ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

# A New Authentication Mechanism Based on Graphical Password

**V Ramesh**
M.Tech (CSE),
Department of Computer Science & Engineering,
Nagole Institute of Technology & Science, Hyderabad.

**Dr. P. Venkateswarlu**
Professor & HOD,
Department of Computer Science & Engineering,
Nagole Institute of Technology & Science, Hyderabad.

**S. Sree Hari Raju**
Assistant Professor,
Department of Computer Science & Engineering,
Nagole Institute of Technology & Science, Hyderabad.

## Abstract:

Security is playing vital role in the field of web applications and online transactions. Especially in the banking and financial transactions the security methods are highly solicited. The hackers are guessing the passwords. They are fixing the passwords and breaking the financial transactions of others.  Password authentication is very important and it should be used with high definition. The main destiny of authentication systems should support the users in selecting the tough passwords and prevent the hackers to guess the same. The persuasive click points will be remarkably remembered by the user and can not be guessed by the hackers. The persuasive click points on the image passwords will prevent the guessing attacks for online financial transactions and applications. The research goal is to prevent the guessing attacks on the online applications by incorporating the persuasive click points on the graphical passwords with the identification points in terms of X and Y axis. This method is going to give tough fight for the Brute Force Attacks and Dictionary attacks commonly seen in online applications. The test results of the application has revealed the facts that the present application can successfully incorporated a high security passwords which can't be broken by any hacker.

## Keywords:

password security, password authentication, Image passwords, persuasive click points .

## Introduction:

For password securities and recovery operations the standard human-computer-interaction are normally used. The predominant goal for user authentication mechanism is to provide the support for the users to select the most suitable passwords. The attackers will predict the passwords according to the environment, date of birth, name and other environmental situations. A strong mechanism is essentially needed to admeasure the guessing attacks to the online applications. To avoid this practice and to suggest a strong system of assigning the passwords for the application security a graphical picture assignment is suggested. In this graphical password authentication system, images or replications and representations of images are used as passwords.

The images can be taken from the folder or download from internet and stores in the database. The persuasive click points are counted with the help of X-axis and Y-axis points. It is suggested just because of the nature of the human brain which remember the pictures more impressively rather than the textual passwords. Some of the banks have started the secured user authentication when the user is accessing the online banking accounts with the combination of graphical password selected from the  list with the combination of Customer ID and password.

## The project deliverables:

1.To create a web application rich with image password and persuasive click points authentication with at least two images. .

2.To create a web application to demonstrate the persuasive click points on graphical Images in terms of X-Axis and Y-Axis to denote the user authentication points.

3.To produce a web application to store the details of the  user along with  the username and password in combination of persuasive click points.

4.To implement a mechanism to reduce the guessing attacks of outsiders who can login to the system with the text passwords.

5.To implement an application design to provide different images as user identification passwords as well as high complexity with the persuasive cued click points.

## Project Contribution:

The present dissertation report is on A New Authentication Mechanism Based on Graphical Password. The project is a novel piece of work in the filed of online application security and system security. The project is defining the new way of defining the passwords to operate an online application. The project is going to give a novel methodology for implementing new password system to online users. By using this novel concept of using graphical passwords with persuasive cued click points the passwords will be preserved with great privacy and can't be guessed by any attacker of online application. The project will be contributing well to the field of security authentication and application security. The project method is novel and paved the way to restrict the guessing attacks, Brute Force Attacks and Dictionary attacks.

## Authentication Methods:

Authentication is a process, to distinguish the identity of the user to access the specific application. This identification process can be incorporated with the user name and password storage and verification methods. The attackers guess the password according to the name, environment, working culture, qualification and other standard memorable events of the person. The human brain generally remember the events and objects which are mostly acquainted to the person. This phenomena can be adopted by the hackers and apply guessing attacks, Brute Force Attacks and Dictionary attacks. To come out of these attacks the research studies have revealed many authentication methods. These are regarded as token based authentication, Biometric Based Authentication, Knowledge Based Authentication, Image Based Authentication, Cued Recall Based Technique, pass points based authentication and Cued Click Points based authentication. In this Persuasive Technology has given a way to keep the passwords unpredectively without guessing by any hacker.

In this technology an advancement has been generated in the form of Persuasive Cued Click Points. This technology has removed the fears from guessing attacks. This mechanism will set the password of the user with high security and privacy with the help of image cued click points position viewport.'Gloriya Mathew [2013]3'

## Image Password Authentication:

Image password authentication system is a latest mechanism frequently used in online financial transactions. Graphical password authentication is regarded as an alternative mechanism for textual passwords. It is also very simple for user to remember rather than the textual passwords. The present paper is illustrating the combine mechanism for more authentication with the graphical passwords as well as the mouse points on an image. This type of method will be called as the mouse gestures. The alternative mechanism for textual passwords has been successfully implemented to arrest the guessing attacks on online applications. The textual passwords can be cracked by the intruders and eavesdroppers. The graphical passwords with persuasive cued click points are easy to remember for online users and difficult to crack the passwords for online intruders. This graphical password is providing increasing security to the online applications. G.ManiMayuri, et.al [2013]

## Persuasive Cued Click Points:

Knowledge-based authentication is well identified as text based passwords. The knowledge-based authentication demands to use memorable passwords. User always choose the memorable passwords from the nearest circumstances or components from birth dates, years, memorable events or persons. This phenomenal tendency is the loophole for the attackers to guess the passwords of the person.At this juncture the graphical password authentication system is introduced along with the persuasive cued click points. In this method the user should select an image and select the part of the image for click points. In this method if the user selects the more attractive spot of the image, the attacker could easily identify the password and leads to successful dictionary attacks. The persuasion is imposed to the user in selecting click based graphical passwords with unpredictable choice with more random points.

This persuasive cued click points mechanism has created more confusion and difficulty to the attackers. The poor choice of click points sometimes leads to dictionary attacks. Persuasive Technology is incorporated by Fogg.

This has been introduced to motivate and encourage the users to behave in a desired manner. The persuasive technology probes the user to remember persuasive elements of the image with path-of-least resistance. The click points are regarded as hot spots. The more hot spots on image in a cued manner creates m -Iranna A Met.al.,[2013]

## The need of the project:

Guessing attacks have stirred online financial applications of the world. All B2B business application have windup and close down their operations because of online attacks and intruders. The applications data has been looted by the intruders and hackers. The quest of solution has begun.

## First Solution:

After long explorations and innovative research works the online application are provided with the encrypted passwords. The encrypted mechanism has given tight security to the applications. The tight security has been broken by the hackers. As and when the security is broken the new security digital encryption standards have been generated and invented. The advanced digital encryption standards have been incorporated but all these innovative experiments have been dominated by the intruders.

## Second Stage solutions:

The greatest quest has begun for alternative arrangement against the guessing attacks on online applications. The guessing attacks have become unstoppable by the online applications. At this point of time in the place of textual passwords the image passwords have been introduced by the wisest computer specialist of 21st century. The user has to select a specific image as the password for his application login. This mechanism has given good solution for guessing attacks. But these solution has also digested by the attackers and started the guessing the user selected images.

## The third stage and previous approach:

The previous approach has given by the research scholars has remarkably addressed the guessing attacks problems. The guessing attacks have been reduced with the advent of click points on image. The predominant work done by the scientist has paved the way with storing the click point with x axis and y axis points of the image in the database.

This mechanism verified the click points of every time login to the application and allowed the user to access the application. This is also has flaws that the user may select the most attractive points of the image. The predominant and attractive points are sometimes guessed by the attacker and broken the security. This flaw has to be addressed and the lowest percentage of application breakage should be avoided.

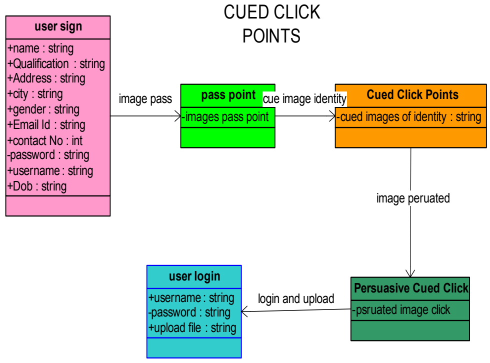
## The present application – Persuasive Cued Clicks:

The innovative solution has been introduced in this application with persuasive cued clicks on the image. The persuasive cued clicks mechanism will avoid the user to select un important points of the image. The persuasive mechanism will direct the user to select very casual and normal image from the pool of images. The selection should be normal and not attractive for image and cued clicks on the image. The click will be stored in the database in a sequential format, which is called as cued clicks. The sequential order should be recorded in the application database. Whenever the user wants to access the application the cued clicks should be verified.

The clued click points should be tallied with the previous one. If the user forgets the cued clicks the application should allow the user to receive onetime password to his mobile or email to enable the user to reset the cued click points. This application is going to address the present guessing attacks with great deal. The persuasive mechanism will guide the user not to select the predominant points of the image and not to select the predominant images from the image pool. The persuasive mechanism helps the user to select the images as well as the cued click points in random and unimportant way. The persuasive cued click points can't be broken by any hacker or intruder with guessing attacks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

Class diagram
FOR
PERSUASIVE
CUED CLICK
POINTS



The internal deliverables of the project depicts the internal mechanism developed with required technologies. The present application is a web based application.

The internal mechanism, stored procedures, n tire architecture has been developed using ADO.Net and C#.Net technologies.

The project is rich with persuasive cued click points on a user selected image. This persuasive cued clicks operation should be recorded in the user interface screens. The internal mechanism will be written in the components available in the user interface screens.

## Functionality of the project:

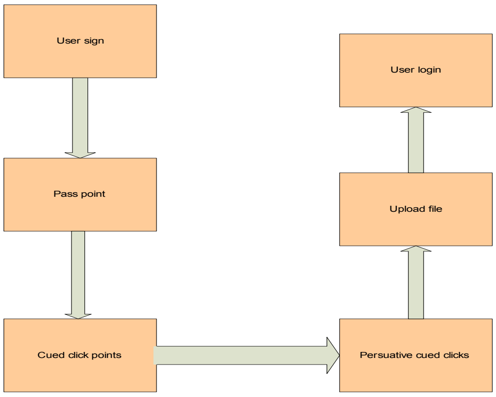
The project is designed to demonstrate the highest grade of security provision for online applications. The security is given against the guessing attacks.

This has been incorporated with the persuasive cued click points on an image selected by the user along with the user name and password.

The present project security mechanism is combined with textual passwords along with the image passwords with persuasive cued click points. The project is an online application with security mechanism to protect the application from guessing attacks.

The project is predominantly highlighting the security mechanism with image passwords, textual passwords and persuasive cued click points.

Data flow diagram



## Critical Evaluation:

Guessing attacks predominantly affected the business of B2B. The financial transactions of the banks should be kept online. So that the business of the banks will get improved. To keep the financial transactions a strong online security mechanism should be developed. The need of a security mechanism for financial transactions conducted by the financial institutions is very high. The security mechanism should act against the guessing attacks. Guessing attacks are more powerful and breaking the passwords of the online financial transactions and stealing the data. The present proposed project is development of a security mechanism against the guessing attacks. The proposed project is also creating a security layer for the financial transactions and obstructs the intruders into the financial online applications.

The research studies revealed that the investigations have done and found a admeasure with the password security. The mechanism has run for a period until the hackers started to break these passwords with their creative mechanism. Then the researchers have developed the advanced encryption standards against the hackers' attacks. Those increased security mechanism have not endure much time in protecting the web applications.

## CONCLUSION:

The revolutionary experimental research work has been done in incorporating the security with encrypted mechanism. The revolutionary changes and innovative changes have been done in deploying advanced digital encryption standards.

The digital encryption standards have been deployed to hide the real password of the user and tried to protect the interest of online financial application users. All the trails have become in vain. Even digital encrypted textual passwords also decrypted with the wise characteristics of hackers and intruders. The hackers again started looting the valuable data of the financial organizations. The hackers and attackers have adopted sophisticated cracking techniques for textual passwords and intrude into the applications and caused irrevocable damage to the application storing data.

The scientists and computer experts have started investigating the remedy for strengthen the situation. The several research factors have supported different solutions. All these solutions have become small before the wisest mentality of the hackers and attackers techniques.

The guessing attacks have stirred the online applications and financial mechanism of the bankers. The new tools and techniques have been applied to generate a new system. The final search has given the solution in the form of image password implementation in the place of textual passwords.

## References:

### Books:

9.1.1. Persuasive Advertising - Author : J.Scott Armstrong

9.1.2. Picture password authentication using cued click points - Author : Harikrishnan Nair

9.1.3. Graphical User Authentication (GUA): Graphical Password Algorithms and Analysis Published in – December 3, 2010 by ArashHabibiLashkari (Author) , FarnazTowhidi (Author)

9.1.4. A Calculus to Detect Guessing Attacks by BogdanGroza, Marius Minea Published in 2009.

### Articles:

S Chiasson - 2012 - Cited by 29 - Related articles on Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication May 10, 2012 - home • articles ... Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism ... users to select more random, and hence more difficult to guess, click-points.

essays, articles and other content including Persuasive Cued Click-Points: ... Posts from DIGG that contains the high definition-digital video disc

### Previous Research Published Papers:

1.Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE [2011] Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism downloaded from http://hotsoft.carleton.ca /~sonia/content/ Chiasson_tdsc_pccp_author_copy.pdf

2.D.AnuRadha [2013] A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks Published by: PIONEER RESEARCH & DEVELOPMENT GROUP(www.prdg.org) IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791

3.Gloriya Mathew, Shiney Thomas [2013] "A Novel Multifactor Authentication System Ensuring Usability And Security" - Published In Computer Science Journal

4.Chippy.T and R.Nagendran [2012] DEFENSES AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS BY USING PERSUASIVE CLICK POINTS published in International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012

5.Ms. Resmipriya M G Ms. Sangeetha N [2013] "An Efficient Approach for Preventing Online Password Guessing Attacks" International Journal of Computer Science and Management Research Vol 2 Issue 3 March 2013.

6.Seth Thigpen [2005]Authentication Methods Used for Banking Published in East Carolina University articles

7.DharmendraChoukseUmesh Kumar Singh Deepak SukhejaRekhaShahapurkar [2010] Implementing

New-age Authentication Techniques using OpenID for Security Automation International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010

8.Hafiz ZahidUllah Khan [2010] Comparative Study of Authentication Techniques International Journal of Video& Image Processing and Network Security IJVIPNS-IJENS Vol:10 No:04 9 103304-2929 IJVIPNS-IJENS © August 2010 IJENS I J E N S

9.G.ManiMayuri, S.Vineela Krishna, M.Tech[2013] Graphical based Secure Authentication System for Online Applications published in International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 8–August 2013

10.Wayne Jansen,SerbanGavrila, VladKorolev, Rick Ayers, Ryan Swanstrom [2003]Picture Password: A Visual Login Technique for Mobile Devices published at Information Technology Laboratory, National Institute of Standards and Technology

11.Serena [2007] An IntroductIon to AgIle Software development.

12.Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. van Oorschot [2012]Persuasive Cued Click-Points:Design, implementation, and evaluation of a knowledge-based authentication mechanism.

13.Iranna A M1,PankajaPatil [2013] Graphical Password Authentication Using Persuasive Cued Click Point. Published in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.

14.Kailas I Patil, JaiprakashShimpi [2013] A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devicespublished in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013 155.

15.Head of W3C Greece Office, Associate Researcher, Institute of Computer Science-FORTH

16.Glenford J. Myers (2013)The Art of Software Testing, Second Edition Revised and Updated by Tom Badgett and Todd M. Thomas with Corey Sandler