ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152www.ijmece .com

Vol 6, Issuse.2 May 2018

Examining a Knowledge-Based Authentication System with Influencive Cued Click Points

Ch Venkatesh, B Sravanthi, B Ramya, PALLE AKHILA

Abstract

Most users use simple passwords that are easy for hackers to deduce, while robust passwords generated by the system are difficult for end users to remember. This research examines the three-pronged usability and security assessment of the Persuasive Cued Click Points graphical password system. Helping users make informed decisions is a crucial part of any authentication system. Stronger passwords. Improving safety by allowing for more effective password space to be used. Bad passwords contribute to the development of hotspots in click-based graphical passwords, which are regions of an image where users are more likely to choose click-points, facilitating more effective dictionary attacks by hackers. In order to make click-based graphical passwords more secure and harder to crack, the authors of this research used a persuasive technique based on the principle of social influence.

1. Introduction

Users have a hard time committing complex passwords to memory, and those that they do have a hard time forgetting are trivially simple to crack [1, 2, and 3]. Passwords should be strong and not easily guessed, but the authentication mechanism should nevertheless make them easy to remember. Stability, safety, and protection. Users are given a degree of freedom in creating their own passwords, while yet being nudged toward more secure options by the system. Choosing weak passwords (those are simple for attackers to guess) is a more time-consuming job, thus users should avoid doing so. By design, these authentication methods make it difficult to choose a strong password. The system should propose a strong password, and it's simpler for people to use that password than to come up with one on their own (a feature absent in most schemes).

The strategy relies on a lab research (20 individuals) to build the convincing click-based graphical password system. According to the data, our Persuasive Cued Click Points method successfully decreases the number of hotspots [2]-[3] (areas of the picture from which users are more likely to pick click points) without compromising usability. This study examines the trade-off between tolerance value and security rate. There's been a lot of talk about how visual passwords are the superior method of authentication since it's so simple to evaluate different users' password preferences. The method's adaptability to passwords in the form of text is specifically noted.

2. Background

Despite their widespread use, text passwords provide both security and usability challenges. Biometric systems and tokens are two examples of alternatives, although each has its own problems. [1]- [3]. In this work, we will be focusing on a

ASSISTANT PROFESSOR[1,2,3], STUDENT[4]
Department of CSE
Arjun College Of Technology & Sciences
Approved by AICTE& Affiliated to JNTUH

SPONSORED BY BRILLIANT BELLS EDUCATIONAL SCOITEY

Different kind of alternative: passwords made out of images. In 1996, Blonder defined the graphical passwords [3]. In general, methods for creating passwords using images are split into the sub-categories of recognition-based and recall-based visual methods. Users authenticate themselves with recognition-based approaches by looking at a series of photographs and picking out the ones they previously picked in the registration phase. During the registration process, the user will create or pick a graphical password, and then be prompted to remember that password. The technique of memory recall serves as the foundation of this work. Common text-based passwords are a common issue with knowledge-based authentication systems. Passwords created by individuals are notoriously simple for hackers to crack, whereas strong system-assigned passwords are notoriously difficult to remember. With a password authentication mechanism in place, users are urged to use complex yet easy-to-remember passwords. A strong password is recommended, and it is suggested that authentication mechanisms provide users that option. Weak passwords are less likely to be chosen since the system makes it more of a hassle to do so. Selecting a more robust password becomes the path of greatest resistance thanks to this method. Instead of making users work harder, as is the case with most schemes, this one makes it simple for them to use a secure password by simply following the system's recommendations.

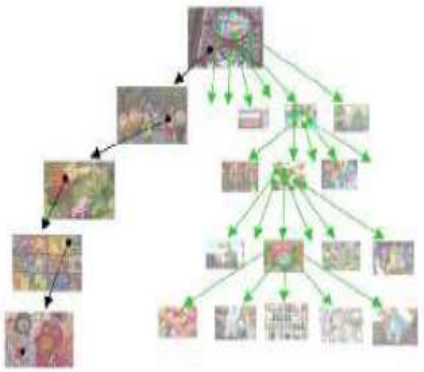


Fig. 1 User navigation trough images to form a PCCP password

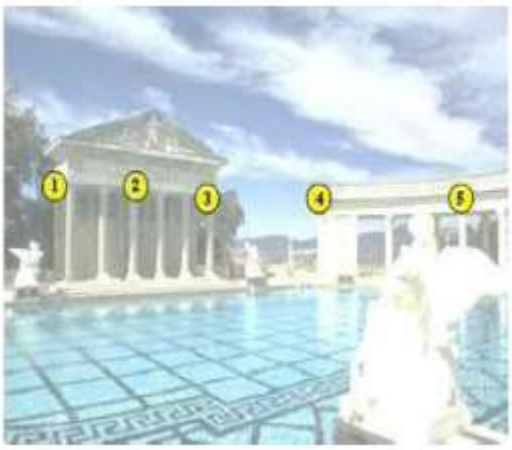
The goal of this strategy is to develop a graphical password system with improved usability and security based on user feedback gleaned from usability and security tests conducted on the Persuasive Cued Click-Points (PCCP) prototype. This study offers a unified integration of prior research and two web-based investigations, reinterpreting and updating statistical methodology to account for bigger data sets, and so offering a fresh assessment of passphrase handouts it provides a more thorough security analysis, up to and including the most recent assault on the system, and it lays out key implementation details. In order to improve comprehension before the actual implementation of new security mechanisms, the systematic assessment offers a thorough and integrated evaluation of PCCP including both usability and security problem. PCCP is compared to both text passwords and two comparable graphical password systems via eight user surveys. According to the findings, PCCP successfully eliminates hotspots and prevents patterns from being established by click-points inside a password without compromising usability.

I. Graphical Passwords That Are Clickable

Graphical password systems are an example of knowledge-based authentication that aims to capitalize on people's natural ability to remember visual cues. The comprehensive analysis of graphic passwords has already been written and published elsewhere. Visual passwords that can be recalled with a click are of particular importance here (which is also known as the loci metric). In such programs, the user chooses a target within an image (or several pictures) that they have already marked. In this case, the pictures serve as visual clues to help in memory recall. Among these systems are the Cued Click-Points (CCP) [4] and the Pass Points [5].

A password in Pass Points is a series of five clickable locations on a specific picture (refer Fig. 2). Customers may set their passwords by clicking on certain areas of a picture. To log in, the user must re-create the same series of clicks in the same precise order, within a tolerance square of the original click-points as established by the system. For this system, the usefulness and safety were assessed by the first writers, and then more that followed. We observed that although it is useable, there are still some security issues to be resolved. The primary issue with security is "hotspots," or instances where people repeatedly utilize the same click locations in their passwords. Attackers may construct attack dictionaries and guess Pass Points passwords with more success if they have access to information about these hotspots via means such as password harvesting or automated image processing. To conduct a dictionary attack, one must have a list of possible passwords (preferably

sorted in order of decreasing chance) and then attempt each one to determine whether it leads to a successful login for a specific account. An attack might either focus on a specific account or spread out across several other accounts in the aim of cracking one of them.



To lessen the prevalence of patterns and the value of hotspots to attackers, Cued Click Points were implemented in PCCP. CCP displays a series of five photos, each with a single clickable area, rather than five separate areas on a single image. The next picture shown depends on the position of the click-point entered (refer to Fig. 3), making the way through an image depending on the user's input. Photo album Users may only get to the next picture by clicking past the current one. Because a fresh picture sequence is generated whenever a password is created with various click-points [6].

The most significant benefits arise from the fact that entering passwords can now be thought of as a real cued-remember situation, in which each picture serves to instantly recall its associated click-points. Since the system displays the photos sequentially, users don't need to keep track of the order in which they clicked on each one. The CCP also offers hidden feedback that is said to be helpful to verified users alone. In the event that a user is attempting to log into the system and an unfamiliar picture appears, they will be prompted to renter their password after being informed that their previous attempt was unsuccessful. As a safeguard against incremental guessing attacks, an explicit indication of authentication failure is provided after the final click-point. Pattern-based assaults are ineffectual based on user testing and analysis, which found no indication of CCP. Despite the fact that exploiting hotspots requires far more effort on the part of attackers, the findings showed that this was still an issue [7].

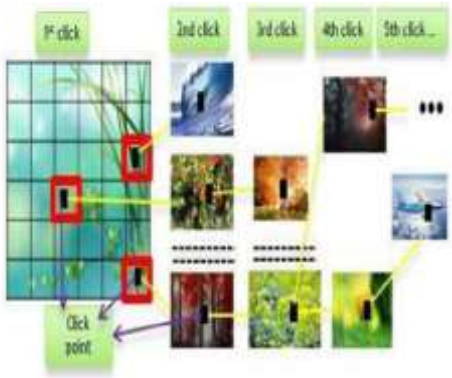


Fig. 3 click points as a password

II. Persuasive Technology

Fog [8] initially defined persuasive technology as the use of technology in order to inspire and persuade others to act in a predetermined way. An authentication system that uses persuasion technology should help and encourage users to choose strong passwords, but it shouldn't force users to accept passwords produced by the system. In order for it to be useful, people must not disregard the arguments and generated passphrases ought to be easy to recall [9]. PCCP does this by increasing the difficulty of choosing a weak password. Choosing a more secure password (one that isn't made up of of known hotspots or predictable patterns) is the hardest thing a user can do. As a result of a more uniform distribution of click-points, the formation of hotspots among users is reduced. Due to the more dispersed nature of click points, the method reduces the likelihood of hotspot development among users [10, 12].

3. PERSUASIVE CUED CLICK POINTS

Previous models have shown that the issue with click-based graphical passwords is the presence of hotspots, which narrows the effective password space and makes dictionary attacks more feasible. This article looked at whether users' password preferences may be swayed if they were encouraged to choose more randomly distributed click-points while still meeting the minimum requirements set by the system. The primary objective was to increase conformity by making the less secure activity (i.e., picking the lousy passwords) more onerous. To act safely now is to take the hard road. Using the CCP as a foundation, we've included a persuasive feature to encourage users to choose strong passwords and to hinder them from choosing passwords with all five click-points being vulnerable. In this case, slightly tinted images with a randomly placed viewport were used when users generated passwords (refer Fig. 4). Although the viewport is placed arbitrarily with the exception of avoiding existing hotspots, attackers

might use this knowledge to better their guessing and therefore create new hotspots. The viewport's dimensions were chosen to maximize the number of points on display while yet covering an acceptable subset of the whole set. Users could only make their click selections within of the highlighted viewport. They may hit the "shuffle" button to randomly rotate the viewport if they didn't want to or couldn't choose the click point in the area. Since users may reshuffle whenever they liked, the password generation process slowed down dramatically. Password entry prompted the appearance of a viewport button and a shuffle option. Login screens and pictures were seen properly throughout this confirmation phase; the viewport was not darkened, and users could click anywhere.

Our working hypothesis was that a) Users may tailor their level of security to their own requirements and preferences by drawing from a variety of perspectives.

- As a result, (b), the user will be less worried that they've chosen a potential danger zone.
- Users' clicks will be distributed at random, and thus will not cause the emergence of any new hotspots.
- Compared to the legacy CCP system, login security success rates will improve.
- Success rates for login security will rise when perspective drops.
- Users of the PCCP system will feel safer about sharing their passwords than they did with the previous CCP.

Fig. 4 PCCP Create Password interface

For every given password scheme, the theoretical password space is simply the maximum possible number of different passwords. As the theoretical password space grows, the probability that every given guess will be right for a given password decreases. Given an image of dimension ((w h)/t2) c), where w and h are the width and height, respectively, the theoretical password space in PCCP is Click-points in a password are multiplied by the picture's width and height in pixels (w * h) divided by the size of a tolerance square (t2) to yield the total number of tolerance squares per image (c, usually set to 5 in our experiments).

4. SYSTEM DESIGN

Modules for user registration, image selection, and system login make up the system's trifled structure (refer Fig. 5).

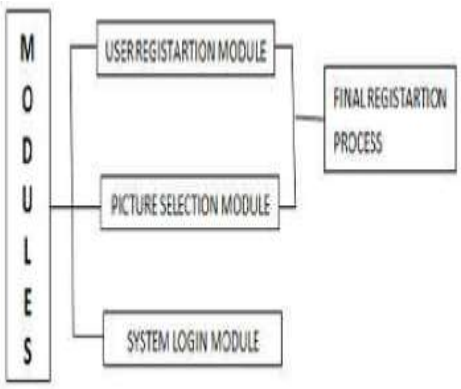


Fig. 5 System modules

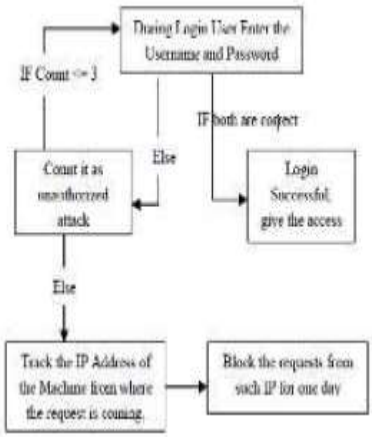


Fig. 6 system login module

A user's user name may double as a tolerance value in the user registration module's user name field (tolerance value which is use to compare registration profile vector with the login profile vector). User registration data submitted during the first phase of usage are kept in a database and retrieved during subsequent logins. To the testing and validation phase. In the picture-picking stage, users choose images to use as passwords; these images are then broken down into a series of five click-points. Users are free to utilize any part of the picture as a password entry point. During the process of making a password, the screen becomes

dark except for a tiny view port at an arbitrary location. Clicking anything requires the user to choose where in the viewport they want to click. The Shuffle button allows users to randomly move the view port if they are unable or unable to choose the location in the current view port. Passwords chosen at random are less likely to include hotspots, as shown by the view port. The user who is set on a certain click point may still do so by repositioning the view port till it reaches the desired spot, but doing so will take much more time and effort. After logging into the system, the photos are shown properly, without a viewport, and the clicks are replicated in the right order within a tolerance square of the original click-points as stated by the system.

I. User registration flow chart

The user registration process, which includes the registration and photo selection steps shown in the flowchart below (see Fig. 7), is shown in detail below. Initiating the process begins with entering a user id and a tolerance value. After a user has filled out all of their profile information, they may go on to the next level, which is choosing between one and five click points on the created photos. When the preceding steps are finished, a user profile vector will be generated.

II. Login flow chart

Referring to Figure 8, the first step in the login process involves inputting the same unique user ID that was used during registration. With the system-defined tolerance square of the original click-points, the pictures are shown properly, either by shade or the viewport, and they play back the sequence of clicks in the right order. Following the steps outlined above, a user's profile vector may be opened.

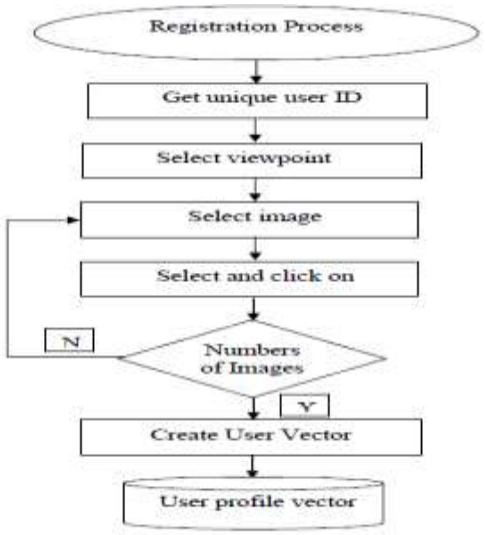


Fig. 7 User registration flowchart

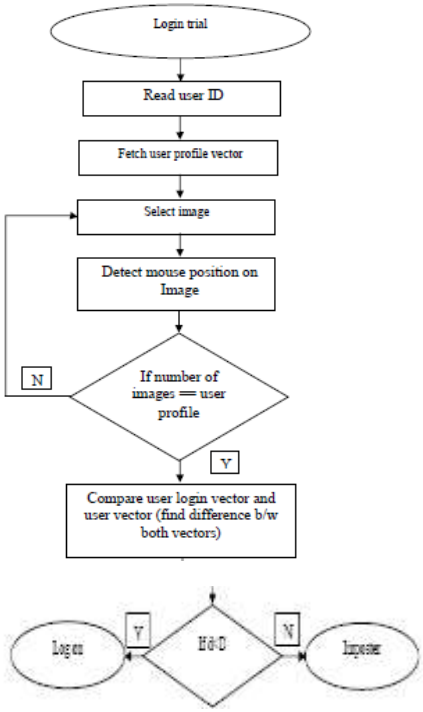


Fig. 8 Login phase flowchart

5. RESULTS

We performed a lab study to compare the login success rate and security success rate of current CCPs and suggested PCCPs, and our research was geared at discovering methods for improving the efficiency of the tolerance value.

I. Efficiency of the tolerance value

At first, eight people are taken into consideration for the study. For each person to unlock the password, they must choose 5 click points across 5 unique photos. There are many distinct characters (image details) in each picture, and the user must choose one of these characters (image details) to complete the sequence of clicks. Similarly, participants choose a click location in each of the visuals. The participant then logs in using the password, while the other participants are arranged in a line behind the first and instructed to look over his shoulder while he enters the password (click points on the images)[14]. After the first user logs out, the other users are prompted to use the same password they saw the initial user use.

Valuation of tolerance: This number represents how near you are to the actual "click" location. Given that it is unreasonable to expect a user to click on a single precise pixel, we allow for a "tolerance zone" that encompasses the area surrounding the initial click point. The success rate is the proportion of total trials that result in a positive outcome. Rates of success are determined by tallying the number of runs that ended with no hiccups or restarts. Shoulder surfing refers to when an observer stands behind a person inputting a

password and reads it off of their shoulder. In this case, the attacker attempts to capture their target. When an attacker intercepts user input or tricks victims into disclosing their credentials, they are committing a direct password assault. The effectiveness of the PCCP approach with respect to the tolerance value is shown in table I below. Figure 9 displays the findings on a graph depicting the tolerance value vs. the success rate in terms of security (refer fig. 10).

Table I Efficiency of tolerance value in PCCP method

Sl. No	Tolerance Value	Success Rate	Percentage of success rate	Security (in percentage)
1	5	7/8	87.5	12.5
2	4	5/8	62.5	37.5
3	3	3/8	37.5	62.5
4	2	2/8	25	75
5	1	0/8	0	100

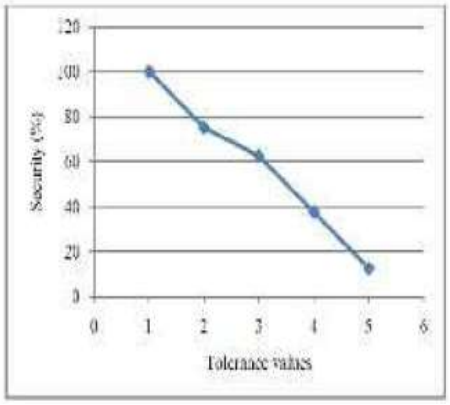
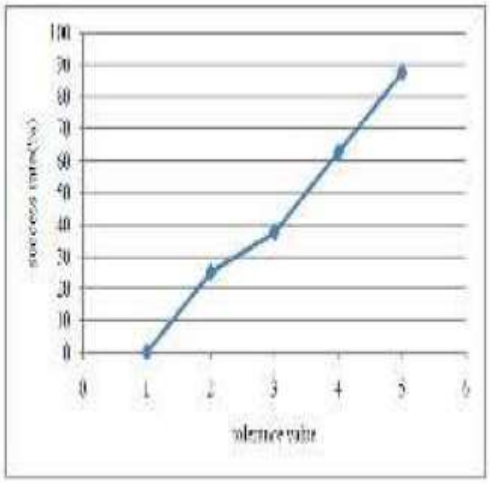


Fig. 9 Security Fig. Increases with decrease in the tolerance value.



. 10 Success rate increases with increase in the tolerance value

II. Comparison between login Success rate and security success rates of existing CCP and proposed PCCP

There is information on the proportion of people who are successful on their first try and within three tries. When the password is entered properly on the first try, without making any typos, we say that it was a first-try success. There were less than three failures per 100 tries. If the wrong password is entered after clicking the Login button, an error will ensue.

Table II PCCP success rates (all level) and security success rates compared to CCP

	CCP		PCCP (100*100 VP)		PCCP (75*75 VP)		PCCP (50*50 VP)	
	Success rate (%)	Security Success rate (%)	Success rate (%)	Security success rate (%)	Success rate (%)	Security Success rate (%)	success rate(%)	Security Success rate(%)
User1	4/5 (80)	20	3/5 (60)	40	4/5(80)	20	2/5(40)	60
User2	3/5 (60)	40	2/5 (40)	60	2/5(40)	60	3/5(60)	40
User3	5/5 (100)	0	4/5 (80)	20	2/5(40)	60	2/5(40)	60
		20 (mean rate)		40 (mean rate)		70 (mean rate)		80 (mean rate)

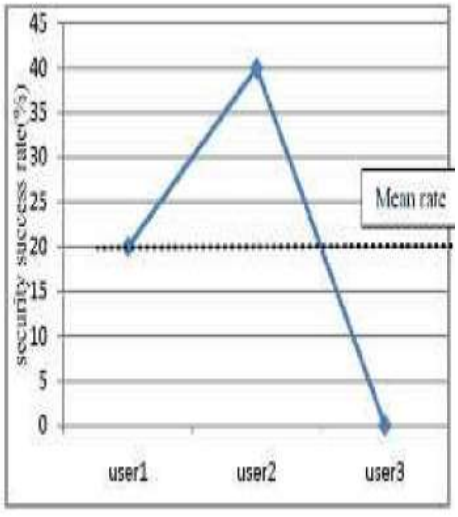


Fig.11 CCP mean rate

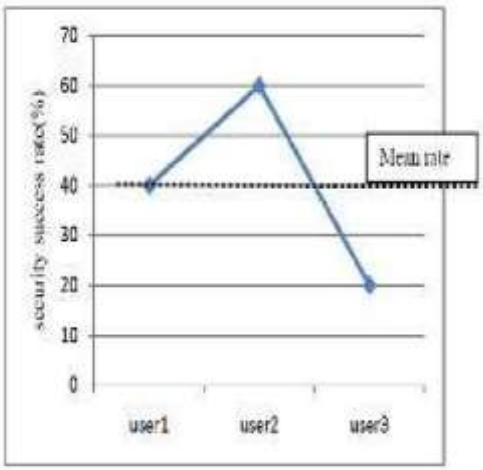


Fig. 12 PCCP mean rate

Higher scores usually imply more favourable findings for PCCP in Table III because the scores were reversed before computing the means and medians during the question-and-answer round with 20 respondents.

Table III Questionnaire responses. Scores are out of 10

Query	View point 100*100	View point 75*75	View point 50*50
I could easily create a graphical Password	8	8	7.5
Logging on using a graphical password was easy	6.4	7	8.3
Graphical passwords are easy to Remember	6	5.7	5
I prefer text passwords to graphical Passwords	4.9	5	5.2
Text passwords are more secure than graphical passwords	6	6.2	6.5
I think that other people would choose different points than me for a graphical password	7.2	7	8
With practice, I could quickly enter my graphical password	8.3	8	7.2

8. CONCLUSION

One of the primary goals of authentication systems is to aid users in choosing strong passwords and expanding the available password field. If the user interface is improved, users will be more likely to use secure passwords. Example: creating a prototype and testing the usability of a persuasion technique called persuasion-cued click-points (PCCP). Research to determine how well it works here, we found success from a safety and efficacy standpoint, as well as two others. The PCCP steers users toward the more secure and unpredictable graphical passwords that are selected with a click of the mouse. PCCP's "path-of-high-resistance" approach to password creation makes it more successful than systems that make following security protocols more of a hassle for users. This method successfully mitigates the emergence of hotspots, steers clear of the security vulnerability known as "shoulder surfing," and offers a high level of protection without sacrificing usability.

REFRENCES

[1] S.B.Sahu, A. Singh "Survey on Various Techniques of User Authentication and Graphical Password," published in International Journal of Computer Trends and Technology (IJCTT), vol.16, pp 98-102, no.3, Oct. 2014.

[2] S. Chanson, A. Forget, O. Biddle, P.C. van Borscht "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," published in IEEE transactions on dependable and secure computing, vol. 9, no. 2, pp.222-235, Apr. 2012.

[3] S. Chanson, A. Forget, O. Biddle, P.C. van Borscht "Influencing Users Towards Better Passwords: Persuasive Cued Click-Points," Published in Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, vol.1, sep. 2008, pp.121-130.

[4] S.B.Sahu, A. Singh "Secure User Authentication & Graphical Password using Cued Click-Points," published in International Journal of Computer Trends and Technology (IJCTT), vol.18, no.4, pp.156-160, Dec. 2014.

[5] Usher T, Tara H R, G I Shidaganti "Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points," published in International Journal of Engineering Research & Technology (IJERT), vol. 2, no 6, pp.258-266, Jun. 2013.

[6] A. Cummings 2012, Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector [online], Available: http://www.sei.cmu.edu/reports/12sr004.pdf

[7] G. Niranjana, K. Dawn "Graphical Authentication using Region based Graphical password," published in International Journal of Computer Science and Informatics ISSN, vol.2, no.3, pp.114-119, feb.2012.

[8] G. Niranjana, K. Dawn "A Novel Gesture Based Graphical Authentication Using Bounding Box and Corner Detection Algorithm," published in International Journal of Computer Science and Informatics ISSN, vol.12, no.3, pp.114-119, Nov. 2012.

[9] U. D. Yadav, P. S. Mood "Adding Persuasive features in Graphical Password to increase the capacity of KBAM," Published in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, vol.2, Mar.2013, pp.513-517.

[10] S. Chanson, A. Forget, O. Biddle, P.C. van Borscht "Improving Text Passwords through Persuasion," Published in Symposium on Usable Privacy and Security (SOUPS), vol. 4, pp.1-12, Jul. 2008.

[11] Wei-Chi Ku, Dum-Min Liao, Chia-Ju Chang, Pei-Jia Qiu "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme," Published in Symposium on Privacy and Security in Commutations, vol.4, pp.204-208, Oct.2014.

[12] S. Chiasson, C. Decamps, E. Sober, M. Flyway, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, " The MVP Web-Based Authentication Framework," Published in Proc. Financial Cryptography and Data Security (FC), LNCS, vol.7397, pp 16-24, Mar.2012.