ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Defending Online Password Hunch Attacks Using Persuasive Cued Click Points

D.Lavanya*, Bethini Saiteja, S. Bala Moulika, P.Rakesh Reddy
*B.TECH- IVth YEAR ,ECE , Vidya Jyothi Institute of Technology, Hyderabad, India
B.TECH- III rd YEAR ,ECE , Vidya Jyothi Institute of Technology, Hyderabad, India
B.TECH- III rd YEAR ,ECE , Vidya Jyothi Institute of Technology, Hyderabad. India
B.TECH- III rd YEAR ,ECE , Vidya Jyothi Institute of Technology, Hyderabad, India

Abstract

Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. Therefore, this project work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points. To address the issue of hotspots, Persuasive Cued Click Points (PCCP) was proposed. As with CCP, 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 view port moves to the specific location

Keywords: pp, pccp, ccp, Human brain, Graphical passwords.

Introduction

Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character.

Objective

There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. Therefore, this project work merges persuasive cued click points and password guessing resistant protocol. The major objective of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

Existing System*:* Existing approaches to users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

difficult for users to remember. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. 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.

Proposed System: The proposed system is provide a PKI based remote authentication scheme by this server usually stores either copies of the certificates or corresponding hash values that it can authenticate.

Modules

- Pass Points Module.
- Cued Click Points Module.
- Persuasive Cued Click- Points Module.

Pass points module

Based on Blonder's original idea, Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

Cued click points module

Cued Click Points (CCP) was developed as an alternative click based graphical password scheme where users select one point per image for five images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

Persuasive cued click- points module:

To address the issue of hotspots, Persuasive Cued Click Points (PCCP) was proposed. As with CCP, 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 view port moves to the specific location, but this is a time consuming and more tedious process.

System requirements specifications

After analyzing the requirements of the task to be performed, the next step is to analyze the problem and understand its context. The first activity in the phase is studying the existing system and other is to understand the requirements and domain of the new system. Both the activities are equally important, but the first activity serves as a basis of giving the functional specifications and then successful design of the proposed system. Understanding the properties and requirements of a new system is more difficult and requires creative thinking and understanding of existing running system is also difficult, improper understanding of present system can lead diversion from solution.

Analysis Of Thegraphical Password System

SDLC Methdologies:

This document play a vital role in the development of life cycle (SDLC) as it describes the complete requirement of the system. It means for use by developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.SPIRAL MODEL was defined by Barry Boehm in his 1988 article, "A spiral Model of Software Development and Enhancement. This model was not the first model to discuss iterative development, but it was the first model to explain why the iteration models.As originally envisioned, the iterations were typically 6 months to 2 years long. Each phase starts with a design goal and ends with a client reviewing the progress thus far. Analysis and engineering efforts are applied at each phase of the project, with an eye toward the end goal of the project.

The steps for Spiral Model can be generalized as follows:

- The new system requirements are defined in as much details as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

- A preliminary design is created for the new system.
- A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
- A second prototype is evolved by a fourfold procedure:
    1. Evaluating the first prototype in terms of its strengths, weakness, and risks.
    2. Defining the requirements of the second prototype.
    3. Planning an designing the second prototype.
    4. Constructing and testing the second prototype.
- At the customer option, the entire project can be aborted if the risk is deemed too great. Risk factors might involved development cost overruns, operating-cost miscalculation, or any other factor that could, in the customer's judgment, result in a less-than-satisfactory final product.
- The existing prototype is evaluated in the same manner as was the previous prototype, and if necessary, another prototype is developed from it according to the fourfold procedure outlined above.
- The preceding steps are iterated until the customer is satisfied that the refined prototype represents the final product desired.
- The final system is constructed, based on the refined prototype.
- The final system is thoroughly evaluated and tested. Routine maintenance is carried on a continuing basis to prevent large scale failures and to minimize down time.

Input and output design of the project

Input design

Since the project is a click based system, the input to be given is click points. The image is divided in to pixels. The pixel values of the click points are stored in the database.

The project includes three modules.

- **Pass points module:** Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image. To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.
- **Cued click points module:** It is an alternative click based graphical password scheme where users select one point per image for five images. The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image.
- **Persuasive cued click points:** In this module 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.

Help button is provided for the user to know about each module so that the user can choose the specific module as per the level of security.

Output design:

- Output of the project involves validating the click points.
- On successful login, it directs the user to the home page for files sharing.
- If login fails, it leads to infinite clicks and misguides the attacker.

Minimum software and hardware requirements

Software:

Technologies	: ASP .Net and C#.net
Database	: MS-SQL Server 2005/2008
IDE	: Ms-Visual Studio .Net 2010

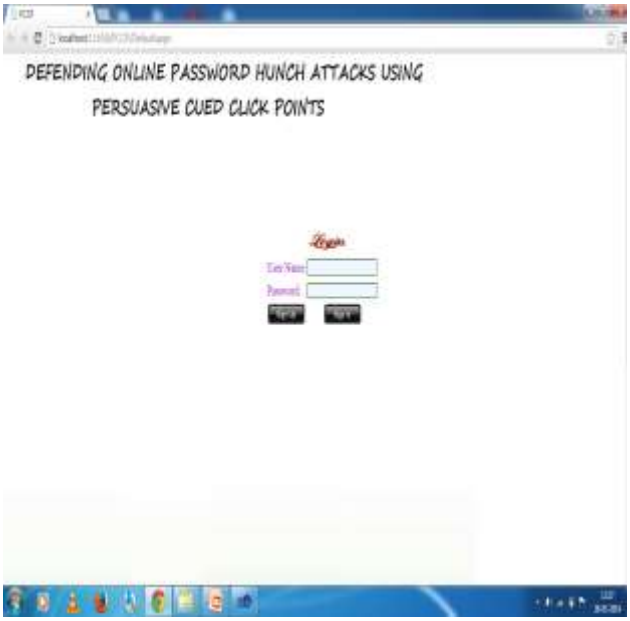
Hardware:

Processor	: Pentium IV
RAM	: 512 MB
Hard Disk	: 40 GB

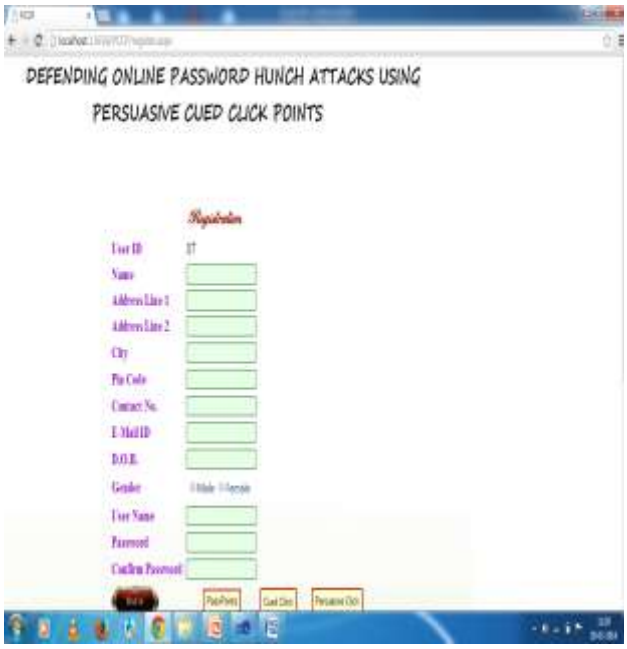
Screen shots

HOME:

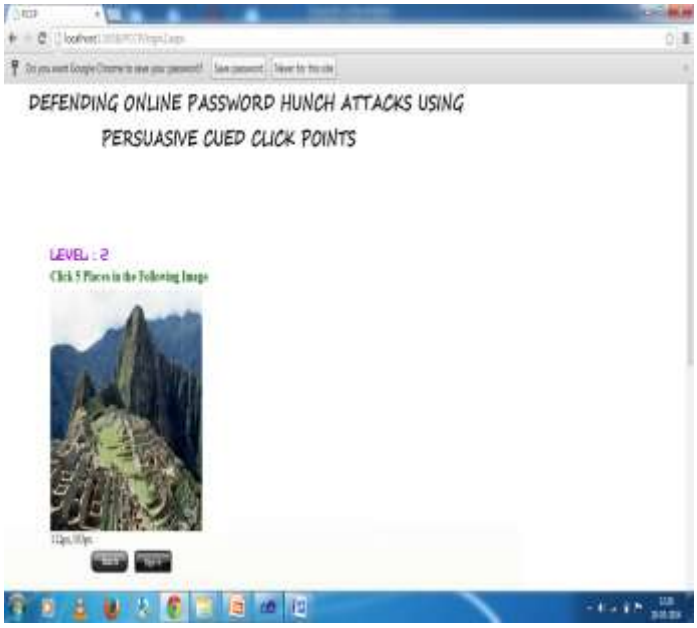
ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114



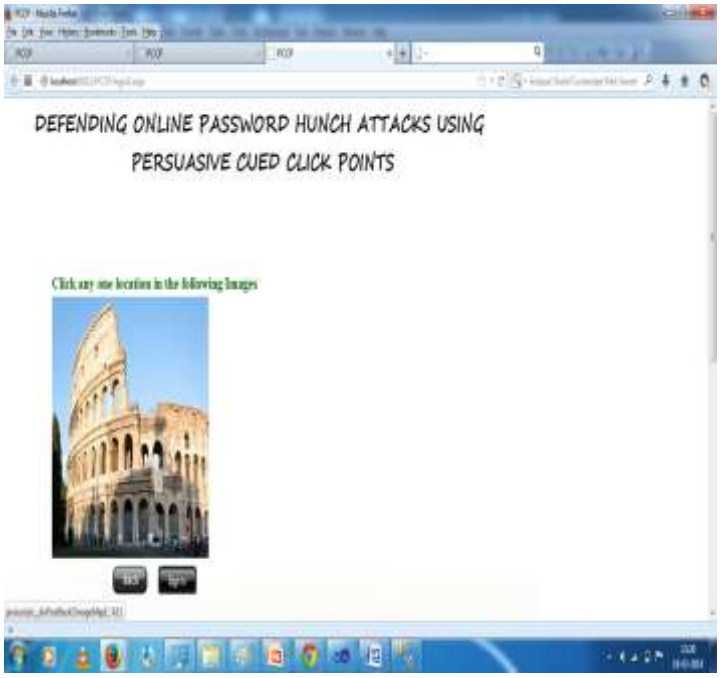
Registration:



PASS Points:

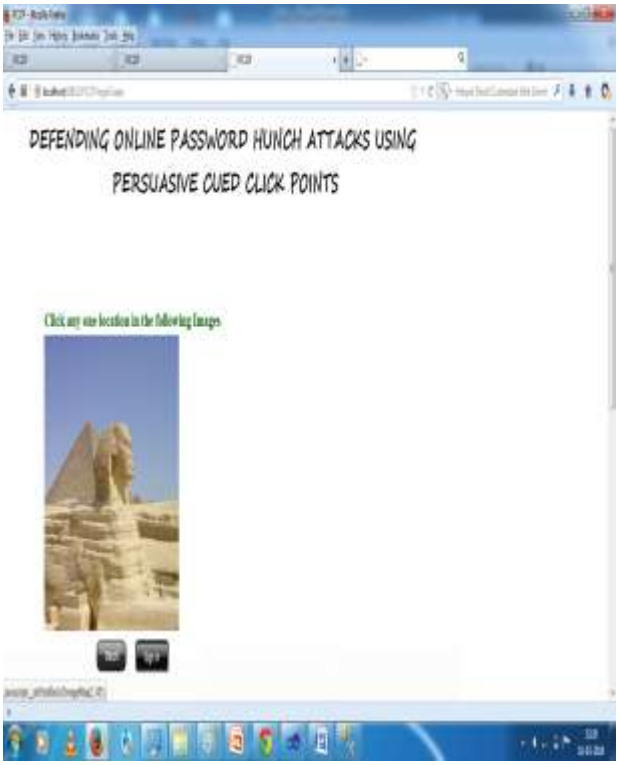


CUED click points (PAGE 1):

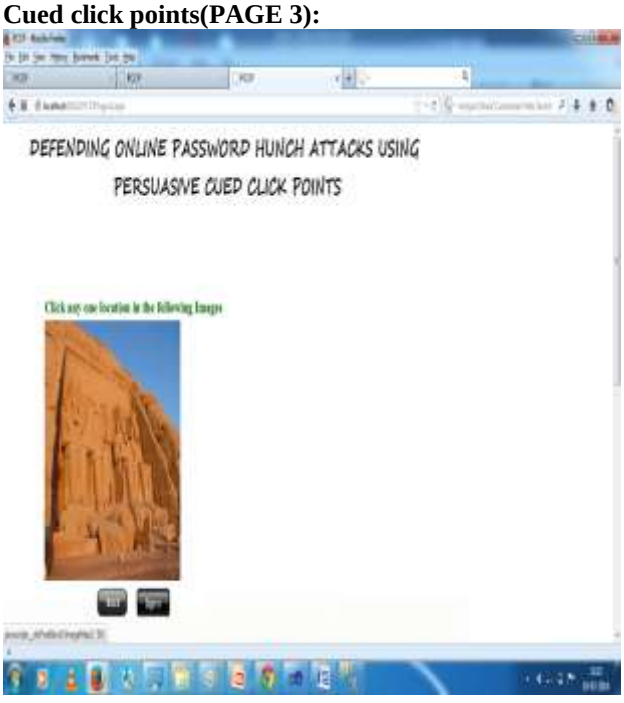


ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

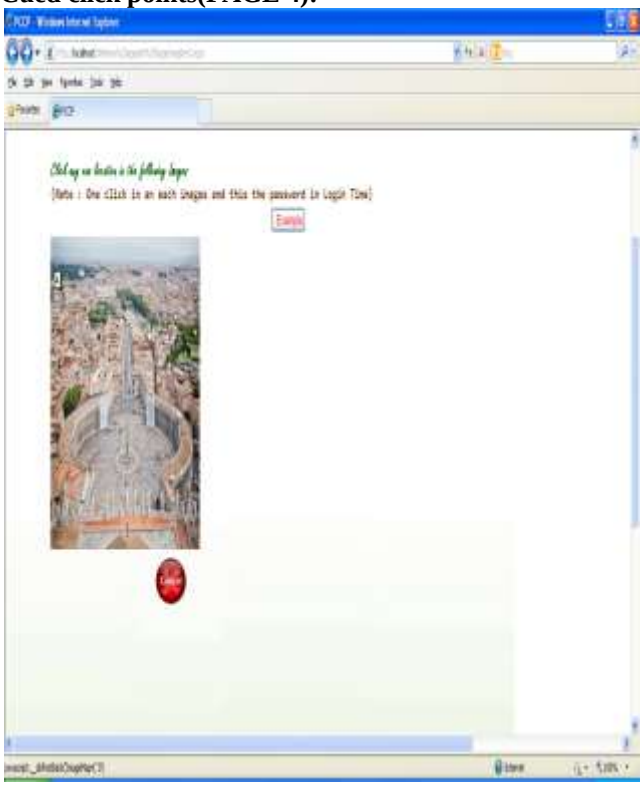
Cued click points(PAGE 2):



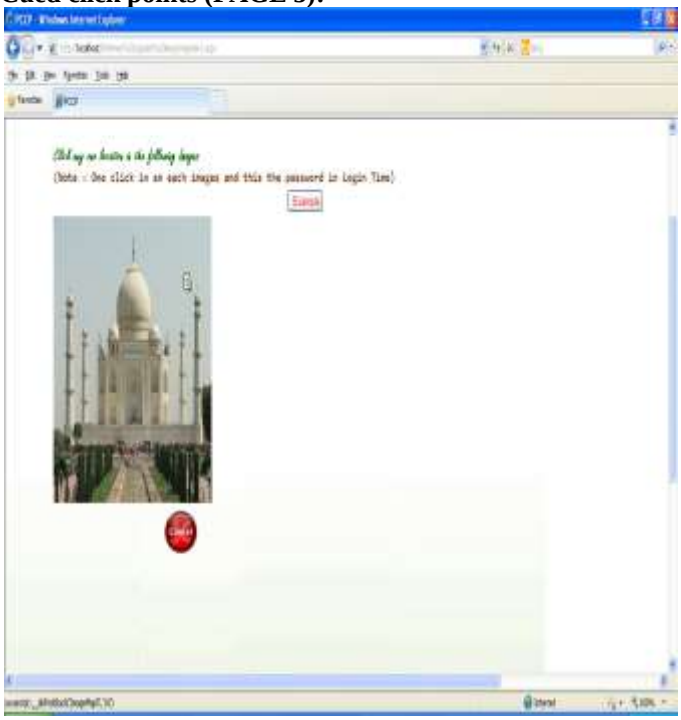
Cued click points(PAGE 3):



Cued click points(PAGE 4):

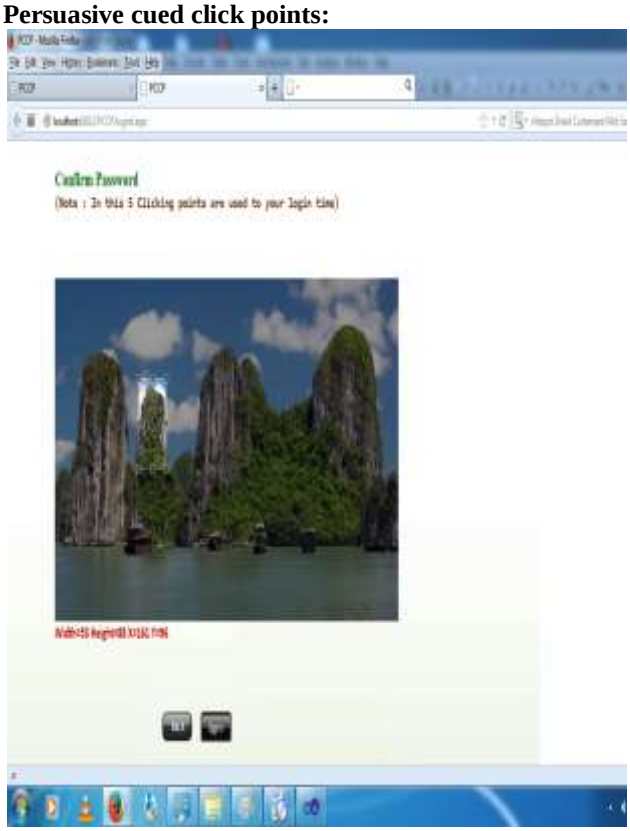


Cued click points (PAGE 5):



ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Persuasive cued click points:



Test cases

Test cases for login page:

Controls	Test Cases	Result
Label	Displaying	Yes
Edit text (Username)	Allowing to enter the username	Yes
Edit text (Password)	Displaying asterisk	Yes
Signup Button	On click redirecting to registration page	Yes
Sign in Button	On click redirecting to next page	Yes

Test cases for registration page:

Controls	Test Cases	Result
Label	Displaying	Yes
User id	Displaying the user id number	Yes
Edit text(Address Line 1)	Allowing to enter the address	Yes
Edit text(Address Line 2)	Allowing to enter the address	Yes
Edit text(city)	Allolwing to enter the city	Yes
Edit text(pin code)	Allowing to enter pincode	Yes
Edit text(contact no)	Allowing to enter number	Yes
Edit text(email id)	Allowing to enter email id	Yes
Edit text(D.O.B)	Allowing to enter the date of birth	Yes
Radio Button(gender)	Allowing to select the gender	Yes
Edit text(Username)	Allowing to enter the username	Yes
Edit text(Password)	Allowing to enter the Password	Yes
Edit text(Confirm Password)	Allowing to confirm the password	Yes
Button(Back)	Redirecting to the previous page	Yes
Button(Pass Points)	Redirecting to the Pass Points page	Yes
Button(CCP)	Redirecting to the CCP page	Yes
Button(PCCP)	Redirecting to the PCCP page	Yes

Test cases for pass points page:

Controls	Test Cases	Result
Label	Displaying	Yes
Button(Back)	Redirecting to the previous page	Yes
Button(next)	Redirecting to the home page	Yes

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Test cases for cued click points page:

Controls	Test Cases	Result
Label	Displaying	Yes
Button(Back)	Redirecting to the previous page	Yes
Button(next)	Redirecting to the home page	Yes

Test cases for pccp page:

Controls	Test Cases	Result
Label	Displaying	Yes
Button(Back)	Redirecting to the previous page	Yes
Button(submit now)	Redirecting to the home page	Yes

Test cases for home page:

Controls	Test Cases	Result
Label	Displaying	Yes
Button(update)	Redirecting to the registration page to update user profile	Yes
Button(upload)	Allowing the user to upload files	Yes
Button(logout)	Redirecting the user to go to Login page	Yes

Future scope

In future it has great scope. User authentication is necessary for providing and verifying the claimed identity of users in a distributed environment. Three factors such as user's knowledge, belongings and biometric traits are usually considered for the purpose. A sort of multi factor authentication may combine those factors the way that a user provides the requested multi factors separately, for improving the accuracy and security of authentication. However, such a combination of distinct factors require each different human-computer interfaces. Rather we introduce our on-going work to associate knowledge-based authentication with biometrics for requiring less interfaces and examine the benefits expected from it in a conceptual level. we can also allow the user to draw the images or symbols on the virtual screen and can use those images as passwords. We can also provide locking of the account for certain period of time if login fails.

Conclusion

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets.

References

1. International Journal of Communications and Engineering ,Volume 03– No.3, Issue: 01 March2012
2. User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
3. Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.
4. Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.
5. Data Communications and Networking, by Behrouz A Forouzan.
6. Computer Networking: A Top-Down Approach, by James F. Kurose.
7. Operating System Concepts, by Abraham Silberschatz.
8. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
9. The apache Cassandra project," http://cassandra.apache.org/.
10. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
11. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficientand differentiated data availability guarantees in data clouds,"in Proc. of the ICDE, Long Beach, CA, USA, 2010.
12. O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems,vol. 28, no. 1-2, pp. 177 – 189, 2000.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

13. A. Helsinger and T. Wright, "Cougaar: A robust configurablemulti agent platform," in Proc. of the IEEE Aerospace Conference,2005.
14. J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes,M. Seltzer, J. Shank, and S. Youssef, "Egg: an extensible andeconomics-inspired open grid computing platform," in Proc. of the GECON, Singapore, May 2006.
15. J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeatingspikes with a free-market application cluster," in Proc.of the International Conference on Autonomic Computing,New York, NY, USA, May 2004