Implementation Of A Graphical Based Password For Folder Cryptography

Ms. Shilpa. L. Dhapade

GUIDE: Prof. Nilmani Verma, Department of Computer Science and Engineering
School of computer Engineering and IT, MATS University, Aarang, Raipur(C. G)

Abstract— **Now a day's most of the user are facing problem for providing the security to the folder, so that it will not be accesses by the unauthorised user. Sometimes our folder is going to be corrupted by the viruses which will corrupt our important files. Taking in action all these problems I have designed a model which will provide a best security to your folders and also save it from the viruses using graphical password authentication model. A Graphical Password based System are the systems in which images are used as a password instead of text password. Alphanumeric passwords are generally used for authentication process in most of the current systems. These passwords are usually short and memorable that's why they can be easily guessed by the attacker, but strong system-assigned password are difficult to remember In Graphical based system user click on images to authenticate themselves rather than type alphanumeric strings. Beginning around 1999, a multitude of graphical based password scheme which have been proposed as alternative to text based password scheme, motivated by the promise of improved password memorability and thus usability. This paper presents a detailed evaluation of the Persuasive Cued Click Points password scheme which provides high level of security and provides security to your folder with a platform independent environment. This paper also presents the SHA (secure hash algorithm) implementation used by the software for folder security used for folder security in java.**

Keywords— **Authentication, graphical password, usability, secure hash algorithm, software.**

I. INTRODUCTION

Because of the increasing threat to computer system and the information they store and process are valuable resources which need to be protected. Authentication refers to the techniques where users have to prove the claim of their identity to the identifier. There are many techniques through which users can be authenticated. Some of the password authentication techniques are knowledge based, token based, and biometric. Text password based technique and graphical password based technique comes under knowledge based authentication technique. A text password is a secret word or string of character that is used for user authentication to proven identity or for access approval to gain access to a resource. The easier a password is for the owner to remember generally means it will be easier for an attacker to guess. However, passwords which are difficult to remember may also reduce the security of a system because 1) user might need to write down or electronically store the password, 2) users will need frequent password resets and 3) users are more likely to re-use same password. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks [25]. A graphical based password is one promising alternatives of textual passwords, as according to human psychology, humans brain can recall or memories the visual thing in a well manner than text[24]. In graphical password based technique sequence of images are uses which are more memorable than sequence of characters. There are many graphical based password scheme is available. Of interest herein are cued-recall click-based graphical passwords. Example systems include passpoint, cued click points and persuasive cued click points. The guessing attacks capture attack, and hotspot problems reduce the security of passpoints and cued click points[15]. To overcome this we are trying to implement persuasive cued click points technique that is here we are using image password for authentication and security and we are also implementing SHA for encrypting the folder to provide more security to folder. The paper is structured as follow. We discuss about graphical password technique, persuasive cued click point, methodology, modules description, application, security and conclusion.

Fig. 1 Folder Security

II. BACKGROUND

Folder Security

Providing security to the folder is most challenging job for the developers to be developed which will neither access or decrypted by the crackers. So taking in action the concept I have developed a software model in java proving best security to your folder. For developing the same I have used a graphical based password for entering into the folder to be encrypted using secure hash algorithm. Persuasive Cued Click-Points (PCCP) is a click-based graphical password system in which a user is presented with a number of images in sequence, and is asked to choose one click-point on each image. The first image is assigned by the system, but each subsequent image in the sequence is determined by the user's

previous click. This means that clicking in different places on an earlier image leads the user to different next images. This provides users with a clue towards the correctness of their password entry attempt — if they see the correct image, they know they have selected the correct click-point. As with other click-based graphical passwords the user cannot be expected to repeat exact pixel selections. Thus an invisible *tolerance square* is defined around each click-point so that any of the enclosed pixels are considered acceptable. To help create more secure passwords, PCCP assists users during password creation by providing a *viewport* that highlights part of the image and asks users to choose a click-point within the viewport, thus resulting in more randomized choices. If users are unable to select a memorable point in the current viewport, they may press the shuffle button, which randomly repositions the viewport.

The random viewport, together with the shuffle button, has been shown to ensure that click-points are randomly distributed, addressing a problem seen in earlier schemes. PCCP has been shown to be more secure than other click-based password systems while maintaining login times and success rates comparable to text passwords. However, to be used as a replacement for text passwords, PCCP needs to be at least as secure as standard text passwords. We can adjust the security of PCCP by manipulating its parameters, which in turn affect the size of the theoretical password space.

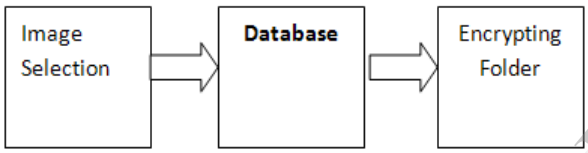

Fig: 2 Password creations

For providing the security to the folder, user will have to use image as a password which will be stored in the database with their pixel rate.

Graphical Password Techniques

Graphical passwords provide an alternative to text-based passwords that is intended to be more memorable and usable as human brain is good in remembering picture than textual character [26]. The technique used here is a cued click point concept. In systems using this concept, the users will have to identify the previously selected locations within the images available. The cued recall click points concept is based on selecting a particular location in the image that will be displayed to the user during the authentication process. To select particular location in this project the view port is provided. View is nothing but the framed area and persuades the user choice of selecting location or pixel within that framed area to create the password. Also this selection of locations or pixels in the image will be based only on the particular sequence. When the location or pixel in the first image is given correctly, then the next image will be displayed to the user in a particular sequence. The user will have to select the correct location or pixel in the sequence of images that will be displayed consequently. Sonia Chiasson , Elizabeth Stobert, Alain Forget , Robert Biddle , P.C. van Oorschot compared PCCP to text password and two related graphical password systems. Result show that PCCP is effective at reducing hotspots (area on the image where users are likely to select click-points within a password, while still maintaining usability.

III. PERSUASIVE CUED CLICK POINTS

Persuasive Technology used to motivate and influence people to behave in a desired manner and it insist users to select stronger passwords. The persuasive technology was first proposed by Fogg as a technology to make the users to have a better authentication system. A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click point, creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence. The authentication method using the persuasive click points uses a more secure scheme for passwords. In this method we have to select a location or pixel or tolerance area in the given image. When the pixel value is given correctly then the next image will be opened in a sequence. The pixel value will be generated in a random manner. So it is difficult for the hackers to find the pixel value which will be generated in a random manner. The random order in which the pixel value should be given will be known only to the user. This is made possible by a simple technique. The images that are used for the password will be stored in a database. In case if the hacker finds the first image by brute force attack, it will be difficult for the hackers to find the second pixel value as the pixel value will be generated randomly. The other advantage of this method is, if the pixel value entered proves to be wrong, then the next image will be displayed even in such cases. But the secure way that lies here is that only if the correct value is given, the user will be able to login. If the wrong pixel value is entered, next image will be displayed which not lead to the correct login will screen. The other advantage is that, only the user will know the random order of the pixel value generated [28]. An important goal of the authentication system is to provide support to users in selecting better passwords thus increasing security by expanding password space.

IV. METHODOLOGY

Our proposed system is new graphical passwords based hybrid system which is a combination of recognition and recall based

techniques and consists of two phases. During the first phase called Registration phase, the user has to type his username and create his password by clicking on the image provided by the systems in which a password consists of five click-points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location. After creation of graphical password user will browse the folder which he want to protect by encryption. Now user will be able to encrypt the desired folder and folder will get encrypted or locked.

During the second phase called Authentication phase user has to give his username and graphical password. , the user attempts to login with his username, he will be presented with the same initial image but this time with no view port but only all the tolerance squares will be effective. Now the user selects his choice in the first image that is to log in, a user must click within some system-defined tolerance region for each click-point. When he selects, our application will bring the next image related to that choice (tolerance square) and present to the user for next selection. When the user finishes selecting that way in five sequential images, and the selections matches the user's stored information, the things would unlock.

Steps for Password Creation:

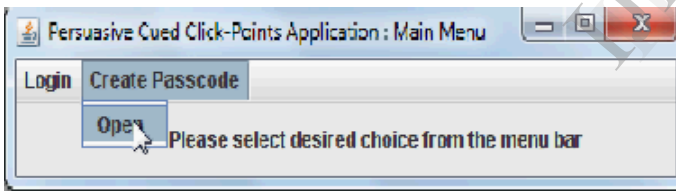

Fig: 3 Create Password

It is clear from the Fig:3 that user will have two process through which they can create the password and provide security to the folder whereas login will provide an authentication checking before accessing and decrypting the folder.

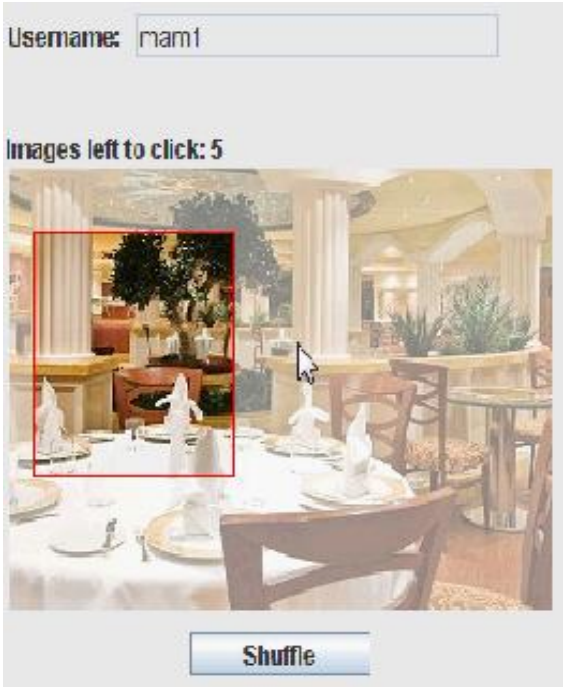

Fig: 4 Pixel Selections

Figure 3 illustrate an example of selecting the pixel rate from an image from a viewport.

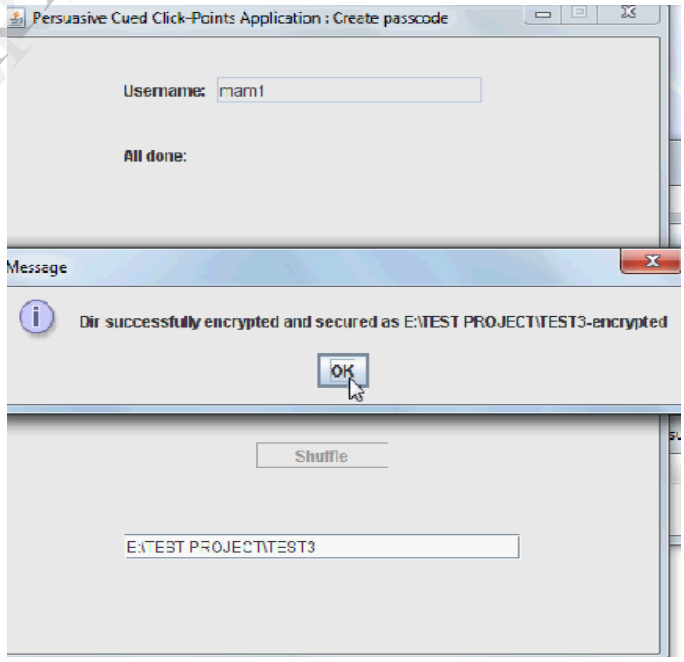

Fig:5 Successfully Execution of folder Security

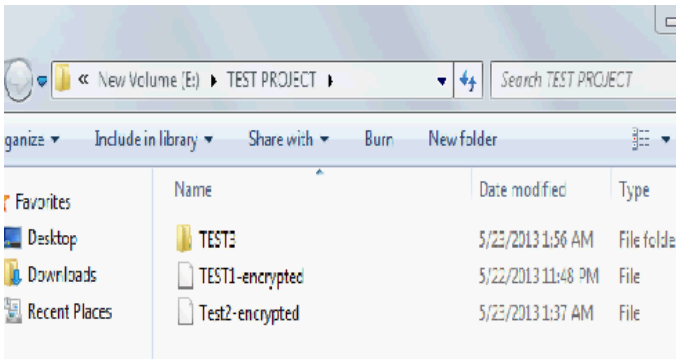

Fig: 6 Encrypted Folder TEST1 and TEST2

Database Checkout

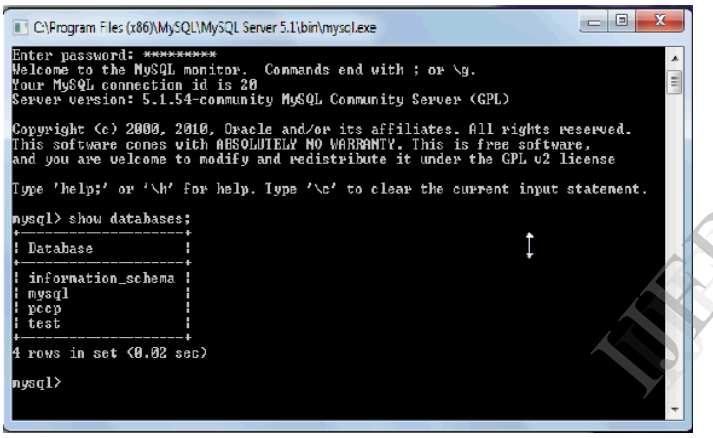

Fig: 7 Database check

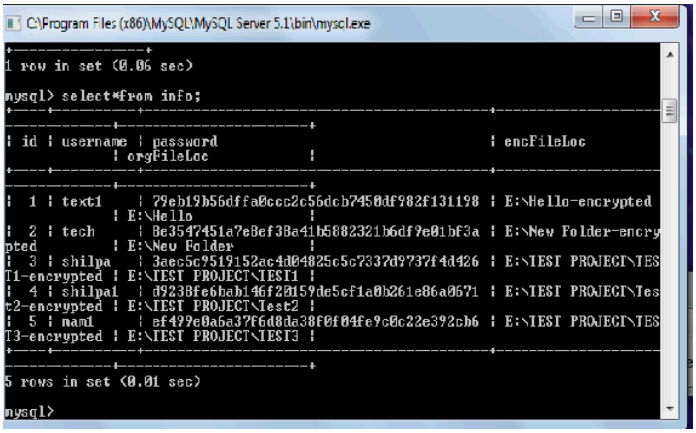

Fig: 8 Password Encrypted folders

V. MODULES DESCRIPTION

Modules attached with the application:

1) Registration process (create passcode): To implement registration process the following aspects come under it. A) PCCP technique for creating password .
2) Security process: Here we use SHA for encrypting folder
3) Authentication process (Login process)

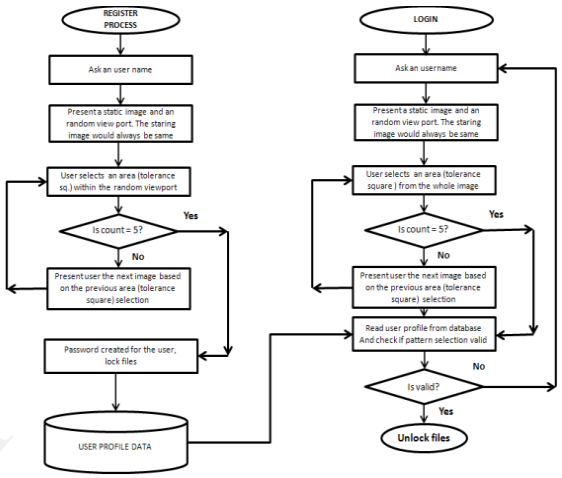

Fig: 9 Data Flow Diagram

VI. APPLICATION

We can apply this method of authentication in the online section, for windows security, drive cryptography, file cryptography etc. The increasing number of online services has raised another serious issue of number of web accounts a user has to maintain. As every website requires the user to register before accessing its resources, the user has to register with each website separately and maintain multiple login accounts. Remembering several password pairs are difficult for the users due to human memory limitations with alphanumeric passwords. Therefore, for easy recall of passwords, the users either set simple passwords (sometimes same) for all their accounts or set alphanumeric passwords and write it on piece of papers. But such practices suffer from various online attacks such as guessing, dictionary, phishing etc. and often lead to compromise of user's. This method of authentication is also applicable in network related application. This technique is highly suitable for places where high level security is required. This paper present the application of PCCP technique in our prototype model which is in folder form.

VII. SECURITY ASPECTS

This section discusses standard threats to graphical passwords and how PCCP's resistance to these threats. Attacks are classified as guessing or capture attacks (including malware which captures passwords).

7.1 Guessing Attacks

PassPoints and its relatives have attracted the most security analysis among graphical schemes. Efficient dictionary attacks have been enabled by two major weaknesses, both related to user choice. Hotspots [17, 2] are popular points or areas of an image with higher probability of being chosen by users as click-points. Patterns [3] are lines or simple geometric shapes formed by user-chosen click-points in a password. The attacks below target PassPoints itself, as opposed to evolved systems like PCCP.

8.2 Capture Attacks

Password capture attacks occur when attackers directly obtain passwords by intercepting user entered data, or by tricking users into revealing their passwords. Shoulder surfing and malware falls under the category capture attack. Shoulder-surfing is a targeted attack exacerbated by the visual aspect of graphical passwords. As users enter login information, an attacker may gain knowledge about their credentials by direct observation or external recording devices such as video cameras. High-resolution cameras with telephoto lenses and surveillance equipment [27] make shoulder-surfing a real concern if attackers target specific users and have access to their geographic location. Several existing graphical schemes believed to be resistant or immune to shoulder-surfing and one of those schemes is PCCP.

VIII. RESULTS

All the parameter in this research paper shows that implementing the technique PCCP for folder security provides a safe mechanism to the folder. It does not allow the unauthorized user to access the folder and also it protect from the viruses, malwares for corrupting the files present in the folder. Normally we can implement this technique in case of banking sector, security section, defense, online password, captcha, and drive cryptography.

IX. CONCLUSION

Taking in action all the security attack, viruses, malwares, the designed module will provide security to the folder preventing unauthorized access of your folder. It is clear from the above descriptive modules that, it will almost not possible to crack or guess the password by unauthorized users. The PCCP technique and Secure Hash Algorithm provides an environment in which the folder will be in safe condition. While encrypting the folder, it will be converted into zip file and then encrypted, which will not allow to enter any viruses and making damage to the files present in the folder. It will one of the safe mechanism for folder security.

This result might allow other considerations to be taken into account when making modifications to the system, such as the size of the screen on a mobile device, which would favour the use of smaller images. Future work in this area might include a field study to investigate these modifications in a more ecologically valid situation and more investigation into how the cost to usability is similarly

AFFECTED BY BOTH CLICK-POINTS AND IMAGE SIZE.

REFERENCES

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. Van Oorschot. Persuasive Cued Click-Points: Design ,implementation, and evauation of a knowledge-based authentication mechanism. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Oct 2011.

[2] K. Golofit. Click password under investigation. 12th European Symposium On Research In Computer Security, LNCS 4734, Sept 2007.

[3] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, Springer, 8(6):387-398, 2009.

[4] Sonia Chiasson , Alain Forget, Robert Biddle and P. C. Van Oorschot. Influencing user towards better password: Persuasive Cued Click-Points. I n Human Computer Interaction (HCI), The British Computer Society, September 2008.

[5] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 'An association-based graphical password design resistant to shouldersurfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005.

[6] Susan Wiedenbeck Jim Waters, Jean-Carnille Birget, Alex Brodskiy Nasir Memon. SOUPS' 05, July 6-8, 2005, Pittsburg, PA, USA.

[7] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe. Purely automated attacks on passpoints-style graphical password. IEEEE Trans. Info. Forensics and security, vol. 5, no. 3, pp. 393-405, 2011

[8] Stobert, S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. Exploring usability effects of increasing security in click-based graphical password. In Annual Computer Security Applications Conference (ACSAC), 2010.

[9] P. C. van Oorschot and j. thorepe. Exploting predictability in clicked-based graphical password, Journal of Computer Security, 2011..

[10] "Waziir Zada Khan, Mohammed Y Aalsalem and Yang Xiang. A Graphical Password Based System for Small Mobile Devices. International Journal of Computer Science Issue, Vol. 8, Issue 5, No 2, September 2011

[11] S. Wiedenbeck, J. Water, J. Birget, A. Brodskiy, and N. Memon, Passpoints: Desing and Longitudinal evaluation of a graphical password system. International Jounral of Human- Computer Studies, vol. 63, no. 1-2, pp. 102-127, 2005.

[12] Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" In Proceedings of the 9th USENIX Security Symposium, August 2000.

[13] L.Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002.

[14] E. Tulving and Z. Pearlstone. Availablity Versus Accessibility of information in memory for words. Journal of Verbal Learning, Vol. 5, pp. 381-391, 1966.

[15] S.Chiasson, A. Forget, and R. Biddle. Graphical password authentication using cued click points. In European

Symposium On Research in Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[16] A. Salehi-Abari, J. Thorpe, and P. van Oorschot. On purely automated attacks and click bassed graphical password . In Annual Computer Security Application conf.(ACSAC), 2008.

[17] A. Dirik, N. Menon, and J. Bireget. Modeling user choice in the passpoints graphical password scheme,. In 3rd ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[18] J. Thorpe and P. C. van Oorschot. Human –seeded attacks and exploiting hot-spots in graphical passwords. In 16th USENIX Security Symposium, August 2007.

[19] L. Jones, A. Anton, and J. Earp. Towards understanding user perceptions of authentication technology. In ACM Workshop on Privacy in electronic Society,2007.

[20] A. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. Transaction on Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, 2006.

[21] I. Jenmyn, A. Mayer, F. Monrose, M. reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX security Symposium August 1999.

[22] Robbert Biddle, S. Chaisson, P. C. van Oorschot. Graphical Password: Learing from the first Twelve Years, School of Computer Science, Carleton University, Tech.Rep. TR-11-01,January4, 2011.

[23] P. C. van Oorschot and J. Thorpe. On predictive modles and user-drawn graphical password. In ACM Transaction on information and System Security, 10(4):1-33, 2008

[24] J. Wolf. Visual Attention . In K. De Valois, Ed. Academic Press, 2000, pp. 335-386.

[25] Alankrita Ladage, Swapnil Gaikwad, Prof. A. B. Chougule. Graphical Based Password Authentication. International Journal of Engineering and Technology, vol. 2, Issue 4, April 2013.

[26] Nelson, D. L., Reed, U.S., and Walling, J. R. Pictorial Superiority Effects. Journal of Experimental Psychology. Human Learing and Memory 2(5), 523-528, 1976.

[27] B. Laxton, K. Wang, and S. Savage. Reconsidering physical key secrecy. Teleduplication via optical decoding. Conference of Conputer and Communication Security, 2008.

[28] Karthhik. K, Keerthana. R, Porkodi.A, Udhayakumar. S, Kesavan. S, Mr. Balamurugan. P.Defenses against Large Scale Online Password Guessing by Using Persuasive Cued Click Points. International Jounral of Computer Science and Mobile Computing.