 further expanded the aforementioned categories to include Recognition, Pure-recall, and Cued-recall [8].

2.1 Recognition Based and Recall Based User Authentication

Generally, all authentication scheme consists of two important stages. The first is the registration stage. Users in this stage are required to select and register login credentials, which are then safely stored and used to establish who is granted access in future login sessions. The second stage is the authentication stage. This could involves single or multiple rounds. At each login round, users are required to reproduce login credentials they had earlier provided in the registration stage before gaining access.

Recognition-based GUA schemes basically involve users creating a password from a set of images, icons or symbols in the registration stage [10]. On the other hand, recall-based GUA schemes involves composing a password by drawing an image or pre-selecting click locations on an image in the registration stage, reproducing such at the authentication stage. This paradigm heavily relies on human memory compared to recognition schemes.

Although GUAs significantly addresses the human memorability problem of text passwords, GUAs are yet to match the security level of text passwords. Current available GUA schemes offer theoretical entropy of between 12 and 23 bits which is far from the 39 to 53 bits offered by text passwords [11].

3 CONTEXTUAL AUTHENTICATION PARAMETERS

User authentication research has become a complex endeavour [12]. Research has revealed user authentication entails several contextual parameters that need to be taken into consideration [12]. These parameters fall under 3 categories which are the Human Factor, Technology Factor and User Authentication Design Factor as illustrated in figure 1

From the human perspective, research revealed that individual characteristics, known as Human Factors, affect user authentication tasks and consequently security. Examples of such Human Factors are users' age, gender, culture, cognitive disabilities and cognitive processing abilities [13][14][15][16]. From the technology perspective, studies indicate that some device characteristics, such as, device type, screen size, input device, input style etc. also have significant impact on users' performance and behaviour in user authentication tasks [17][18] [19]. From the design perspective, research has shown that design characteristics also known as User Authentication Design Factors, such as authentication type (textual vs. graphical), pool of characters used in password policies, distribution of user chosen images, image type (e.g., faces vs. single-object images) in recognition-based graphical authentication, image saliency, image grid size during graphical key creation and image distortion affect task completion performance and security [20] [21] [22] [23] [24] [25].

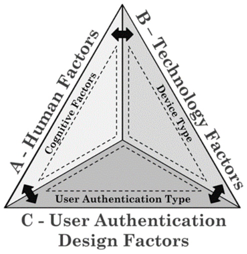

Figure 1: The interplay between human cognitive factors [1]

A research by Katsini et al., in 2018 asked the research question "Does Image Grid Visualization Affect Password Strength and Creation Time in Graphical Authentication?" [10]. Considering the fact that GUAs are considered a better fit for interaction environments which lack a physical keyboard, security vulnerabilities still exist. This motivated the researchers to investigate the effectiveness of advanced visualization layouts (a contextual parameter) in selecting stronger passwords. Via a between-subject study, two-dimensional and a three dimensional visualization where compared. Results revealed that advanced visualization techniques provided a more suitable framework for deploying graphical user authentication schemes. Another research by Katsini et al., in 2017 titled "Influences of Users' Cognitive Strategies on Graphical Password Composition" investigated how different visual behaviours of individuals with varying cognitive strategies affects the security aspects of GUA across device types [12]. Via a user study (N=51) on graphical password composition using a recognition-based GUA scheme, results revealed differences on key strength and complexity, as well as on gaze-based entropies between users with different cognitive strategies. The researchers suggested this information could be used in the design of User Adaptive GUA schemes. A research by Cain et al., in 2017 took steps to directly compare three prototypical graphical password schemes to determine their relative resistance to "Over the shoulder- attacks" employing a within-subjects design [5]. Results revealed schemes requiring cognitive operations in response to target patterns were superior to direct selection of targets. The most secure scheme going by results was "Convex Hull Click", followed by "What You See is What You Enter", while "Use Your Illusion" showed high vulnerability to OSA.

Seeking a better understanding of these contextual parameters cannot be over emphasized. This is simply because such proper understanding would potentially inform improved methodologies for the design of sustainable, secure and usable authentication schemes, hence the need to take a closer look at various GUA categories. This study seeks to specifically focus on Pure Recall-based schemes.

Table 1: Categorization of Pure Recall schemes based on login credential entry approach and Design Styles.

SN	Scheme	Year Developed	Login Approach			Deign Style	
			Draw	Click	Type	Grid	Images
1	Syukri Algorithm	1998	√	-	-	√	-
2	Draw-A-Secret (DAS)	1999	√	-	-	√	-
3	Passdoodle	2004	√	-	-	√	-
4	Multi-Grid DAS (MGDAS)	2006	√	-	-	√	-
5	Qualitative Draw-A-Secret (QDAS)	2007	√	-	-	√	-
6	DAS with Rotation (R-DAS)	2007	√	-	-	√	-
8	Pass-Go	2008	√	-	-	√	-
8	PassShape	2008	√	-	-	-	-
9	Yet another Graphical Password (YAGP)	2008	√	-	-	√	-
10	Zheng (Shape & Text)	2010	Shape		√	√	
11	Android Unlock Pattern	2012	√	-	-		-
12	TMD	2013	√	-	-	√	-

4 RECALL GRAPHICAL USER AUTHENTICATION SCHEEMS, FIRST 20 YEARS

Researchers have not only explored for novel GUA schemes but have also sought to push the boundaries of existing schemes, striving to harness their full potentials with regards to security and usability. However each scheme is characterised by various strengths and weaknesses. This paper attempts to make observations that will ultimately lead to hypothesis subject to verification on how to better position Pure Recall-based GUA schemes in terms of security and usability. This study thus seeks to consider Pure Recall GUA schemes developed from inception1996 to 2016 (the first 20 years), in a later study consider others and synthesize findings.

4.1 Pure Recall-based Graphical User Authentication Schemes

Blonder is widely regarded as the founder of the graphical authentication notion as Blonder scheme was the first GUA introduced to the research community in 1996 [26][27]. Pure recall GUA schemes are considered difficult for users in practice due to their heavy reliance on human memory. Interestingly, A few Pure recall GUA schemes going by published results, offer higher entropy levels compared to text passwords [29][30][27]. For example, an 8 alphanumeric character text password offers an entropy of 53 bits, while a 20 strokes "Yet another Graphical Password" (YAGP) GUA pure recall scheme offers entropy of 232 bit [27]. By implication YAGP offers higher security level in this scenario. Hence the specific interest in pure recall-based GUA schemes. Login credential in GUA schemes can be provided in three categories of actions during the authentication stage. Users could either be required to draw, click or type login credentials [27].

Draw based schemes generally require users to digitally draw an image using a digital pen, touchpad, computer mouse, or finger on touch-enabled devices. This image could be on a blank or gridded background and is then stored as the login credential at pre-set degree of accuracy. Typical draw schemes use grid intersections, coordinates, values of occupied grid cells to encode the drawing information. Table 1 categorize Pure Recall schemes based on login credential entry approach and Design Styles.

Synthesized draw backs associated with draw based pure recall schemes in general are as follows.

1 The difficulty with which login credentials are recalled from memory without cues [28].
2 Difficulty in use associated with input devices for drawing [31] [7].
3 Levels of accuracy with which pre-registered drawings are reproduced [31][32][33].
4 Users' ability of drawing symmetric images with few strokes thereby decreasing password space [33].
5 Possibility of smudge attacks, oily finger marks left on device screens [34].

Click-based schemes typically involves click events on user selected click points. These click events are informed by "something" presented to the user, in most instances an image or a grid. It implies secret points of the image/grid are pre-selected, stored and later have reproduced. The image/grid therefore plays an assistive role thereby easing recall. By implication these schemes are less burdensome on the human memory compared to pure recall schemes and are therefore regarded as cued recall. Thus, help in this context (recall) are referred to as cues. An interesting login credential entry mechanism introduced to GUA schemes is the use of keyboard as to mouse. The use of keyboard is so rare amongst pure recall based schemes, only Zheng (Shape & Text) under the period of consideration was observed to make use of the keyboard. However the use of keyboards stand to offer potential benefits. According to a study by Tari, Ozok and Holden, replacing the mouse with the keyboard in some GUA schemes reduced the risk of shoulder surfing [35]. Given that both screen scraping and keystroke logging will be required, the use of a keyboard makes shoulder surfing more difficult.

4.2 Observations and Findings

First observation, Table 1 reveals most of the developed pure recall-based GUA schemes within this time frame are draw-based. By implication it is highly expected that subsequent developed draw based pure recall schemes are likely to inherit the draw backs associated with the draw based category. Hence the research question, can draw based pure recall schemes be designed without necessarily inheriting draw backs associated with the draw based category? Also this establishes the need to explore alternative design approach to pure recall-based GUA that ensures such draw backs are not inherited.

Secondly, observed across pure recall schemes so far is that login credentials at the authentication stage, have to be reproduced, particularly in the exact same manner and order they had earlier been produced in the registration stage. At this point, we will like to call that "Static Credential Entry". Take the android pattern lock scheme for example, having registered an "L" shape in the registration phase, a user must reproduce the "L" shape in the exact same manner at every subsequent login sessions to be granted access. "Static" because the exact same series of steps must be followed across multiple login sessions. A major down side associated with static credential entry is that it supports observable repetitive routines, a characteristic detrimental to security. Observation attacks such as shoulder surfing, coordinated position noting, click based screen short capturing and camera recording attacks leverage on repetitive routines to acquire login credentials and compromise security [36].

Credential entry however takes a different characteristic with most recognition based schemes. For example "Passfaces", a Recognition based GUA authentication scheme based on face identification. Passfaces generates and assigns random set of human faces from a large image portfolio in the registration stage. These generated images form the user's password. The user is expected to memorize the presented faces through a familiarization process. The familiarization process imprints the assigned faces on the users mind. In the authentication stage, the user picks out earlier assigned faces one at a time, from successive group of nine (3x3 grid) faces to gain access to the system. Based on the image shuffling algorithm, it is highly unlikely that the image position will be the same for successive login sessions even though the underlining resulting password is the same. This, we refer to as "Dynamic credential entry". In other words, performing "different perceived" set of actions that results in the same underlining password and ultimately grants a user access to a system, reducing noticeable patters to the barest minimum. Logically a dynamic credential entry procedure such as found in Passfaces and other recognition based GUA schemes will better protect a user against such observation attacks. Hence another interesting research question, are all pure recall-based GUA schemes designed based on static credential entry? If they are, it is worth exploring for pure recall based GUA designed to accept dynamic credential inputs.

Thirdly, click based schemes thus far are only feasible in schemes that particularly involve images or cues. This clearly is the reason there are no schemes associated with user click events as credential input mechanisms in table 1. This is simply because clicks are only needed when images or cues are involved, thereby declassifying the resulting scheme as pure recall. At this point and interesting research question is raised, can pure a recall GUA schemes be built to accept login credentials on click events without losing its Pure recall characteristic?

5 CONCLUSION

This study categorized Pure Recall schemes based on login credential entry approach and Design Style in an attempt to take a closer look and analysis of schemes developed between the first 20 years (1996 to 2016). Via this categorization 3 key observations were made. First, that the vast majority of those schemes were draw-based, and expected to inherit the draw backs associated with the draw based category, unless there is a rethink to explore alternative design approaches. A second observation was that all schemes under review required users to reproduce login credentials, particularly in the exact same manner and order earlier produced in the registration stage, "Static credential entry". Unlike pure recall, most recognition based schemes rather the "Dynamic entry" approach. Thirdly observed was that no grid based scheme thus far was associated with click events as credential input approach. All observations are pointing to credential entry mechanisms of pure recall based GUA scheme. Hence the need to consider "Credential Entry" as a Contextual parameter associated User Design Factor. A later study will focus on this findings as basis to evaluate recent pure recall schemes. If results are consistent with these initial findings, credential entry mechanism approach will be worth exploring as basis for repositioning pure recall schemes as alternatives to text passwords.

REFERENCES

[1] Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2017c). The interplay between humans, technology and user authentication: A cognitive processing perspective. Computers in Human Behavior, 76, 184-200.

[2] Koved, L., & Stobert, E. (2016). Who are you?! Adventures in authentication (WAY). Workshop at the Symposium on Usable Privacy and Security (SOUPS 2016), USENIX Association.

[3] Seqrite. (2018) Importance of user authentication in network security. [Online]. Available: https://blogs.seqrite.com/

[4] Suo, X., Zhu, Y. & Owen, G. (2005). 'Graphical Passwords: A Survey'. 21st Annual ComputerSecurity Applications Conference (ACSAC'05). Tucson, USA: IEEE.10 pp.-472.

[5] Cain, A. A., Werner, S., & Still, J. D. (2017, May). Graphical authentication resistance to over-the-shoulder-attacks. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (pp. 2416-2422). ACM.

[6] Monrose, F. & Reiter, M. (2005). 'Graphical passwords'. Security and Usability. O'Reilly, ch.9, pp 147-164.

[7] Suo, X., Zhu, Y. & Owen, G. (2006). 'Analysis and Design of Graphical Password Techniques'. Advances in Visual Computing, (4292). pp 741-749.

[8] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005). 'PassPoints: Design and Longitudinal Evaluation of a Graphical Password System'. International Journal of Human Computer Studies, 63 (1). pp 102-127.

[9] Alsaiari, H. (2016). Graphical one-time password authentication. University of Plymouth: Faculty of Science and Engineering. 1-242.

[10] Katsini, C., Raptis, G. E., Fidas, C., & Avouris, N. (2018). Does image grid visualization affect password strength and creation time in graphical authentication?. In Proceedings of the 2018 International Conference on Advanced Visual Interfaces (p. 33). ACM.

[11] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. (2016). Security and Usability in Knowledge-based User Authentication: A Review. In Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI'16). ACM, New York, NY, USA, Article 63, 6 pages. https://doi.org/10.1145/3003733.3003764

[12] Katsini, C., Fidas, C., Belk, M., Avouris, N., & Samaras, G. (2017). Influences of users' cognitive strategies on graphical password composition. In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (pp. 2698-2705).

[13] Ma, Y., Feng, J., Kumin, L., & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. ACM Transactions on Accessible Computing, 4(4), Article 15, 27 pages.

[14] Nicholson, J., Coventry, L. & Briggs, P. (2013a). Age-related performance issues for PIN and face-based authentication systems. In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2013), ACM Press, 323-332.

[15] Belk Marios, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2015. A Personalized User Authentication Approach Based on Individual Differences in Information Processing. Interacting with Computers 27, 6: 706–723. http://dx.doi.org/10.1093/iwc/iwu033.

[16] Belk, M., Fidas, C., Katsini, C., Avouris, N., & Samaras, G. (2017a). Effects of human cognitive differences on interaction and visual behavior in graphical user authentication. In Proceedings of the IFIP TC13Conference on Human-Computer Interaction (INTERACT 2017), Springer-Verlag (to appear)

[17] Melicher, W., Kurilova, D., Segreti, S., Kalvani, P., Shay, R., Ur, B., Bauer, L., Christin, L., Cranor, L., &Mazurek, M. (2016). Usability and security of text passwords on mobile devices. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2016), ACM Press, 527-539.

[18] Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobiledevices on password composition and authentication performance. In Proceedings of the Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI 2014), ACM Press,461-470.

[19] Schlöglhofer, R., & Sametinger, J. (2012). Secure and usable authentication on mobile devices. In Proceedings of the ACM Conference on Advances in Mobile Computing & Multimedia (MoMM 2012),ACM Press, 257-262.Katsini, C., Raptis, G. E., Fidas, C., & Avouris, N. (2018). Does image grid visualization affect password strength and creation time in graphical authentication?. In Proceedings of the 2018 International Conference on Advanced Visual Interfaces (p. 33). ACM.

[20] Mihajlov, M., & Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interacting with Computers, 23(6), 582-593

[21] Thorpe, J., Al-Badawi, M., MacRae, B., & Salehi-Abari, A. (2014). The presentation effect on graphicalpasswords. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI2014). ACM Press, 2947-2950.

[22] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In Proceedings of theConference on Human Factors in Computing Systems (CHI 2011), ACM Press, 2595-2604.

[23] Hayashi, E., Hong, J., & Christin, N. (2011). Security through a different kind of obscurity: Evaluating distortion in graphical authentication schemes. In Proceedings of the ACM Conference on HumanFactors in Computing Systems (CHI 2011), ACM Press, 2055-2064.

[24] Alshehri, M., & Crawford, H. (2016). Using image saliency and regions of interest to encourage stronger graphical passwords. In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC 2016), ACM Press, 127-138.

[25] Belk, M., Pamboris, A., Fidas, C., Katsini, C., Avouris, N., & Samaras, G. (2017b). Sweet-spotting security and usability for intelligent graphical authentication mechanisms. In Proceedings of the International Conference on Web Intelligence (pp. 252-259).

[26] Greg E. Blonder, Graphical Password U.S. Patent No.5559961, 1996.

[27] Alsaiari, H., 2016. Graphical one-time password authentication (Doctoral dissertation, University of Plymouth).

[28] Biddle, R., Chiasson, S. & Van Oorschot, P. (2012). 'Graphical Passwords: Learning From theFirst Twelve Years'. ACM Computing Surveys (CSUR), 44 (4). pp 1-41.

[29] Tao, H. & Adams, C. (2008). 'Pass-Go: A Proposal to Improve the Usability of GraphicalPasswords'. International Journal of Network Security, 7 (2). pp 273-292.

[30] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. & Rubin, A. D. (1999). 'The design and analysisof graphical passwords'. Proceedings of the 8th USENIX Security Symposium. Washington, USA,pp 1-14.

[31] Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H. & Bhogle, P. (2015). 'Comparison ofGraphical Password Authentication Techniques'. International Journal of ComputerApplications, 116 (1). pp 11-14.

[32] Wu, T.-S., Lee, M.-L., Lin, H.-Y. & Wang, C.-Y. (2014). 'Shoulder-surfing-proof graphicalpassword authentication scheme'. International journal of information security, 13 (3). pp 245-254.

[33] Gupta, S., Sahni, S., Sabbu, P., Varma, S. & Gangashetty, S. V. (2012). 'Passblot: A HighlyScalable Graphical one Time Password System'. International Journal of Network Security & ItsApplications (IJNSA), 4 (2). pp 201-216.

[34] Chiang, H.-Y. & Chiasson, S. (2013). 'Improving User Authentication on Mobile Devices: ATouchscreen Graphical Password', Proceedings of the 15th international conference on Humancomputerinteraction with mobile devices and services. ACM, pp. 251-260.

[35] Tari, F., Ozok, A. & Holden, S. H. (2006). 'A Comparison of Perceived and Real Shoulder-surfingRisks Between Alphanumeric and Graphical Passwords'. Proceedings of the Second Symposiumon Usable Privacy and Security (SOUPS'06). Pittsburgh, USA: ACM, pp 56-66.

[36] Agarwal, M., Mehra, M., Pawar, R., & Shah, D. (2011, February). Secure authentication using dynamic virtual keyboard layout. In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (pp. 288-291).