# Graphical Password Authentication System

**Mr.Jadhav Rajesh S.** **Mr.Chandole Durgesh K.**
**Mr.Wani Milind D.** **Mr.Kusalkar Santosh R.**
**Mr.Shinde Kiran G.** **Mr.Dighe Mohit S.**
**Shri Chhatrapati Shivaji College of Engineering,Rahuri-Factory**

***Abstract*- Naturally for human mind it is hard to remember text based password. Text based passwords are easy to guess because the use of general set of numbers, character and special symbol, for that purpose we implemented the Graphical Password Authentication System. In that we had used Image based & Pair based authentication system. Firstly in Imaged based password user can choose pixels on that image as password. For each image only one pixel is selected. After selection one pixel change the image select second pixel from second image similarly users select three pixels.**

**In pair based password, user chooses characters from columns and rows simultaneously from the grid then getting that intersection point as a password. We have provided shuffling option for interchanging character sequence it helps to prevent the shoulder suffering attack. So we have improved security by using PCCP and Imaged based password system which having ability of protect from the attacker, crackers etc.**

**Index Terms—authentication, graphical passwords, session passwords, usable security, studies.**

## I. INTRODUCTION

The most common and popular method used for authentication is text password. The vulnerabilities of this method such eves dropping, dictionary attack, shoulder surfing, and burst force attacks are well known. Random and long text passwords can make the system secure. But the main problem is the hardly to remember those passwords. Studies have shown that users enter to small or short passwords or passwords that are easy to remember. But, these passwords can be easily guessed or cracked by attacker. The alternative techniques are graphical passwords. There are many graphical password schemes that are proposed in the few last year. But most of them suffer from shoulder surfing problem which is become quite a major problem. There are graphical passwords schemes that have been proposed which are prevent to shoulder-surfing but they have their own limitations like usability problem issue or taking more time for user to login or having long procedure levels.

## II. BACKGROUND

Text passwords are the most popular user authentication method in today, but have security and user friendly problems. Graphical passwords offer another alternative, and are the focus of this paper. Graphical password systems are a type of Image-based authentication that attempt to understand the human memory for visual information. A comprehensive review In Pass Points, passwords consist of sequence pixel click-points on a given image. Users may choose one pixels in that image as click-points for their password. To log in process, they repeat the sequence of clicks in the same order,

I. PERSUASIVE CUED CLICK POINTS (PCCP)

In persuasive cued click point algorithm, image divided in small grid or small parts of view, after that user choose any one grid of that image, then choosing one pixel on that selected grid and those chooses pixel set as password.

During user name creation, the most of the image is fragmented in a small view grid area that is randomly positioned on the image as shown in Figure. Users must choose it's own a click-point within the view grid. If they are choose wrong pixel or to choose a wrong point in the current view grid, they may click on move button to randomly reposition the view grid.

This procedure repeated in three times that is three different images user is choose. After one pixel choosed then next image is come and choose second pixel and similarly choose third pixel on next image. If user chooses wrong pixel then system manipulate to user i.e. wrong image is come and user doesn't authenticate in system.

The view grid'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 choose a click-point within this highlighted view grid area and cannot click outside of the view grid area, unless they click on move button to randomly reposition the view grid area. While users may move as often as desired, this significantly slows password creation. The view grid and move button appear only during password creation. During later password entry, the images are displayed normally, without shading or the view grid, and users may click anywhere on the images.

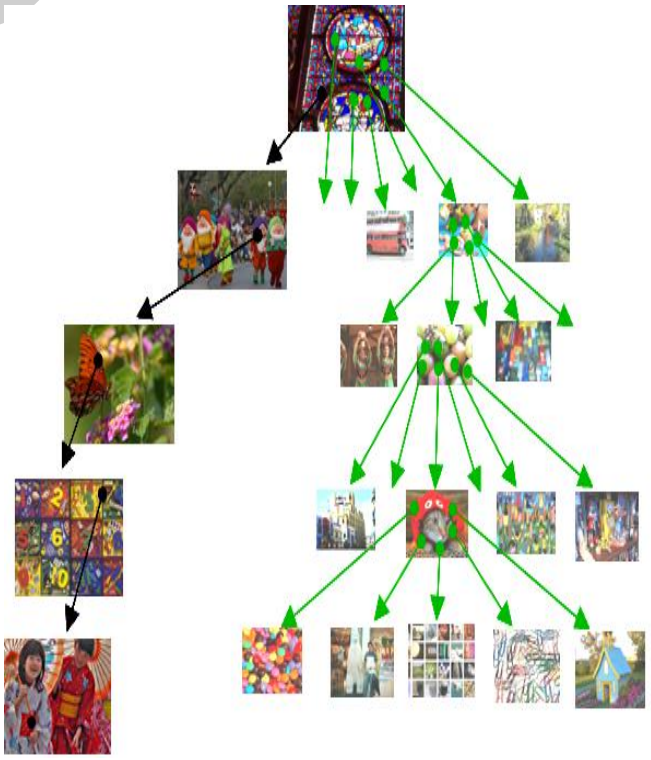


Fig.1: Persuasive Cued Click-Points

Algorithm Step:

1.User Registration: User chooses user name and set of image pixels as password for first time.
2.Login: At the time of login user enters same user name and pixel images as password which was stored in database at time of registration to get log-in.
3.Verification: After submitting set of image pixels choosed they are matched with database for checking whether they are valid or not.
4.Confirmation:After verification is done on the basis of that it is confirmed whether to give access to user or not

.

## II. PAIR-BASED PASSWORD

At the time of registration, user needs to enter user name and secret pass. When user enters a user name grid consist of set of character get grid displayed. User has to choose secret pairs of characters, in this pair first character belongs to column and second character belongs to row.

After on completion of registration data is store in database. At the time of login user needs to follow same procedure as like registration phase. Password should be consisting of minimum five characters. At the login time when user enter password and submit it goes to verification phase in which enter password is match with password entered at registration phase which is stored in database.

We can use pair based password in web login application, ATM Machine, banking application, mobiles and many more.

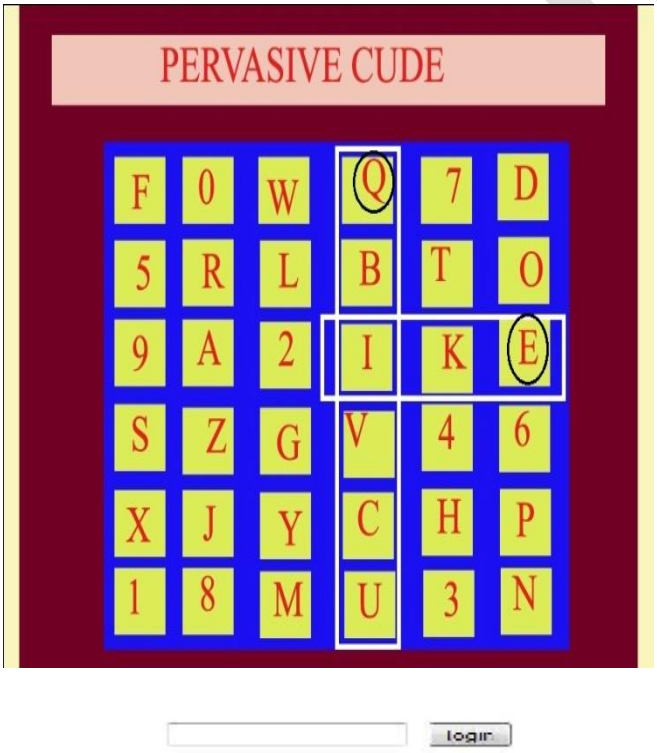
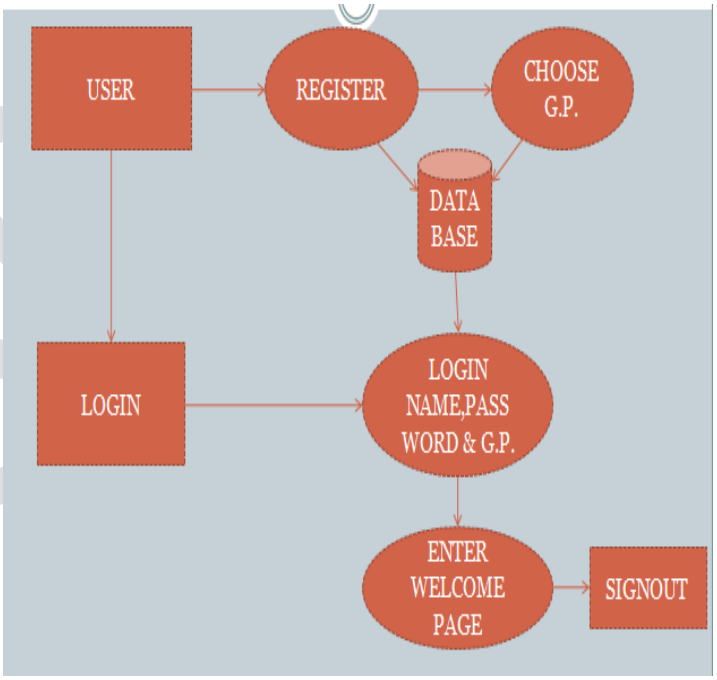



Fig.2 : Pair-based Login Screen for user name QE

Algorithm Step:

1.User Registration: User chooses user name and pair of letters as password for first time.
2.Login: At the time of login user enters same user name and letters pair as password which was stored in database at time of registration to get log-in.
3.Verification: After submitting pairs of letters choosed they are matched with database for checking whether they are valid or not.
4.Confirmation:After verification is done on the basis of that it is confirmed whether to give access to user or not.

Architecture Diagram :




System architecture is build up of set of connected together for processing one by one. In this architecture there firstly registration is carried out for new user at that time user chooses particular password type along with user name which is then stored in database. At the time of login users needs to enter same password for successful log-in into system.

## III. PROJECT IMPLEMENTATION

To enter in system set of pixel choosing, the pixel point with which registered. As we are choosing a pixel for each pixels co ordinates are generated, these pixel co ordinates should be properly get matched in order to which interface of system.
Co ordinates are stored in format of (xi, yi), in this xi point is belongs to x-axis and yi point is belongs to y-axis. Like this for each pixels xi & yi co ordinates are calculated. All these pixel co ordinates stored in database which are going to be verification phase.

PCCP Algorithm Study:

Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere of interest herein are cued-recall click-based graphical passwords [1]. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include PassPoints and Cued Click-Points. 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 [2]. 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 security weaknesses make passwords easier for attackers to predict. Hotspots 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. Users also tend to select their click-points in predictable patterns (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 [3]. A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the Usefulness of hotspots for attackers. Rather than their click-points on one image, CCP uses one click-point on five different images shown in sequence [1]. The next image displayed is based on the location of the previously entered click-point creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence.

## IV. TEST RESULT:

PERVASIVE CUDE CLICK POINT

**Input:**

User can choose a pixel as input on given Picture.

To click on Picture six times that is select the six points on Picture.

**Output:**

More safe or secure our system through graphical password.

**Process**

To login process, there is need of entering the sequence of clicks a pixel in the correct order, within a system-defined or user defined tolerative square of the original click-points. Normally hotspots are said to be the areas of image that are more probability of choosen by user for passwords. Attackers try to gate the charge of hotspot choosen and try to create the dictionaries for attacks to find the password. Normally users of system try to select number of pixel-points with respect to the commonly used points, which attackers try to break with respect to knowledge of passpoints.

In PCCP, Cued Click-Points(CCP) was created for making chances lower for attacker to analyze patterns and used by them to attack on to pixels point. In this instead of selecting pixels on single image, user select single pixel one image and then proceed for next image for another pixel. There are two set of images one set for correct choosen pixel and another set is for wrongly choosen pixel. New password is generated by selecting different set of images with different sequence.

PAIRED BASED

In during registration ,user can submits his password. We have enter maximum length of the password is 6 and it is called as secret password. These secret password should contain even number of characters. These session passwords are generated based on this secret password. During login phase, when the user enters his username and the grid is displayed. This grid is of size 6 x 6 and this grid consists of alphabets or character and numbers. These alphabets and number are randomly placed on the grid and the interface changes every time when one character placed. User has to enter the his password is depending upon the secret password. User has to consider these secret pass in terms of pairs. These session password consists of alphabets and digits. The first character in the pair is used to select the column and the second character is used to select the row. The point of intersection character is part of the session password. This process is repeated for all pairs of secret password.

## V. RESULT ANALYSIS:

Effort Estimate Table:

In this the system is handed over to number user for demo purpose and after there usage results are obtained and then result analysis is done for making statement about the system.

Effort Estimate Table:

| Task | Effort weeks | Deliverables | Milestones |
|---|---|---|---|
| Analysis of existing systems & compare with proposed one | 4 weeks | | |
| Literature survey | 1 weeks | | |
| Designing & planning | 2 weeks | | |
| o System flow | 1 weeks | | |
| o Designing modules & it's deliverables | 2 week | Modules design document | |
| Implementation | 7 weeks | Primary system | |
| Testing | 4 weeks | Test Reports | Formal |
| Documentation | 2 weeks | Complete project report | Formal |

Table 2: Phase Description

Phase Description:

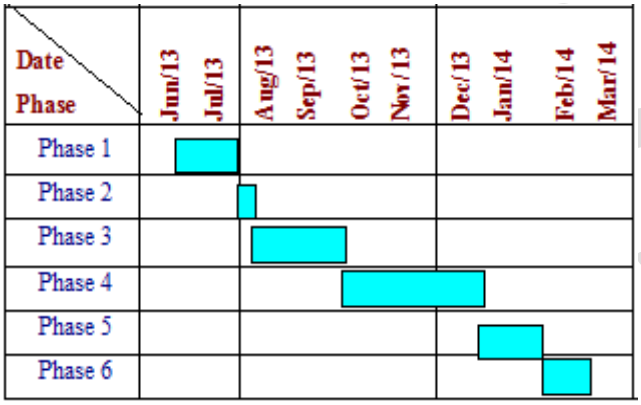
This includes systematically distribution of working phases of the project, in this work is divided into the set of steps for accomplishment of system.

| Phase | Task | Description |
|---|---|---|
| Phase 1 | Analysis | Analyze the information given in the IEEE paper. |
| Phase 2 | Literature survey | Collect raw data and elaborate on literature surveys. |
| Phase 3 | Design | Assign the module and design the process flow control. |
| Phase 4 | Implementation | Implement the code for all the modules and integrate all the modules. |
| Phase 5 | Testing | Test the code and overall process weather the process works properly. |
| Phase 6 | Documentation | Prepare the document for this project with conclusion and future enhancement. |

Project Plan:

It consists of month wise distribution of the project for its processing. Modules are divided and assigned with a date that needs to be followed for accomplishment.

Table 3: Project Plan




## VI. SECURITY ANALYSIS

As we are using dynamic password dictionary attacks can't Happened. Hidden camera is also unable to capture secret pass.

We are implemented shuffling strategy is difficult for attacker to analyze the secret pass pattern.

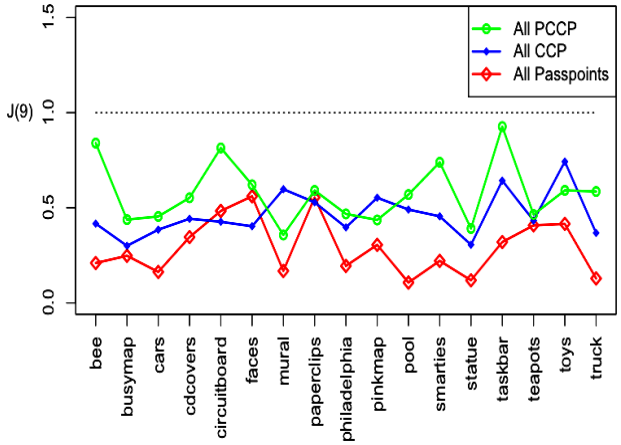



Fig.4.Security Analysis

## VII. ADVANTAGES

**Dictionary *Attack***: Dictionary attack is carried out on texual- password. In these type of attack attacker uses set of dictionary word to crack the password. In these attacker enters different combination of words and symbol to enter the system. The dictionary attacks are unable to get succeed to get authenticated.

As we are implemented dynamic passwords are used for every login.

**Shoulder *Surfing***: In shoulder surfing attack, attacker stood behind the user, try to watch password from shoulder of the user. As we are used secret mechanism at registration time, the password remains abstract from other.

Shuffling technique is used so even though if attackers watching behind the shoulder he didn't recognized the secret pass.

**Guessing**: Guessing is concept in which attacker normally guesses password on the tendency of user. As normally user tends to chooses password like birthdates, pat name, account number etc it become guessable and attacker is possible to break the system.

We are used secret pass technique so it can't be guessable for any attacker.

**Brute force attack***:* A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

**Complexity:** The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 5, the complexity is 368. In the case of the Image based Authentication Scheme the complexity depends on colors and ratings. The complexity is 8! if ratings are unique ,otherwise it is 8^8.

## VIII. APPLICATIONS

Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices**.** Two new authentication schemes are proposed for PDAs. These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication schemes use text and colors for generating session passwords

## IX. CONCLUSION

On completion of our project after result analysis we reach to conclusion the mechanisms we used like secret pass, click point and shuffling provides higher level security measured. Using graphical password system we can minimize the attack like dictionary attacks, brute force attacks, guessing attacks, shoulder surfing attacks. Graphical password surely comes in handy as graphical representation is more memorizable over text password.

## X. ACKNOWLEDGEMENT

We would like to gratefully acknowledge the enthusiastic guidance of Prof.Dighe M.S. during this work. We thank for the technical discussions on the spectral response model and for the help with optical measurements and relevant discussions. In particular We would like to acknowledge the help of Prof.Jadhav H.B.(Coordinator) for his support. Our all project group are thanked for their assistance with all types of problems at all times.From the staff Prof.Gade D.P. HOD, Computer Engineering Department whose invaluable guidance supported us in completing this Report. We would like to express deepest appreciation towards Dr.Nagraj T.K., Principal of Shri Chhatrapati Shivaji College of Engineering. At last We must express our sincere heartfelt gratitude to all friends and staff members of Computer Engineering Department who helped us directly or indirectly during this course of work. We also thankful to all Teaching and non Teaching members of Computer Engineering Department who helped us throughout this task.

## XI. REFERENCES

[1] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013).

[2] IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING VOL.9 NO.2 YEAR 2012.

[3] IEEE Transactions on dependable and secure computing Vol.9 No.2 Year 2012.

[4] R. Biddle, S. Chiasson, and P. van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Computing Surveys (to appear), vol. 44, no. 4, 2012.

[5] World Research Journal of Human-Computer Interaction ISSN: 2278-8476 & E-ISSN: 2278-8484, Volume 1, Issue 1, 2012.

[6] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[5] 33rd Annual IEEE International Computer Software and Applications Conference. Towards Usable Solutions to Graphical Password Hotspot Problem 2009

[7] S. Chiasson, A. Forget, R. Biddle, P.C.van Oorschot, *Influencing Users Towards Better Passwords: Persuasive Cued Click-Points.* HCI 2008, September 1-5 2008.

[8] ESORICS 2007, Dresden Germany, September 2007. J.Biskup and J. Lopez (Eds.): ESORICS 2007, LNCS 4734, pp.359-374, 2007.c Springer-Verlag Berlin Heidelberg 2007.

[9] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC' 2005.

[10] D. Davis, F. Monrose, and M.K. Reiter, *On User Choice in Graphical Password Schemes.* In Proceedings of the 13th USENIX Security Symposium, San Diego, 2004.