International Journal of Research in Industrial Engineering
www.riejournal.com

Restricting Shoulder Surfing: A Modified Graphical Password Technique

P. Pandey[*]

Department of Master of Application, Jain Deemed to-be University, Jayanagar, Bengaluru, Karnataka, India.

ABSTRACT

Graphical passwords are the ways in which user click on the image or user can select the image to authenticate themselves instead of giving passwords. This technique is more secure that textual password techniques. In this article, the shoulder surfing preventive mechanism of graphical password authentication is given. Finally the login password system is proposed to deal with such type of problems. First time, we are introducing a modified approach is given to resolve the shoulder surfing based on recall and recognition based concepts. Usually it is seen that the most common vulnerability of graphical password is shoulder surfing attack. This research aims to analyze the usability feature of recognition based and recall based graphical password methods and present a technique to apply an image based password that is safe from the shoulder surfing attack. In the similar context, the purpose of this paper is to present an alternative way to apply the recall and recognition based technique that will be protective for guess through shoulder surfing. And this graphical technique will be easy to memories the authentication password and process of authentication.

Keywords: Graphical Password, Security, Authentication.

Article history: *Received: 04 August 2019* *Revised: 01 November 2019* *Accepted: 23 November 2018*

1. Introduction

Information technology has become the integral part of our life. To satisfy the need of the society, almost in each work, we use the technology. In current era computer science is major subject. It has many real life applications such as cloud computing [1], Internet of Things (IOT) [2, 3, 4, 5, 6, 7, 8, 9], artificial intelligence [10], virtualization environment [11], shortest path problem [12, 13, 14, 15, 16, 17, 18, 19], transportation problem [20, 21], internet security [22], uncertainty [23, 24, 25, 26] and so on. Information Technology (IT) is a mode by which user can use

[*] Corresponding author
E-mail address: praveenkumarpandey21@gmail.com

DOI: 10.22105/riej.2020.219732.1122

computers and internet to store, fetch, communicate, and utilize the information. So, all the organizations, industries and also every individual are using computer systems to preserve and share the information. The internet security plays a major role in all computer related applications. The internet security appears in many real-life applications, e.g. home security [27], banking system [28], education sector [29], defense system [30], railway [31], and so on. In this manuscript we discuss about the protection of authentication which is a part of internet security.

In some type of security system, user authentication has the primary importance. It provides the basis of access control and user accountability. Enforcing the rigorous password policy sometimes shows an incompatible effect [32]. Users interrelate with security technologies either directly or indirectly. For passive use comprehensibility may be adequate for users. For active use users need much more from their security results: ease of use, memorability, efficiency, effectiveness and satisfaction [33].

The companies and related organization or individual has the confidential information. When they operate in IT environment, their data security is very important. This is the primary concern that their identity and their data should be safe and not exposed to the outer world without user's permission. Authentication is the way to determine that the user is permit to access the specific recourses and systems or not. To safeguard the information, we use the passwords in systems. The most popular way is textual password techniques. We can apply this way of authentication to computer security, information security, device security and to secure the identity of a user. We use the alphanumeric username and password for authentication which has the significant drawbacks [34]. To overcome the vulnerability of the tradition authentication process, the visual and graphical techniques come to existence [34] that is the alternative solution for the existing systems. With the use of the password systems, we ensure that the particular authenticated user is able to get the access of the resource but now a day the standard methods of password authentication are subject to compromise with number of attack techniques. The graphical password techniques provides more secure way of password authentication rather than the textual authentication. Traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit [33].

Now to overcome the drawbacks the graphical password techniques introduces. It is proven that the images are easy to memorize rather than the complex alphanumeric passwords. It is resistant to social engineering, dictionary attack, key logger because images are used as a password [35].

Graphical password techniques can be categories into two categories such as: Recognition based and Recall based graphical password techniques.

Technique 1. (Recognition base password technique). In this, some images are presented at the time of registration and user has to select few images. While login, user has to select the correct image sequence from the images selected at the time of registration [36, 37, 38, 39, 40].

There are few techniques in recognition based graphical techniques which ensures to identify the images which was picked earlier [41]:

- Dhamija and perrig algorithm [36].
- Sobrado and Birget algorithm [37].
- Man et al. algorithm [38].
- Jansen et al. algorithm [39].
- Takada and Koike [40].

Technique 2. (Recall based graphical technique). In recall based graphical technique, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [42, 41, 35, 43, 44, 45]. Recall based algorithm techniques are categorized into two main parts and further they categorized into subparts as [35]:

- Pure recall-based technique:
  - Passdoodle technique [44].
  - Signature technique [43].
- Cued recall-based technique:
  - Blonder technique [42].
  - Pass points technique [45].

The above techniques entirely focus on recall mechanism and each has its importance to design the password systems.

Image based authentication mechanism is well known to deal with security attack. Pictorial authentication techniques are described by some researchers. The main contributions of this paper are as follows.

- To the best of our information, the solutions of image-based authentication present today have long authentication process and complex. The given solution of authentication is easy to memories and simple.
- A login technique that give the smooth and secure functioning in authentication without much mathematical complexities and technical issues. It will secure the login from shoulder surfing.
- Our proposed authentication has compared with some other existing image based login system for protection against shoulder surfing attack and anyone without more technical knowledge can use the given login process in very simple way.

The above techniques present the strong and improved process to safe the authentication process using the pictures. Some technique will give ways to protect the system from the shoulder surfing attacks. In Section 2, short discussions on existing system on graphical password systems are given and problems are distinguished. In Section 3, shortcomings and limitation of some of the existing model has been discussed. Section 4, describes our proposed system. The impact of the proposed system and their importance have discussed in Section 5. The final Section of this paper includes the conclusion about the work done to safeguard the system from shoulder surfing.

2. A Short Discussion on Existing Systems

The graphical password technique commonly faces the security compromise from shoulder surfing attack. Many researchers have given several ways to over the stated attack but the common thing is to secure the system with user friendly password recognition and easy to memorize the password. Some presented the strong ways to protect the password authentication but hard to memorize and tough to implement. Akansha et al. [35] presented a system that take the specified picture at the time of registration process and validate the user with grid of 25 images and in 2nd phase of login the user has to select the intersection point image and the user has to select the correct size of the click area, that calculate the X and Y axis. Zhao and Li [46] integrated both text based and image based techniques without changing the user profile for password but this is little complicated and longer login process. Gao et al. [47] gave the algorithm to reflect the drawing trends and position and user have to draw the password but the problem is to redraw the password with 100% accuracy, the gaps between user drawings are uncertain while the similarity threshold value is fixed [46]. Almulhem [32] introduced the system to chooses several Point-of-Interest (POI) regions in the picture at the time of registration and at login time user has to correctly pick the POIs and type the associated words but it is hard to recognize and less user friendly. Wiedenbeck et al. [33] presented a game like graphical architecture of authentication that extends the challenge response paradigm but the challenge is the longer time to carry out authentication. Wiedenbeck et al. [48] discussed the convex hull click scheme that extends the challenge response paradigm to resist shoulder-surfing but is suffering with the slow input speed drawback. Kumar et al. [49] introduce the system that input the sensitive data input by selecting from an on-screen keyboard using only the orientation of their pupils but demerit is that similar error rates to those of using a keyboard and needs marginal additional time over using it. Pictures may be a solution to few problems connected to traditional knowledge-based authentication process but that they are not a simple universal cure, since a week design can abolish the picture supremacy effect in memory [50].

The all above technique are analyzed on the basis of usability and security concern. It is seen that few techniques are strongly secure but nor easy to use and few are easy to user but longer response time and also some easy techniques are not fully reasonable for shoulder surfing. The proposed and implemented technique in this paper is easy to memorize and recognize as well as protect the password authentication from the shoulder surfing attack and some other type of attack techniques.

3. Shortcoming and Limitations on Some of the Existing Model

Akanksha et al. [35] has given concept of login through image-based authentication. Man et al. [38] have also given the login system based on Passface selections. As per my analysis the both the models have the following limitations:

3.1. Limitation on Akanksha et al. Proposed Model

Akanksha et al. [35] give the solution which is strongly covers the brute force attack but the selection of image need preciseness and mathematically calculations. To use the stated technique for password authentication, user should have some technical knowledge. Also, the presented system uses the session disconnection and calculation of password area. So, for the end user it is little difficult to remember the image selection.

3.2. Limitation on S Man et al. Proposed Model

S Man et al. [38] has given the technique to select the lot number of picture has to select as pass object associated with unique code and user has to type the string with unique code that is not easily memorable and the relative location in reference to no of eyes, are also not feasible for quick login process. The discussed techniques have some limitations in terms of technical and calculative knowledge to access the login and usually users feel difficulty to interact with the system.

4. Our Proposed System

According to the limitations discussed in above section, we are giving the reliable, easily accessible and identifiable approach of login and authentication. We are proposing the improved solution for the discussed authentication system. The methodology which is common for authentication is to use alphanumerical usernames and passwords. To sort out this problem, few researchers have proposed authentication process that use pictures as passwords [32]. The graphical approach replaces the close recall of alphanumeric codes with the identification of formerly learnt pictures, a skill at which peoples are remarkably skilled [51]. In continuation, the graphical password technique derived here is the joint process of recall and recognized base password technique with some textual code verification process by email or OTP. This system has two phases:

- Registration phase.
- Login phase.

4.1. Registration Phase

The following processes of registration are as follows:

Table 1. Process of registration.

Steps	Process of Registration
Step I:	User will enter the username.
Step II:	User will enter email.
Step III:	User will enter the valid contact number.
Step IV:	After that five security questions asked related to family questions e.g. birth place, grandfather name, father's name, date of birth and the person in family you like most.
Step V:	Now user can select the number of relation to use as password from the dropdown menu.
Step VI:	In next stage user has to select a family relation and their corresponding group of images according to the selection from dropdown menu. The family relation names are already given in a checkbox.
Step VII:	After that image category are displaying to right hand side having 10 images in each category. User has to select one category of image for one relation name, another category of image for next relation name on so on. And along with that there are some random images in the database with no category.
Step VIII:	Now to selecting picture category for respective relation name you have to specify that how many categories of images minimum you have to select to validate the password but you cannot give choice less than 3. For example if you chose 3 then you have to choose 3 type of images according to 3 relations in the family like mother, father, sister. If it is 4 then it can be grandfather, father, sister, uncle etc.
Step IX:	In the family each relation has its own id according to the relation and it would be the first latter of the relation name like father has id f, mother has m, brother has b, grandmother has gmo and so on. User has to give the distance value to select the image for first attempt, second attempt and third attempt. Suppose he will give 100px for first attempt 250px for second attempt and 300px for thirst attempt but the distance should not be more than 400px.
Step X:	After that registration will complete. This phase with be the recognition based graphical technique.

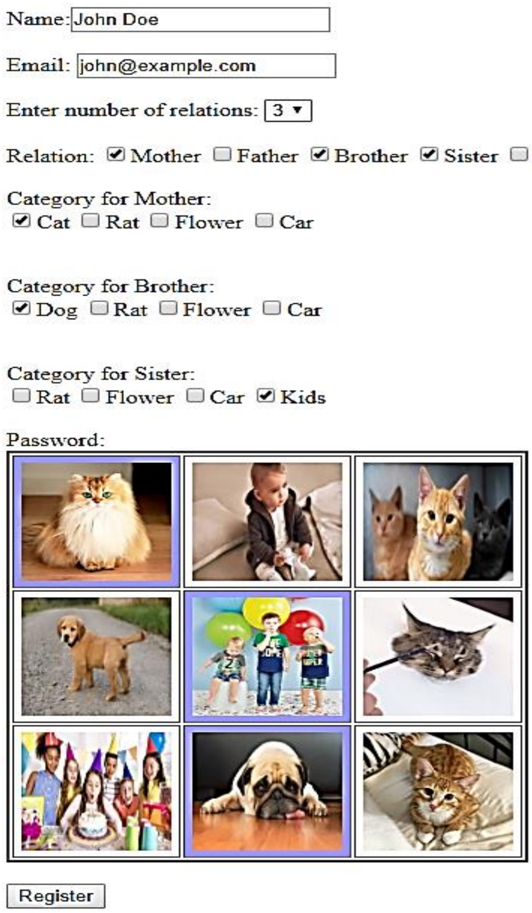
4.2. Login Phase

In the login phase user has to login to authenticate himself. This phase would be based on the recall based graphical technique. It includes the following steps.

Table 2. Process of login phase.

Steps	Process of Login Phase
Step I:	User has to give his valid username.
Step II:	After that the user has to give the password but password can be selected from the grid of images which will at the time of login according to registration process long with some random images. User has to select minimum number of pictures what he specified at the time of registration. At the time of login, Total number of picture grid will show as (n-3). Where n= Total number of relation grid at the time of registration.
Step III:	For each login attempt, according to the relation, first three grid will not display and in place of previous image grid, new 3 grid of images will add to the password picture.

Steps	Process of Login Phase
Step IV:	User has to select the minimum 3 image according to relation that the distance among the relation images should be more that 100 pixels.
Step V:	After that click on validate login button.



Name: John Doe

Email: john@example.com

Enter number of relations: 3 ▾

Relation: ☑ Mother □ Father ☑ Brother ☑ Sister □ Uncle □ Aunt

Category for Mother:
☑ Cat □ Rat □ Flower □ Car

Category for Brother:
☑ Dog □ Rat □ Flower □ Car

Category for Sister:
□ Rat □ Flower □ Car ☑ Kids

Password:

Figure 1. Process of registration.

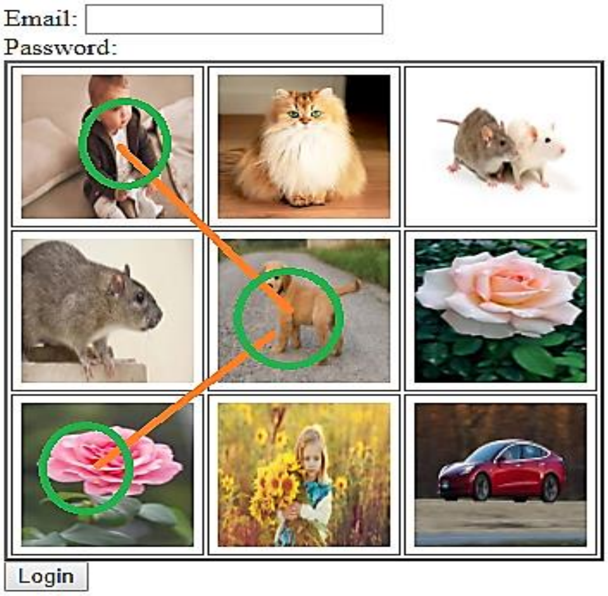


Figure 2. Process of login phase.

5. Result and Discussion

The proposed system overcomes the shortcoming of the Akanksha et al. [35] and Man et al. [38] proposed system and make the login process easy, simple and short as usability point of view ,based on the recognition and recall based technique. The main player of graphical password system is human, and they are good to recognize and memorize the pictures that related to daily life. In the system the creation of the password and the selection of the password both are simple enough to apply. One fact is very important in the process that the human has to memorize the two things: which category of picture is related to the particular relation name and the second one that the distance between the related images for login process. The stated process of login, protects the user from shoulder surfing, CCTV recording etc. In each login process, three image grids are not displaying so if any shoulder surfing occurs next time login it will impossible to guess the pattern of image to login process. Only the valid user can give the right password because he only knows the pattern of family tree images. And the calculation of image distance in the password will also matter because only user will know the distance information to select the graphical password. If user forgets the password then we can recover it by asking the questions related too users family so it is not difficult to memories the security questions. For this issues, in the system there is the security questions that is concern about the user personal practice so that it is easily memorable. To make the login process easy and secure, in the registration process, the password setting is taken from the real time use. Every person is familiar to its relation whether is social or blood relations so it is smooth process of registration for secure login using graphical method. In future there will be the implementation of some more security mechanism to enhance the security level by applying some rules of mathematics along with IoT infra to process the login.

6. Conclusion

This system is an amalgamation of recognition and recall based graphical password techniques. It is very easy to use and secure as contrast to previous graphical password authentication systems. Passwords can be generated and memorized easily because the password are related to the family tree so it is not forgettable. Randomization in both the authentication steps furnish strong security adverse to shoulder surfing. The shoulder surfing is very easy attack process to identify the need for login and you cannot recognize the person easily who is tampering your password. Proposed System reduce the probability of being vulnerable by shoulder surfing and protect your system to use by unauthorized access. Finally, the system is impervious to all other possible attacks also. This system can be used for highly secure systems and user feel more secure and smooth process of authentication rather than traditional methods.

Reference

[1] Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and computer-integrated manufacturing*, *28*(1), 75-86.

[2] MOHAPATRA, H. (2009). HCR using neural network (PhD’s Desertion, Biju Patnaik University of Technology).

[3] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447-457.

[4] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358-365.

[5] Mohapatra, H., Debnath, S., & Rath, A. K. (2019). *Energy management in wireless sensor network through EB-LEACH* (No. 1192). EasyChair.

[6] Nirgude, V., Nirgude, V., Mohapatra, H., & Shivarkar, S. (2017). Face recognition system using principal component analysis & linear discriminant analysis method simultaneously with 3d morphable model and neural network BPNN method. *Global journal of advanced engineering technologies and sciences*, 4. 1-6. https://www.researchgate.net/

[7] Panda, M., Pradhan, P., Mohapatra, H., & Barpanda, N. (2019). Fault tolerant routing in heterogeneous environment. *International journal of scientific & technology research, 8*(8). 1009-1013.

[8] Mohapatra, H., & Rath, A. K. (2019). Fault-tolerant mechanism for wireless sensor network. *IET wireless sensor systems*, *10*(1), 23-30. DOI: 10.1049/iet-wss.2019.0106

[9] Swain, D., Ramkrishna, G., Mahapatra, H., Patr, P., & Dhandrao, P. M. (2013). A novel sorting technique to sort elements in ascending order. *International journal of engineering and advanced technology*, *3*(1), 212-126.

[10] Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, *61*(4), 5-14.

[11] Zheng, H., Liu, D., Wang, J., & Liang, J. (2019). A QoE-perceived screen updates transmission scheme in desktop virtualization environment. *Multimedia tools and applications*, *78*(12), 16755-16781.

[12] Broumi, S., Dey, A., Talea, M., Bakali, A., Smarandache, F., Nagarajan, D., ... & Kumar, R. (2019). Shortest path problem using Bellman algorithm under neutrosophic environment. *Complex & intelligent systems*, *5*(4), 409-416.

[13] Kumar, R., Edalatpanah, S. A., Jha, S., Broumi, S., Singh, R., & Dey, A. (2019). A multi objective programming approach to solve integer valued neutrosophic shortest path problems. *Neutrosophic sets and systems*, *24*, 134-149.

[14] Kumar, R., Dey, A., Broumi, S., & Smarandache, F. (2020). A study of neutrosophic shortest path problem. In *neutrosophic graph theory and algorithms* (pp. 148-179). IGI Global.

[15] Kumar, R., Edalatpanah, S. A., Jha, S., & Singh, R. (2019). *A novel approach to solve gaussian valued neutrosophic shortest path problems*. Infinite study.

[16] Kumar, R., Edalatpanah, S. A., Jha, S., Gayen, S., & Singh, R. (2019). Shortest path problems using fuzzy weighted arc length. *International journal of innovative technology and exploring engineering*, *8*, 724-731.

[17] Kumar, R., Edaltpanah, S. A., Jha, S., & Broumi, S. (2018). Neutrosophic shortest path problem. *Neutrosophic sets and systems*, *23*(1), 2.

[18] Kumar, R., Jha, S., & Singh, R. (2020). A different approach for solving the shortest path problem under mixed fuzzy environment. *International journal of fuzzy system applications (IJFSA)*, *9*(2), 132-161.

[19] Kumar, R., Jha, S., & Singh, R. (2017). Shortest path problem in network with type-2 triangular fuzzy arc length. *Journal of applied research on industrial engineering*, *4*(1), 1-7.

[20] Kumar, R., Edalatpanah, S. A., Jha, S., & Singh, R. (2019). A Pythagorean fuzzy approach to the transportation problem. *Complex & intelligent systems*, *5*(2), 255-263.

[21] Smarandache, F., & Broumi, S. (Eds.). (2019). *Neutrosophic graph theory and algorithms*. Engineering science reference.

[22] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (In Press). Security aspects of Internet of things aided smart grids: a bibliometric survey. *Internet of things*. https://doi.org/10.1016/j.iot.2019.100111

[23] Gayen, S., Smarandache, F., Jha, S., & Kumar, R. (2019). Interval-valued neutrosophic subgroup based on interval-valued triple t-norm. In M. Abdel-Basset and F. Smarandache (Eds.), *Neutrosophic sets in decision analysis and operations research*. IGI-Global.

[24] Gayen, S., Smarandache, F., Jha, S., Singh, M. K., Broumi, S., & Kumar, R. (2020). Introduction to Plithogenic subgroup. *Neutrosophic graph theory and algorithms* (pp. 213-259). IGI Global.

[25] Umer Shuaib, M. S. (2019). On Some properties of o-anti fuzzy subgroups. *Computer science*, *14*(1), 215-230.

[26] Gayen, S., Jha, S., Singh, M., & Kumar, R. (2019). On a generalized notion of anti-fuzzy subgroup and some characterizations. *International journal of engineering and advanced technology (IJEAT)*, *8*(3), 385-390.

[27] Kumar, S. S., Khalkho, A., Agarwal, S., Prakash, S., Prasad, D., & Nath, V. (2019). Design of smart security systems for home automation. *Nanoelectronics, circuits and communication systems* (pp. 599-604). Singapore: Springer.

[28] Philip, J., & Shah, D. (2019). Implementing signature recognition system as SaaS on microsoft azure cloud. In *Data management, analytics and innovation* (pp. 479-488). Singapore: Springer.

[29] Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). The security challenges emerging from the technological developments. *Mobile networks and applications*, *24*(6), 2032-2037.

[30] Tanimoto, S., Takahashi, Y., Takeishi, A., Wangyal, S., Dechen, T., Sato, H., & Kanai, A. (2019, September). Concept proposal of multi-layer defense security countermeasures based on dynamic reconfiguration multi-perimeter lines. *International conference on network-based information systems* (pp. 413-422). Cham: Springer.

[31] Wen, T., Ge, Q., Lyu, X., Chen, L., Constantinou, C., Roberts, C., & Cai, B. (In Press). A cost-effective wireless network migration planning method supporting high-security enabled railway

data communication systems. *Journal of the franklin institute*. https://doi.org/10.1016/j.jfranklin.2019.01.037

[32] Almulhem, A. (2011, February). A graphical password authentication system. *2011 world congress on internet security (WorldCIS-2011)* (pp. 223-225). IEEE.

[33] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. *Proceedings of the 2005 symposium on usable privacy and security* (pp. 1-12). https://doi.org/10.1145/1073001.1073002

[34] Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *International journal of computer science and information security, 6*(2), 145-154. https://arxiv.org/

[35] Gokhale A., & Waghmare, V. (2016). The recognition and recall approach based graphical password technique, *International journal of computer applications*, 975, 8887.

[36] Dhamija, R., & Perrig, A. (2000, August). Deja Vu-A User Study: Using Images for authentication. *Proceedings of the 9th USENIX security symposium* (Vol. 9, pp. 4-4). Denver, Colorado, USA. https://www.usenix.org/

[37] Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2016). A shoulder surfing resistant graphical authentication system. *IEEE transactions on dependable and secure computing*, *15*(2), 180-193.

[38] Man, Sh., Hong, D., & Matthews, M. (2003). A shoulder-surfing resistant graphical password scheme - WIW. *Proceedings of international conference on security and management*. (pp.105-111). Las Vegas, Nevada, USA: CSREA Press.

[39] Jansen, W. (2004). Authenticating mobile device users through image selection. In K. Motgan (Ed), *the internet society: advances in learning, commerce and security.* WIT Press.

[40] *Edited By: K. MORGAN, University of Bergen, Norway and J.M. SPECTOR, Syracuse University, USA*

[41] *WIT transactions on information and communication technologies*, *30*.

[42] Takada, T., & Koike, H. (2003, September). Awase-E: image-based authentication for mobile phones using user's favorite images. *International conference on mobile human-computer interaction* (pp. 347-351). Berlin, Heidelberg: Springer.

[43] Eljetlawi, A. M. (2010, May). Graphical password: existing recognition base graphical password usability. *INC2010: 6th international conference on networked computing* (pp. 1-5). IEEE.

[44] Blonder, G. E. (1996). *U.S. Patent No. 5,559,961*. Washington, DC: U.S. Patent and Trademark Office.

[45] Syukri, A. F., Okamoto, E., & Mambo, M. (1998, July). A user identification system using signature written with mouse. *Australasian conference on information security and privacy* (pp. 403-414). Berlin, Heidelberg: Springer.

[46] Varenhorst, C., Kleek, M. V., & Rudolph, L. (2004). Passdoodles: A lightweight authentication method. *Research science institute*. Retrieved from https://pdfs.semanticscholar.org/8123/44ba01a9ed10db2ec3d17a56e852ac33cc78.pdf

[47] 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*(1-2), 102-127.

[48] Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. *21st international conference on advanced information networking and applications workshops (AINAW'07)* (Vol. 2, pp. 467-472). IEEE.

[49] Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008, December). Yagp: Yet another graphical password strategy. In *2008 Annual computer security applications conference (ACSAC)* (pp. 121-129). IEEE.

[50] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. *Proceedings of the working conference on advanced visual interfaces* (pp. 177-184). https://doi.org/10.1145/1133265.1133303

[51] Kumar, M., Garfinkel, T., Boneh, D., & Winograd, T. (2007, July). Reducing shoulder-surfing by using gaze-based password entry. *Proceedings of the 3rd symposium on usable privacy and security* (pp. 13-19). https://doi.org/10.1145/1280680.1280683

[52] Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In *21st Annual computer security applications conference (ACSAC'05)* (pp. 10-pp). IEEE.

[53] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International journal of human-computer studies*, *63*(1-2), 128-152.

[54] Al-Turjman, F. (2019). Cognitive routing protocol for disaster-inspired internet of things. *Future generation computer systems*, *92*, 1103-1115.