INTRODUCTION

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 [6]. A password authentication [11] system should encourage strong passwords while maintaining memorability. We propose that authentication schemes [13] 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.

We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) [2],[3], and conducted user studies evaluating usability and security. This paper presents a consistent assimilation of earlier work [1],[2],[3],[4],[5] and two unpublished web studies, reinterprets and updates statistical analysis incorporating larger data sets, provides new evaluation of password distributions, extends security analysis including relevant recent attacks, and presents important implementation details. This systematic examination provides a comprehensive and integrated evaluation of PCCP[2],[3], covering both usability and security issues, to advance understanding as is prudent before practical deployment of new security mechanisms[13].

Text passwords are the most popular user authentication [11] method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks. Graphical passwords [1],[12] offer another alternative, and are the focus of this paper. Graphical password [12] systems are a type of knowledge-based authentication [13] that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cue-recall click-based graphical passwords [12]. 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 [9], 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 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. By adding a persuasive feature to CCP, PCCP [2],[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. 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 [9] entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

We looked at several password characteristics to find whether known patterns exist that could help attackers fine-tune an attack strategy. These patterns involve the spatial position of click-points relative to each other and do not consider the background image. In earlier work, we performed this analysis on a subset of the current data, focusing
primarily on data from lab studies. Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user entered data, or by tricking users into revealing their passwords [12]. For systems like PCCP [2],[3], CCP, and PassPoints[9] (and many other knowledge-based authentication schemes[13]), capturing one login instance allows fraudulent access by a simple replay attack. We summarize the main issues below; detailed discussion is available.

An alternative to increasing the number of images is to use larger images but crop them differently for each user. Hotspot analysis would be more difficult for attackers because the coordinates of hotspots could not be directly applied across accounts. If furthermore, each user receives a different pool of images, an attacker would need to collect these data on a peer-user basis when launching an attack.

1.1 OBJECTIVE:

The main aim of this paper is the persuasive cued click points option where the user will be provided an option of selecting the hotspots in an image. And provided an option of selecting the images to create the authentication page. Possibility of monitoring the hotspots by the nearby user is possible.

1.2 SCOPE:

The scope of this paper is to create a Graphical password scheme which includes usability, security evaluations, implementation and integrated evaluation of the password scheme in a graphical manner.

2. SYSTEM ANALYSIS

System Analysis is a combined process dissecting the system responsibilities that are based on the problem domain characteristics and user requirements.

2.1 EXISTING SYSTEM:

Replacing the textual password with a graphical password [7],[12] is the core idea of the paper. In the older ages, the passwords were materialized in the form of graphical passwords with X,Y as co-ordinates on the images. Randomization clicks on the images enable the user to access the system is one of the major drawbacks. To overcome this issue, Persuasive cued click points [2],[3] comes into the picture. A picture [9] will be framed with multiple click points in turn, which will have successive cued clicks on the images. The core point is, the user should select a secure hotspot in the image. 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. Still, if there is a possibility of selecting the correct spot in the first image. The possibility of selecting the second hot spot becomes a complex end where the user will be deviated at various stages and possibility of access the application is not possible.

DISADVANTAGES:

- Users will be provided an option of selecting the images to create the authentication page which is not included in the existing.

2.2 PROPOSED SYSTEM:

The user will be provided an option of selecting the hotspots in an image. The successive selection of the exact hot spots will enable the user to move the next successful images. For login into the system, the user will be provided an option of selecting the hotspot in the continuous 3 images [10]. After reaching the successful login attempt the user will be allowed to access the application. Storing the images in a secure database through file stream data type is one of the option used to secure the images instead of storing the images in the server. Users will be provided an option of selecting the images to create the authentication [11] page which is not included in the existing system. Possibility of monitoring the hotspots by the near by user is possible. To avoid the same the password with matrix formation is one of the complex password scheme in the world. This option is been added in our paper.

ADVANTAGES:

- Integrated evaluation of the password scheme in a graphical manner.
- Users will be provided an option of selecting the images to create the authentication page.

3. SYSTEM DESIGN

System Design involves identification of classes their relationship as well as their collaboration. In object or, classes are divided into entity classes and control classes. The Computer Aided Software Engineering (CASE) tools[5] that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that is helpful only after the construction of the class diagram. In the FUSION method some object-oriented approach likes Object Modeling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Object used the term” agents” to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software paper is worked out by both the analyst and the designer. The analyst creates the user case diagram. The designer [5] creates the class diagram. But the designer can do this only after the analyst creates the use case diagram [5]. Once the design is over, it is essential to decide which software is suitable for the application.

3.1 ARCHITECTURAL DIAGRAM:
3.2 DATA FLOW DIAGRAM:

The Data Flow diagram is a graphic tool [5] used for expressing system requirements in a graphical form. The DFD also known as the “bubble chart” has the purpose of clarifying system requirements and identifying major transformations that become program in system design [5]. Thus DFD can be stated as the starting point of the design [5] phase that functionally decomposes the requirements specifications down to the lowest level of detail. The DFD consist of series of bubbles joined by lines. The bubbles represent data transformations and the lines represent data flows in the system. A DFD describes what that data flow in rather than how they are processed. So it does not depend on hardware, software, data structure or file organization.

4. IMPLEMENTATION

Implementation is the stage of the paper, when the theoretical design is turned out into a working system.

4.1 NEW USER REGISTRATION MODULE:

In this module, the user is permitted to provide the basic authentication information like first name, last name, mobile number, city, user name, password and security questions like your mother’s maiden name?, your childhood friend?, your passport number?. The mobile number should contain only 10 numbers. And other information should contain only alphabets. After entering all the details, then click add user. Then the user will be added successfully.

4.2 COLOR MATRIX FORMATION MODULE:
In this module, the user will be provided with the set of eight colors like red, blue, green, yellow, black, grey, orange and pink. User needs to provide number for each color, from 1-8. And user should remember the number which is provided to the color. After numbering, the user should click the submit button. So that the user color scheme will be updated.

![Fig:4 Color Matrix Formation Module.](image)

### 4.3 Genuine Image Selection Module:

In this module, the user will be provided with some set of images [10]. The user is permitted to select the images and provide appropriate ranking to those images. Once the images were provided with ranking, the user should click the submit ranking button. So that, the image preferences will be saved successfully. Then the users were provided an option of selecting the hotspots in the hierarchy of the images [10]. After selecting the hotspots the fake hotspots will be generated automatically. Once the hotspot is identified, the relevant point boundary of the hotspot is identified with the help of fast image segmentation algorithm. Then the image points for the three pictures will be finalized. Appropriate pixel values of box shaped were taken to avoid discrepancy in identifying the hotspot, during authentication page [6],[13]. The fake images with fake hotspot on the images will increase the complexity of the authentication scheme [6].

![Fig:5 Genuine Image Selection Module.](image)

### 4.4 Authentication Scheme Module:

In this module, the user will be permitted to provide their valid credentials to login into the system. Before finalizing the validation of the user, they need to cross two level of boundaries. The first check will be the matrix validation. Once the user provides valid data, he will be allowed for the second check. In the second check users will be checked for the valid hotspot [8] of the images [10]. Once the user crossed the exact boundaries of valid checks. He will be permitted to view his profile page. If more than a stipulated time, the user have tried the login. In that case, the user will be blocked permanently and it can be overcome by the admin.

![Fig:6 Authentication Scheme Module.](image)

### 4.5 Matrix Verification Module:
In this module, the user needs to enter the correct username. After entering, an 8*8 matrix is formed and it’s displayed to the user. The user needs to verify the color combinations in the matrix. Based on the intersection of the input value provided by the user during registration, the matrix will be manipulated and the user needs to provide the exact intersection points. If the intersection points are valid, he will be the authorized user \[11\], so that he will be allowed for the second level of validation.

**Fig:7 Matrix Verification Module.**

### 4.6 HOTSPOT VERIFICATION MODULE:

In this module, users will be provided with an image \[10\]. So that the user needs to select the successive hotspot \[8\] on the continuous three images \[10,12\]. If the user clicks the correct hotspots, then he will be the authorized user to access the application. If the user clicks the fake hotspots \[8\], then he will not be the authorized user \[11\] to access the application.

**Fig:8 Hotspot Verification Module.**

### 5. CONCLUSION

The problem is that user requires additional effort on the part of users creating passwords and often provides little useful feedback to guide user’s actions. In PCCP, creating a less guessable password is the easiest course of action. A common security goal in password based authentication systems is to maximize the effective password space. In this paper we have bought the color matrix formation method, so that even though the hotspots viewed by the neighboring user while entering the account will not be easy for the users to enter into the others user account. So that to login to the system the user needs to cross the two levels of boundaries. The first one is the color matrix method and the second one is the hotspot click method. So that in this paper the enough security to the user’s account is made successfully.

Better user interface design can influence users to select stronger passwords. 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 behavior 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.

**REFERENCES**


