Graphical Password Authentication For Web Application

M Kirubha [1], V Susmitha[2], M Tamilselvan[3], M Thabaresh[4]
[1]Assistant Professor, Dept of Computer Science and Engineering
[2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4] Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

Abstract- *This paper suggests a two-factor graphical password authentication system, PassPage, which is highly sensitive to hacking and easy to use by distinguishing between web pages. It leverages the unconscious memory dependent on the websites that the user has been to. Whenever the user attempts to log into the website, the server returns 9 tiny pages that ask the user to not only take a guess and mouse over the irrelevant page but also to take a minute to search for 9 pages the user hasn't seen but has seen less than once for authentication along with the text password.*

Keywords- Graphical password, website, memory, server

I. INTRODUCTION

The graphical passwords offer a more satisfying option for a security alternative to standard alphanumeric passwords. Images are easily recalled by the mind and make for a more graphic and more processed image. Our scheme in this expanded abstract requires you to write your password on a piece of paper. We explain the function of the system with some illustrations, and highlight essential aspects of the system.

Authentication is an important part of every information security context. The user should be authenticated. It makes evident to people, as well as to programmers, who is entering one's system. Another form of user authentication is a standard matter of computer password lists or pin numbers, or combinations of numbers that both count and symbolize human input as numbers and provide the same result. They are very scalable and can easily be implemented and used.

Login codes can be in a combination that is at once both alphanumerical (lowercase) and five digits. There would be an easier time remembering them by an imposter, and, at the same time, impossible for an imposter to guess them. Users are known to use easily guessable and/or short passwords, as an easy target for dictionary and brute-forced attacks. This breaks up the rate of effective password recovery. A user will have to write their complicated passwords on a piece of paper for it to be stolen. A much stronger password can lead to a different outcome, since a more complicated password will take more time to memorize.
In addition to drastically increasing a user's chances of guessing passwords, some researchers suggest adding other factors in the process of guessing passwords. It is being said that a more secure alternative to a single letter password is to use the keyword that is easier to recall. A similar suggestion is to replace personal passwords with graphical passwords, in which icons of any kind are used instead of numerical passwords. It can be done be telling the user to down arrow to a certain region in the password rather than typing characters like in an alphanumeric password approach.

Graphical passwords lead to using images (also drawings) to make up passwords. In theory, interactive passwords are easier to recall because humans are best at remembering images instead of words. Even they should be evolved to be more resistant to brute force attacks, since the quest space becomes an infinite space.

Even using a graphical login strategy and creating a memorable password are two different ways of getting the password remembered in the future. In recognition-based approaches, the customer is authenticated by challenge him or her to recognize one or more photographs he or she selects during the registration stage. In recall-based strategies, a person is asked to repeat something that he or she developed or picked earlier during the registration stage

Passface recognition is a facial recognition based process, where the use of a security template provides a challenge to the user for recognition. There have been two early approaches to making passwords: A recall based approach and a graphical approach. In this technique, a customer is presented with many challenges before he/she can finally access his/her account. In the E-mail, the account must be confirmed with consistent actions. The Pass Points network solves the same problem Blonderson addresses, and also improves upon the original in certain ways.

II. LITERATURE REVIEW

Biddle Robert, Sonia Chiasson, and Paul C. Van Oorschot states many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering both usability and security aspects, as well as system evaluation. The paper first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, discuss methodological issues related to empirical evaluation, and identify areas for further research and improved methodology.[1]

Brostoff, Sacha, and M. Angela Sasse proposes proliferation of technology requiring user authentication has increased the number of passwords which users have to remember, creating a significant usability problem. This paper reports a usability comparison between a new mechanism for user authentication - Passfaces - and passwords, with 34 student participants in a 3-month field trial. Fewer login errors were made with Passfaces, even when periods between logins were long. On the computer facilities regularly chosen by participants to log in, Passfaces took a long time to execute. Participants consequently started their work later when using Passfaces than when using passwords, and logged into the system less often. The results emphasise the importance of evaluating the usability of security mechanisms in field trials.[2]

Bianchi, Andrea, Ian Oakley, and Hyoungshick Kim explains the PassBYOP is a new graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a system camera and then enter their password as a sequence of selections on live video of the token. Highly distinctive optical features are extracted from these selections and used as the password. We present three feasibility studies of PassBYOP examining its reliability, usability, and security against observation. The reliability study shows that image-feature based passwords are viable and suggests appropriate system thresholds—password items should contain a minimum of seven features, 40% of which must geometrically match originals stored on an authentication server in order to be judged equivalent. The usability study measures task completion times and error rates, revealing these to be 7.5 s and 9%, broadly comparable with prior graphical password systems that use static digital images. Finally, the security study highlights PassBYOP's resistance to observation attack—three attackers are unable to compromise a password using shoulder surfing, camerabased observation, or malware. These results indicate that PassBYOP shows promise for security while maintaining the usability of current graphical password schemes.[3]

Uellenbeck, Sebastian, et al. proposes an alternative to overcome the inherent limitations of text-based passwords, inspired by research that shows that the graphical memory of humans is particularly well developed. A graphical password scheme that has been widely adopted is the Android Unlock Pattern, a special case of the Pass-Go scheme with grid size restricted to 3 × 3 points and restricted stroke count. In this paper, we study the security of Android unlock patterns. By performing a large-scale user study, we measure actual user choices of patterns instead of theoretical considerations on password spaces. From this data we construct a model based on Markov chains that enables us to quantify the strength of Android unlock patterns. We found empirically that there is a high bias in the pattern selection process, e. g., the upper left corner and three-point long straight lines are very typical selection strategies. Consequently, the entropy of patterns is rather low, and our results indicate that the security offered by the scheme is less than the security of only three digit randomly-assigned PINs for guessing 20% of all passwords (i. e., we estimate a partial guessing entropy G0.2 of 9.10 bit). Based on these insights, we systematically improve the scheme by finding a small, but still effective change in the pattern layout that makes graphical user logins substantially more secure. By means of another user study, we show that some changes improve the security by more than doubling the space of actually used passwords (i. e., increasing the partial guessing entropy G0.2 to 10.81 bit).[4]

Stobert, Elizabeth, and Robert Biddle gives graphical passwords are an alternative form of authentication that use images for login, and leverage the picture superiority effect for good usability and memorability. Categories of graphical passwords have been distinguished on the basis of different kinds of memory retrieval (recall, cued-recall, and recognition). Psychological research suggests that leveraging recognition memory should be best, but this remains an open question in the password literature. This paper examines how different kinds of memory retrieval affect the memorability and usability of random assigned graphical passwords. A series of five studies of graphical and text passwords showed that participants were able to better remember recognition-based graphical passwords, but their usability was limited by slow login times. A graphical password scheme that leveraged recognition and recall memory was most successful at combining memorability and usability[5]

Zhu, Bin B., et al. proposes many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been under-explored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as PassPoints, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security[6].

Gao, Haichang, et al begins numerous graphical password schemes have been proposed, motivated by improving password usability and security, two key factors in password scheme evaluation. In this paper, we focus on the security aspects of existing graphical password schemes, which not only gives a simple introduction of attack methods but also intends to provide an in-depth analysis with specific schemes. The paper first categorizes existing graphical password schemes into four kinds according to the authentication style and provides a comprehensive introduction and analysis for each scheme, highlighting security aspects. Then we review the known attack methods, categorize them into two kinds, and summarize the security reported in some user studies of those schemes. Finally, some suggestions are given for future research.[7]

Renaud, Karen, et al says that users struggle to keep up with all their (textual) passwords is no secret. Thus, one could argue that the textual password needs to be replaced. One alternative is graphical authentication. A wide range of graphical mechanisms have been proposed in the research literature. Yet, the industry has not embraced these alternatives. We use nowadays (textual) passwords several times a day to mediate access to protected resources and to ensure that accountability is facilitated. Consequently, the main aspect of interest to decision-makers is the strength of an authentication mechanism to resist intrusion attempts. Yet, researchers proposing alternative mechanisms have primarily focused on the users' need for superior usability while the strength of the mechanisms often remains unknown to the decision makers. In this paper we describe a range of graphical authentication mechanisms and consider how much strength they exhibit, in comparison to the textual password. As basic criteria for this comparison, we use the standard guessability, observability and recordability metrics proposed by De Angeli et al. in 2005. The intention of this paper is to provide a better understanding of the potential for graphical mechanisms to be equal to, or superior to, the password in terms of meeting its most basic requirement namely resisting intrusion attempts.[9]

Khan, Mudassar Ali, et al says, security is important aspect in day to day life .So, everyone used various ways for security purpose. People use passwords for their security .Generally, everyone uses textual password. Textual password is combination of alphabets and numbers. People keep textual password as name of their favorite things, actors or actress, dish and meaningful word from dictionary. But the person who is very close to that person can easily guess the password. Graphical password is advanced version of password. Graphical passwords have received considerable attention lately as Potential alternatives to text-based passwords. Graphical password is composed of images, parts of images, or sketches. These passwords are very easy to use and remember. To overcome the Drawbacks of previously existing authentication technique. We present a new improved authentication technique, this authentication Scheme is called as “voiced 3D password”. The voiced 3D password is multi-password & multi-factor authentication system as it uses different authentication techniques such As textual password, sound password, graphical password, biometrical password. Most important part of 3d password scheme is inclusion of 3D virtual environment. We proposed that user first can write him/her user name and textual password and then the program provide a studio for choosing the specific sound, and then passed to 3D virtual environment. Shoulder-suffering attack is still can affect the schema of 3D password, so we add the Voiced 3D password to reduce that affect. [10]

III. EXISTING SYSTEM

Most websites are now using the username and text password as the default authentication for an account. Trying to recall a long, hardcoded password everyday can be very hard and potentially dangerous. Phrases like "Password 1,2,3" are bad and can help with stolen cell phones or tablets. Phrases like "Both lowercase letters and no caps" are monitored by networks and not allowed by mobile text messages to prevent viruses and malware attacks. Any websites use a dynamic code as a complement to the password and even for additional security. With two-factor authentication, users need to write down or memorise the passwords, and the codes are generally sent directly to their phones and then entered into web sites.

This is more efficient than typing codes into the browser, but it is often more labor-intensive.

There are several different methods which have been found to help in terms of the deletion of alphanumerical passwords. A possible alternative that is under consideration is to provide a particularly interesting or memorable expression rather than a single word. A proposed method for making passwords easier to memorise are graphics (images) in which users have to remember instead of alphanumerical passwords [7]. One way to sign onto a website is by telling the user to pick regions from a picture rather than typing characters like with the number system that we're familiar.

IV. PROPOSED SYSTEM

The use of the Graphical password protection may be another possible authentication factor which is more user-friendly. Only password system such could provide the protection against password theft, but most such solutions are inconveniently demanding. These take much memory away from the user if used on many websites. Our goal is to suggest a new authentication system that does not throw more stress toward our system or makes our system get hung up on. Our concept is to use the experience the customer has of their affiliate's website. It should be recalled when the user browse web sites that the user is browsing the website. It should have a high complexity rate too.

MODULES

The sign-up module

The customer provides the username, password and email address to sign up and get a new account. To make sure it is documented in the logs, the email address is seen publicly. The transmitted information is sent to the server. If the information is being released for use, the server stores it into the database and returns a session that will be opened on the device. Next, the visitor's computer signs him or herself in to the system.

The Browsing History Recording Module

The computational module (a module that records browsing history) continues to run after the user logs in to the website. When an internet domain is opened, there is a client script running within the domain. The script recognises the string of characters that identify a person, and then logs the browsing history to a database. In certain sites it is not clear what is the correct identification rate and what should be the click rate in order to include it in the article. If the page should be registered, it uploads its HTML content and along with the username, it uploads the HTML content to the server. The server stores the HTML content in a file that has a random name, and then stores the user's username and the file name in the user information database. The file name of the file is then returned to the recipient. Furthermore, in the event that the document requires to be stopped documenting, the script will preserve the fact that the page has been unblocked in between scrollings in the document. When the user closes the webpage window, the web script sends the file name and page size list to the web server. The server stores these measures in your account record: the time you spent on the site, the number of times you scrolled, and so on.

The Decoy Web Pages Maintenance Module.

The server returns a challenge consisting of correct pages and decoy pages when the user logs in, so the server must maintain a decoy web page database.

The server should have access to all the pages on the website. Admin selects random web pages and save them in the decoy page database. The topics of pages can be diverse or from the same website but pages with high click rate and low recognition rate should not be saved. The server saves the pages in HTML files and stores file name, file id of each web page in the database. If the number of decoy pages turns out to be easily guessable, old decoy pages can be deleted at regular time. Then, new set of decoy pages are added to the database.

The login module

This module is for the old users to login to their application. The registered users can directly login for accessing the website.

The user inputs the registered username and password, and then clicks ‘Login’ button. The page will display 9 small pages. The small pages might be transformed beforehand. The user must select all the visited pages from the 9 pages by clicking on them. After selecting all the visited pages, the user can log in. If the graphical authentication is passed and the pages are correct, the login is successful. If the login fails, the user can select the pages again or shuffle them again by refreshing the page. If the user attempts to log in after failing, the server refuses it and the user has to relogin with the text password. After the user clicks ‘Login’ button, the client first sends the username and the password to the server. Only if the password authentication is passed, the graphical authentication could start. The client sends the username to the server. The server returns the file names of 9 web pages, and then the client requests 9 HTML files from the server according to the file names. These 9 web pages consist of pages which have been visited by the user called real pages and pages which have never been visited by the user called decoy pages, and the client will display them. When the user clicks ‘Submit’, the client sends the username and the file names of all selected pages to the server. If the authentication is passed, the server returns a session to the client.

Hardware requirements:

Hardware	: Intel Core i3 Processor
Speed	: 2.01GHz
RAM	: 4GB
Hard Disk	: 500GB
Key Board	: Standard Windows

Software requirements:

Operating System	: Windows 7/8/10
Technology	: Java and J2EE
Web Technologies	: Html, JavaScript, CSS
IDE	: MyEclipse / NetBeans
Web Server	: Apache Tomcat
Database	: My SQL
Java Version	: J2SDK1.8

Page Selection Algorithm

First, the server selects all the pages the user visited and puts them into the allRealPages set, including the file names, the titles, browsing logs and adding time, and gets the size of the set. If size = 0, the graphical authentication is invalid and the email authentication has to be used. If 1 <= size <= 3, the server randomly selects 1~2 page(s) from allRealPages as the real pages. The server should select real pages which are visited by the user. After that, the server takes out decoy pages from the decoy page database, ensuring that the titles of selected decoy pages are different from those in allRealPages. The server takes out 9 pages in total. All the pages are loaded from HTML a file, which means the size of each page is only about 1 KB and all 9 pages can be loaded in a moment.

V. IMPLEMENTATION RESULTS

The following is the output on implementation of the system.

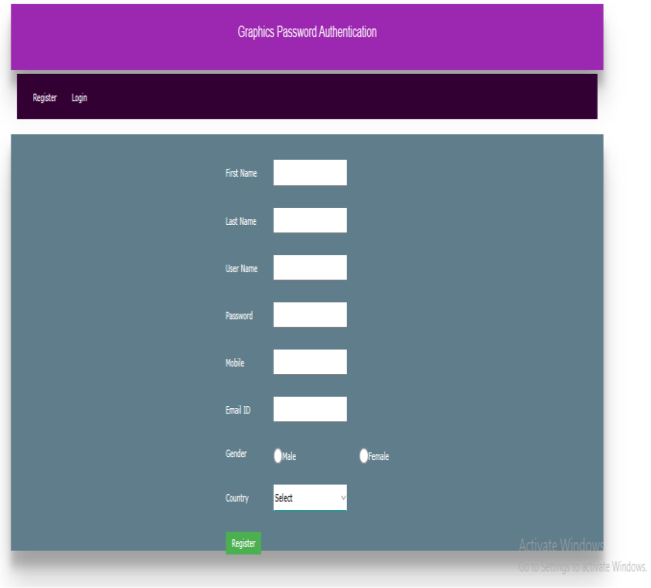
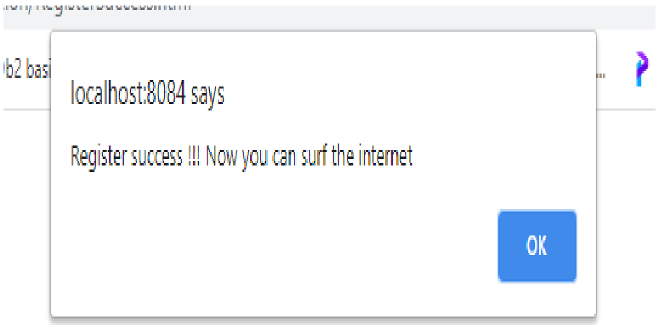


Figure 1: Registration Page

This page is for the new users. The user submits the email address, username and password to sign up an account. The email address is necessary in case the user forgets the secrets. The information is sent to the server.



localhost:8084 says

Register success !!! Now you can surf the internet

Figure 2: Successful registration

The user gets the popup after successful registration to surf the internet to capture web pages for the authentication during their further login.

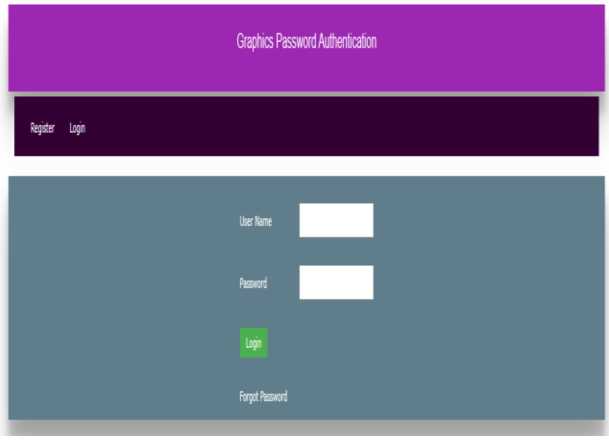


Figure 3: Login page

The registered users can login using their username and password they provided at the time of registration. If user is unable to remember their text password they can click ‘Forget Password’ for further proceedings.

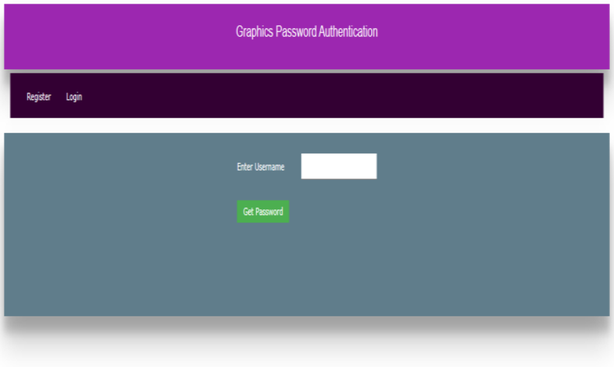
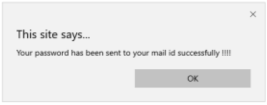


Figure 4: Forget Password Page

In Forget Password page the users need to enter their registered username and click ‘Get Password’.

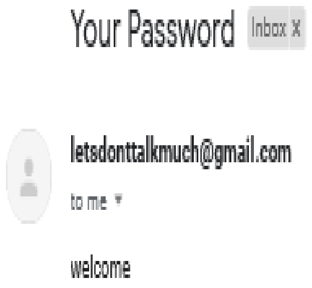


This site says...

Your password has been sent to your mail id successfully !!!!

Figure 5: Success message

In Forget Password page the user’s need to enter their registered username and click ‘Get Password’. Then the password will be sent to the user’s registered E-mail id.



Your Password

letsdonttalkmuch@gmail.com

to me

welcome

Figure 6: Password Mail

The user will receive their decrypted password to their registered email id from the admin. So it is necessary to give valid mail id during the time of registration.

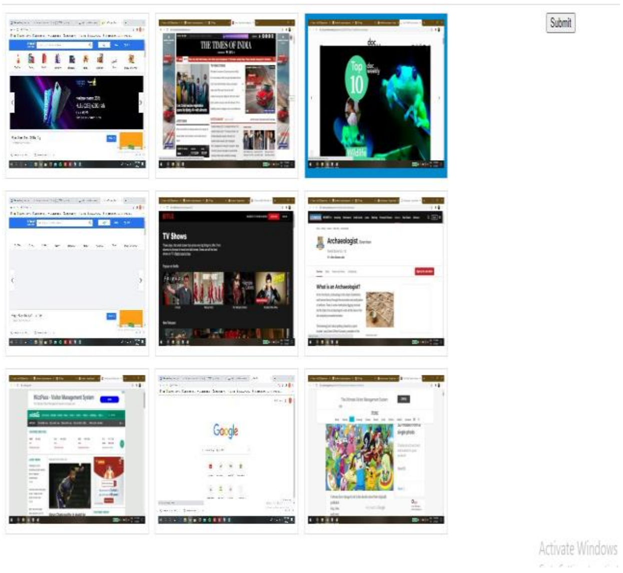
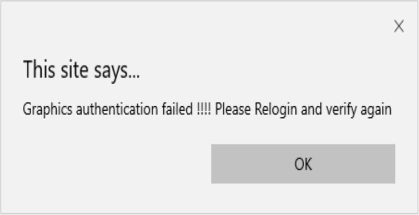


Figure 7: Web Page Password Verification

If the user login successfully using the text password then the next step is verification using the web pages. This is the final step for the authentication. The user has to select the web pages they have visited during the time of registration. After selecting the pages they should click ‘Submit’ button.



This site says...

Graphics authentication failed !!!! Please Relogin and verify again

Figure 8: Verification failed message

If the verification is failed, the user has to relogin using text password and then the web page verification.

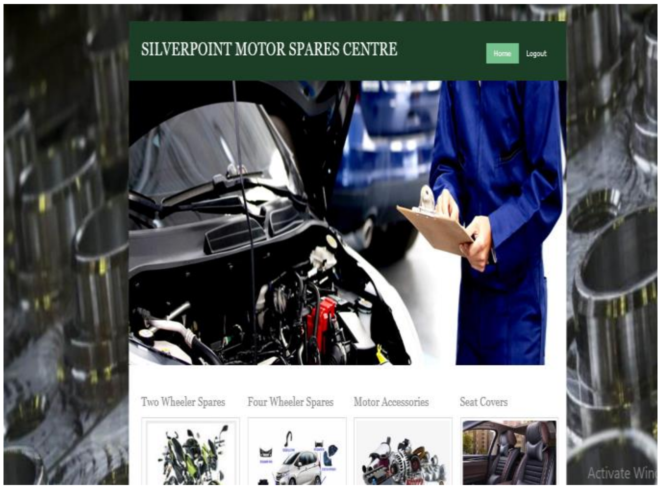


Figure 9: Successful login

If the verification is successfully done then the user is allowed to enter the website.

VI. CONCLUSION

This paper suggests a password scheme, PassPage, in which passwords can be scanned using a one-dimensional image. It is possible to accommodate both password stability and accessibility in one same scheme. It works by using the unconscious memories of surfing web sites.

Usability will always be the major concern to human being. There are new challenges to overcome faults in authentication. On the other hand, people with knowledge on this will always make advances in solving the problem. This paper has introduced a new prototype for pass page password type. A study of usability features of the existing methods has been done and mapping between the available features and features in general also has been done then new usable features extracted to be built in new system to make the graphical password authentication more usable and acceptable.

In the future, we would like to learn more about user habits when reading web pages so that the online graphical authentication problem is better for the users. The server can look at the pages which the user and figure out whether is whether the user can recall and identify easily. Besides, the login mechanism has not been streamlined, and the number of people who are able to register is still very high.

REFERENCES

[1] Biddle Robert, Sonia Chiasson, and Paul C. Van Oorschot. "Graphical passwords: Learning from the first twelve years." ACM Computing Surveys (CSUR) 44.4 (2012): 19.

[2] Brostoff, Sacha, and M. Angela Sasse. "Are Passfaces more usable than passwords? A field trial investigation." People and computers XIV—usability or else!. Springer, London, 2000. 405-424.

[3] Bianchi, Andrea, Ian Oakley, and Hyoungshick Kim. "PassBYOP: bring your own picture for securing graphical passwords." IEEE Transactions on Human-Machine Systems 46.3 (2015): 380-389.

[4] Uellenbeck, Sebastian, et al. "Quantifying the security of graphical passwords: the case of android unlock patterns." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.

[5] Stobert, Elizabeth, and Robert Biddle. "Memory retrieval and graphical passwords." Proceedings of the ninth symposium on usable privacy and security. ACM, 2013.

[6] Zhu, Bin B., et al. "CAPTCHA as graphical passwords—a new security primitive based on hard AI problems." IEEE transactions on information forensics and security 9.6 (2014): 891- 904. 11

[7] Gao, Haichang, et al. "A survey on the use of graphical passwords in security." JSW 8.7 (2013): 1678-1698.

[8] Rao, Kameswara, and Sushma Yalamanchili. "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords." International Journal of Information and Network Security 1.3 (2012): 163.

[9] Renaud, Karen, et al. "Are graphical authentication mechanisms as strong as passwords?." 2013 Federated Conference on Computer Science and Information Systems. IEEE, 2013.

[10] Khan, Mudassar Ali, et al. "g-RAT| A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices." IEEE Transactions on Consumer Electronics 65.2 (2019): 215-223.

[11] Mackie, Ian, and Merve Yıldırım. "A novel hybrid password authentication scheme based on text and

image." IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham, 2018.

[12] Mokal, P. H., and R. N. Devikar. "A survey on shoulder surfing resistant text based graphical password schemes." International Journal of Science and Research (IJSR) 3.4 (2014): 747- 750.

[13] Gaikwad, Anagha. "A Survey in Shoulder Surfing Resistant Graphical Authentication System." International Journal of Emerging Technology and Computer Science 2.3 (2017).

[14] Denning, Tamara, et al. "Exploring implicit memory for painless password recovery." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2011.

[15] Das, Sauvik, Eiji Hayashi, and Jason I. Hong. "Exploring capturable everyday memory for autobiographical authentication." Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. ACM, 2013.

[16] Sun, Huiping, et al. "Passapp: My app is my password!" Proceedings of the 17th International Conference on Human-Computer Interaction with Mobilbe Devices and Services. ACM, 2015.

[17] Nguyen, Ngu, and Stephan Sigg. "PassFrame: Generating image-based passwords from egocentric videos." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017.

[18] Woo, Simon, et al. "Life-experience passwords (leps)." Proceedings of the 32nd Annual Conference on Computer Security Applications. ACM, 2016.

[19] Xian Chu ,Huiping Sun ,Zhong Chen “PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records” Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2019 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020.