

User Authentication Based On Persuasive Cued Click Points with Sound Signature

Jisha Anna Alex

M. Tech. Research Scholar, Dept of CSE
KMEA Engineering College
Aluva, India
jishaannaalex@gmail.com

Sheena Anees

Assistant Professor, Dept of IT
KMEA Engineering College
Aluva, India
sheenanees@gmail.com

A.Neela Madheswari

Associate Professor, Dept of CSE
KMEA Engineering College
Aluva, India
neela.madheswari@gmail.com

Abstract— Various graphical password schemes have been proposed as alternatives to text-based passwords. Researches have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solution. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. Cued click points (CCP) is a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The presence of hotspots remains as an issue in CCP. We propose a new click-based graphical password scheme for authentication called Persuasive Cued Click Points (PCCP) with sound signature. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. In order to provide greater security, the concept of viewport is introduced here. The viewport is positioned randomly, rather than specifically to avoid known hotspots. PCCP offers both improved usability and security. A graphical password system with a supportive sound signature increases the remembrance of the password. Here, user is asked to select a sound signature corresponding to click point. This sound signature will be used to help the user in recalling the click point on an image.

Keywords—Authentication; graphical password; hotspots; sound signature.

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text; graphical passwords are intended to

capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember [7].

A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password—a feature lacking in most schemes.

II. REVIEW OF RELATED WORKS

Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks [9], [10], [11]. Graphical passwords offer another alternative, and are the focus of this paper.

A. Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information [12]. A comprehensive review of graphical passwords is available elsewhere [13]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric [14]). In such systems, users identify and target previously selected locations within one or more

images. The images act as memory cues [15] to aid recall. Example systems include PassPoints [16] and Cued ClickPoints (CCP) [8].

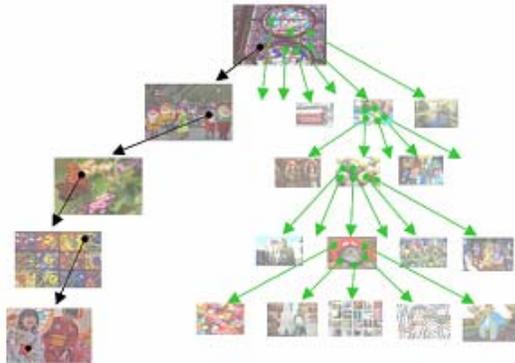


Fig. 1. A user navigates through images to form a CCP password. Each click determines the next image.

In PassPoints, passwords consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable [2], [16], [17], security weaknesses make passwords easier for attackers to predict. Hotspots [18], [19], [20], [21] are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints passwords [19], [20]. Users also tend to select their click-points in predictable patterns [6], [21] (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat [22]. A precursor to PCCP, Cued Click Points [8] 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 (Fig. 1), 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 claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an

image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP [6], so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem [3].

B. Persuasive Technology

Persuasive Technology was first articulated by Fogg [23] as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

III. PROPOSED SYSTEM

Previous work showed that hotspots and patterns reduce the security of click-based graphical passwords, as attackers can use skewed password distributions to predict and prioritize higher probability passwords for more successful guessing attacks. Visual attention research [24] shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue.

By adding a persuasive feature to CCP [8], PCCP [3] encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport (see Fig. 2). The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. The viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport.

While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like PassPoints and CCP, login click-points must be within the defined tolerance squares of the original points. A graphical password system with a supportive sound signature increases the remembrance of the password [42]. In proposed work a click-based graphical password scheme called Persuasive Cued Click Points (PCCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image[43].



Fig. 2. PCCP Create Password interface. The viewport highlights part of the image. (Pool image from [26].)

IV. USABILITY EVALUATION

We consider the following performance measures for memorability and usability [13]: login and recall success rates, the effect of shuffling on success rates.

A. Sound Signature

Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Persuasive Cued Click Points (PCCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image [43]. System showed

very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click-points.

B.Viewport details

The viewport visible during password creation must be large enough to allow some degree of user choice, but small enough to have its intended effect of distributing clickpoints across the image. Physiologically, the human eye can observe only a small part of an image at a time. Selecting a click-point requires high acuity vision using the fovea, the area of the retina with a high density of photoreceptor cells [39]. The size of the fovea limits foveal vision to an angle of approximately 1 degree within the direct line to the target of interest. At a normal viewing distance for a computer screen, say 60 cm, this results in sharp vision over an area of approximately 4cm². We chose the size of the viewport to fall within this area of sharp vision. The viewport size used here is 150x 150 pixels.

C.Shuffles

During password creation, PCCP users may press the shuffle button to randomly reposition the viewport. Fewer shuffles lead to more randomization of click-points across users. The shuffle button should be used moderately. Users used a common shuffling strategy throughout their session. They either consistently shuffled a lot at each trial or barely shuffled during the entire session. Users who barely shuffles selects their click point by focusing on the section of the image displayed in the viewport, while those who shuffled a lot scanned the entire image, selected their click-point, and then proceeded to shuffle until the viewport reached that area. Participants who barely shuffled, they felt that the viewport made it easier to select a secure click point. Those who shuffle a lot feel that the viewport hindered their ability to select the most obvious click-point on an image and that they had to shuffle repeatedly in order to reach this desired point.

V. EXPERIMENTAL RESULTS

The experimental results show that the shuffle button clicks have a significant role in the entire speed of the system and the required system performance is not obtained when more shuffle button clicks are made. Figures 3 and 4 shows the shuffle rate of a user. In Fig. 3, the user does not click the shuffle button. So the Success rate is 100% and Failure rate is 0%. Click prediction chart is another analysis done. Figures 5,6,7 shows the click prediction chart. Here when the user successfully login into the system, then the success of click prediction chart is 100%.When the user doesn't achieve the successful login in a single stretch or if he doesn't achieve

success, the error rate is increased. Fig.5 shows a sample click prediction chart which gives 100% success rate and 0% error rate. It is because the number of wrong clicks is 0. Click Prediction Chart for pass rate = 25% and error rate = 75% is given in Fig. 6. Here the number of wrong clicks is 4. In Fig. 7, the Click Prediction Chart for pass rate = 0% and error rate = 100% is shown. Here the number of wrong clicks is 5. The error rate becomes 100% when the number of wrong clicks is 5, since the maximum number of wrong clicks allowed in the system is 5.

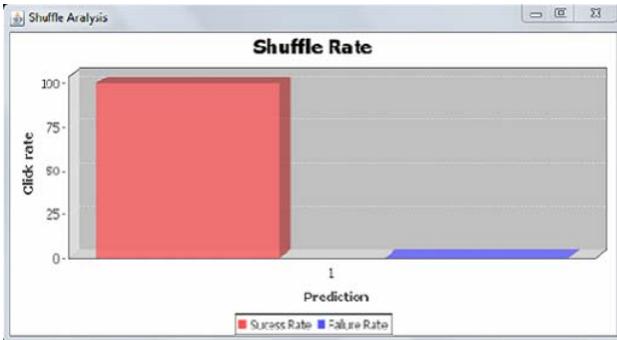


Fig 3: Shuffle Rate for not clicking shuffle button. (Success rate is 100% and Failure rate is 0%)

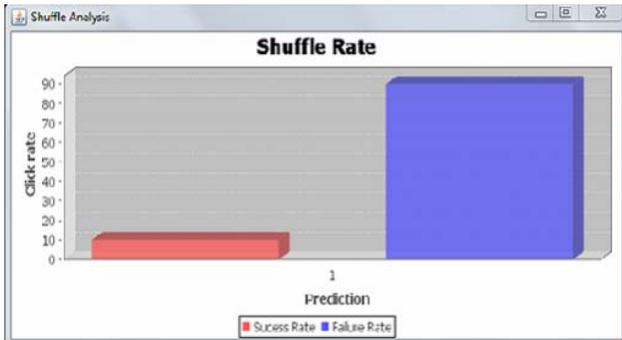


Fig.4 :Shuffle Rate for clicking shuffle button for 9 times.(Success rate is 10% and Failure rate is 90%)

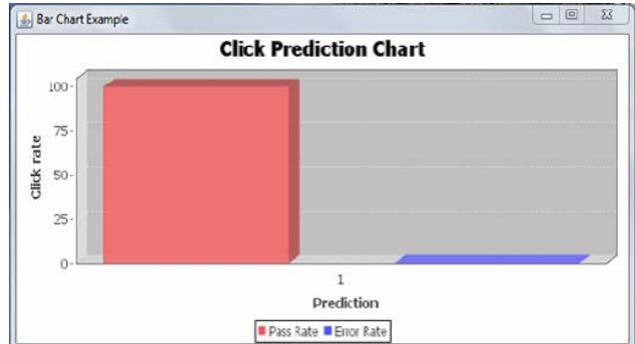


Fig 5: Click Prediction Chart for pass rate= 100% and error rate =0%. (No. of wrong clicks is 0)

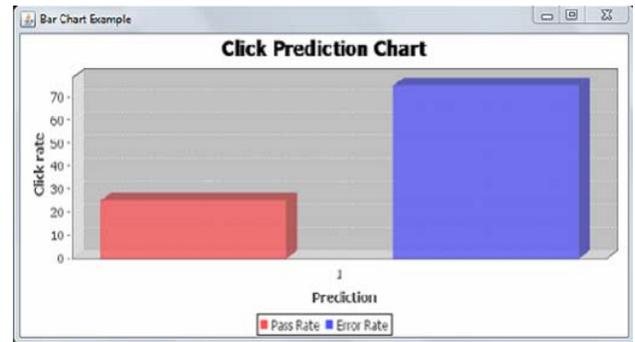


Fig 6: Click Prediction Chart for pass rate = 25% and error rate =75%. (No. of wrong clicks is 4)

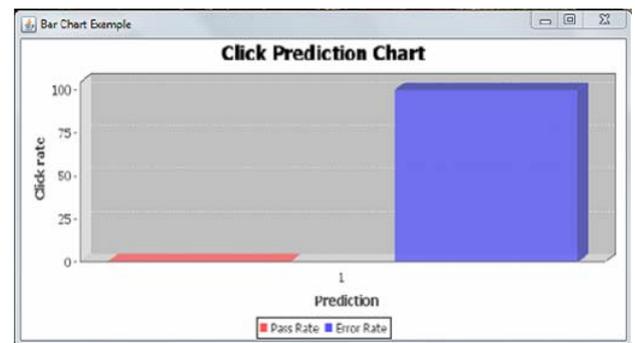


Fig. 7: Click Prediction Chart for pass rate = 0% and error rate = 100%. (No. of wrong clicks is 5)

VI. CONCLUSION

A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved. The approaches discussed in this paper present a middle

ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions. In PCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection. This persuasive strategy has also been used with some success to increase the randomness of text passwords [40]. Better user interface design can influence users to select stronger passwords. Adding sound signature to persuasive cued-click reduces the brute force attack. This system is helpful when user is logging after a long time. A key feature in PCCP is that creating a harder to guess password is the path of least resistance, likely making it more effective than schemes where secure behaviour adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space.

ACKNOWLEDGMENT

I am thankful to the Management, the Department of Computer Science and the Department of Information Technology of KMEA Engineering College for their valuable support and guidance.

REFERENCES

- [1] S. Chiasson, Elizabeth Stobert, Alain Forget, R. Biddle, van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April 2012.
- [2] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
- [3] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued ClickPoints," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
- [4] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.
- [5] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.
- [6] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.
- [7] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
- [8] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
- [9] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
- [10] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.
- [11] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
- [12] D. Nelson, V. Reed, and J. Walling, "Pictorial Superiority Effect," J. Experimental Psychology: Human Learning and Memory, vol. 2, no. 5, pp. 523-528, 1976.
- [13] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
- [14] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005.
- [15] E. Tulving and Z. Pearlstone, "Availability versus Accessibility of Information in Memory for Words," J. Verbal Learning and Verbal Behavior, vol. 5, pp. 381-391, 1966.
- [16] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
- [17] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.
- [18] K. Golofit, "Click Passwords under Investigation," Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept. 2007.
- [19] A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
- [20] J. Thorpe and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," Proc. 16th USENIX Security Symp., Aug. 2007.
- [21] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.
- [22] P.C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely Automated Attacks on PassPoints-Style Graphical Passwords," IEEE Trans. Information Forensics and Security, vol. 5, no. 3, pp. 393-405, Sept. 2010.
- [23] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
- [24] J. Wolf, "Visual Attention," Seeing, K. De Valois, ed., pp. 335-386, Academic Press, 2000.
- [25] D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes," Proc. 13th USENIX Security Symp., 2004.
- [26] PD Photo, PD Photo Website, <http://pdphoto.org>, Feb. 2007.
- [27] D. Florencio and C. Herley, "Where Do Security Policies Come from?," Proc. Symp. Usable Privacy and Security, 2010.
- [28] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), 2010.
- [29] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, "[Short Paper] The MVP Web-Based Authentication Framework," Proc. Financial Cryptography and Data Security (FC), LNCS, 2012.
- [30] S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot, "Centered Discretization with Application to Graphical Passwords," Proc. USENIX Workshop Usability, Psychology, and Security (UPSEC), Apr. 2008.

- [31] P. Diggle, *Statistical Analysis of Spatial Point Patterns*. Academic Press, 1983.
- [32] A. Baddeley and R. Turner, "Spatstat: An R Package for Analyzing Spatial Point Patterns," *J. Statistical Software*, vol. 12, no. 6, pp. 1-42, 2005.
- [33] M. van Lieshout and A. Baddeley, "A Nonparametric Measure of Spatial Interaction in Point Patterns," *Statistica Neerlandica*, vol. 50, no. 3, pp. 344-361, 1996.
- [34] M. van Lieshout and A. Baddeley, "A Nonparametric Measure of Spatial Interaction in Point Patterns," *Statistica Neerlandica*, vol. 50, no. 3, pp. 344-361, 1996.
- [35] P.C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," *J. Computer Security*, vol. 19, no. 4, pp. 669-702, 2011.
- [36] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Click-Based Graphical Passwords," *Proc. ACM SIGCHI Conf. Human Factors in Computing Systems (CHI)*, 2010.
- [37] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," *Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS)*, July 2008.
- [38] B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks," *Proc. Ninth ACM Conf. Computer and Comm. Security (CCS)*, Nov. 2002.
- [39] A. Duchowski, *Eye Tracking Methodology: Theory and Practice*, second ed. Springer, 2007.
- [40] D. Florencio and C. Herley, "A Large-Scale Study of WWW Password Habits," *Proc. 16th ACM Int'l World Wide Web Conf. (WWW)*, May 2007.
- [41] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," *Proc. Fourth Symp. Usable Privacy and Security (SOUPS)*, July 2008.
- [42] Saurabh Singh, Gavrav Agarval, "Integration of Sound Signature in Graphical Password Authentication System", *International Journal of Computer Applications (0975 - 8887)* Volume 12- No.9, January 2011
- [43] Saurabh Singh, Gavrav Agarval, "Integration of Sound Signature in Graphical Password Authentication System", *International Journal of Computer Applications (0975 - 8887)* Volume 12- No.9, January 2011.

AUTHORS PROFILE

Jisha Anna Alex pursued her B.Tech. during 2011 in Computer Science and Engineering from Musaliar College of Engineering and Technology Pathanamthitta, under Mahathma Gandhi University. She is pursuing her M.Tech. in Computer Science and Engineering from KMEA Engineering College under Mahathma Gandhi University, India. Her research interests are in Dependable and Secure Computing.

Sheena Anees received her B.Tech. degree during 2005 in Information Technology from Anna University and M.E. during 2007 in Computer Science and Engineering from Annamalai University. She is currently an Assistant Professor in IT department at KMEA Engineering College, MG University, India. Her research interests are in Network Security and Database Management Systems.

A. Neela Madheswari received her B.E. during 2000 and her M.E. during 2006 in Computer Science and Engineering. She is pursuing her Ph.D. in computer science and Engineering from Anna university, Chennai, India. Her research interests are in parallel computing and web technologies