# Persuasive Cued Click Point Authentication

**C.Pavithra[1], Mrs.K.Dhamayanthi[2]**
[1]Dept of MCA
[2]Associate Professor, Dept of MCA
[1, 2] Francis Xavier Engineering College,Vannarpettai

***Abstract***- *Computer security depends largely on passwords to authenticate human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. However, this method has been shown to have significant drawbacks. Now, several computer systems, networks and internet-based condition are demanding the use of graphical authentication method. Therefore, base of an authentication system is to stimulate users to pick healthier password, which increases security, usability and also refining the password space. According to a recent Computer world news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional user name password authentication, alternative authentication methods, such as biometrics, have been used. In this paper, however, we will focus on another alternative: using pictures as passwords. Cued Click Point (CCP) authentication is a graphical password scheme that requires users to click on pre-selected points in a sequence on an image. CCP offers a promising alternative to traditional alphanumeric passwords by leveraging the users' spatial memory and visual recognition skills. This authentication method is easy to remember, easy to use, and offers enhanced security compared to traditional password schemes. This password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text, psychological studies support such assumption.*

***Keywords***- Graphical password, Authentication systems, Text passwords, CCP

## I. INTRODUCTION

During early days text password was the well-known and only proposed computer authentication scheme to authenticate the user. Initially text passwords were used for authentication system. Text password is nothing but simply collection of characters or string. As how user has to always create their own passwords for different systems, which would be rememberable but hard to guess attackers. But text passwords are easy to hack with some hacking techniques like brute force and fishing attacks. As well as it is again difficult to remember more than one text password for number of different systems to the user. After some time, biometric and token-based password authentication systems were introduced as an alternative to the text password but again it has its own drawbacks as it requires extra hardware setup and cost to setup new system for it. After some time, as alternatives for all those methods introduced is Cued Click Point Authentication system as it is very cheap and best. As well as per psychological studies user can remember graphical passwords very well than text passwords. Graphical password is of three types: Click based graphical password scheme, Choice based graphical password scheme, Draw based graphical password scheme. This project uses Click Based Graphical Password Scheme, where users will click on the image which are in random sequence every-time. Users can click any number of positions as they want, for the password the position the user clicks matter not the images. While user come to login phase, he has to select the point over the image then system again generates the new signature for that point and if both signatures are same then and then user can be said ad authenticated user. Otherwise, the system will say to the user about the failed login, if the user has 3 failed logins his/her account will be locked and only after they login using the link send to their mail their account will be unlocked.

## II. RELATED WORK

H. Gao et.al[1], proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidental login is high and password is too short. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated.

Sreelatha et al[2], In this paper ,the proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed. As the color rating given by the user, the password will generate. Er. Aman Kumar et al[3], In this system the user draws the selected object which is then stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Then the user draws pre-selected objects as his password on a touch sensitive screen with a mouse. Then the system performs preprocessing.

Ramkrishna Khetan et al[4], In this proposed scheme, they propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Afterward, we examine the security and usability of the proposed system, and show the resistance of the proposed system to shoulder surfing and accidental login. The benefit of this system is that it reduces the login time & it is an efficient system.

Ali Mohamed Eljetlawi et al[5], The design process will be divided into two stages, existing user and new user. If the user does not have password which means that he is a new user, so he has to enter his user name and start create his password. The usability features set will be transforming into a proposed graphical password prototype.

Akshay Karode et al[6], In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred to as drawmetric systems because users recall and reproduce a secret drawing.

Xiaoyuan Suo et al[7], One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text-based passwords.

Andrew S. Patrick et al[8], There has been much interest recently in using biometrics, such as fingerprints or voice patterns, for user identification, but these systems can have their own problems. Biometrics can be hard to forge but easy to steal.

Mathuri Pandi et al[9], Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords. Knowledge-based authentication (KBA) is based on Something You Know to identify.

Akin Akinyele et al[10], Pure Recall-Based Techniques -This approach involves the ability of users to reinvent their graphical objects from memory without any assistance from the system. This approach is demonstrated in the research work such as Passdoodle, grid selection techniques and the Draw-A-Secret technique. A group reserchers proposed a technique based on a draw-based method which is known as Draw-A-Secret (DAS). With this approach, usersare required to draw their secret on a 2-grid using stylus or mouse. However, a previous study suggested that DAS users may want to pick weak graphical passwords that are vulnerable to graphical dictionary attack

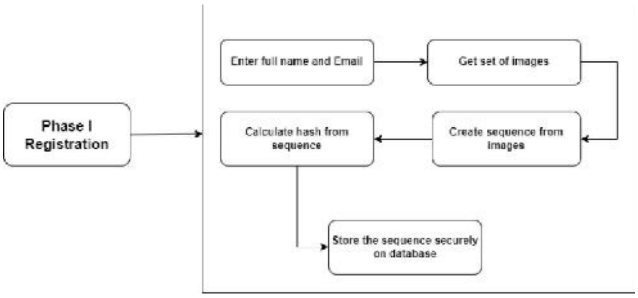
## III. THEORY

Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. Access to computer systems is most often based on the use of alphanumeric passwords.Because human beings live and interact in an environment where the sense of sight is predominant for most activities, our brains are capable of processing and storing large amounts of graphical information with ease. While we may find it very hard to remember a string of fifty characters, we are able easily to remember faces of people, places we visited, and things we have seen. These graphical data represent millions of bytes of information and thus provide large password spaces. Thus, graphical password schemes provide a way of making more humanfriendly passwords while increasing the level of security. Authentication schemes such as sessions method authenticate the user by session passwords which 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. But in this same problem occurs that every time user has to enter password again and again. It is too hard to remember password and as the session password is only for a particular time. To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user-friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing. Here text was combined with image and color to generate the session password and every time user have to enter new password as session ends.

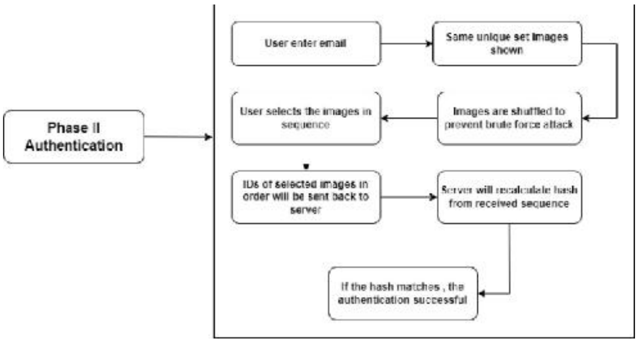
The graphical password-based authentication system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system cued click point to make authentication system more secure. Basically, during password creation, the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hot spots. Therefore, this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides thesystem suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system provides forgot password option to get back their account. Mail sent to the verified phone no so that they can easily get back the account. In case if the user failed to click right point for at least 3 times they will be blocked from login and login link will be send on users registered email.

*A 1. Research Methodology*

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. In a Cued Click Point Authentication system, the user has to select from images, in a specific order,presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords. Therefore, this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space.


Phase I Registration
Enter full name and Email
Get set of images
Create sequence from images
Calculate hash from sequence
Store the sequence securely on database

Registration


Phase II Authentication
User enter email
Same unique set images shown
Images are shuffled to prevent brute force attack
User selects the images in sequence
IDs of selected images in order will be sent back to server
Server will recalculate hash from received sequence
If the hash matches , the authentication successful

Authentication

*A 2. Algorithm Implementation*

The Cued Click Point (CCP) algorithm can also be used in Cued Click Point Authentication systems to improve their security and usability. In this context, the CCP algorithm works by presenting a user with a grid of images, and prompting them to click on specific points within certain images in a predetermined sequence.

The CCP algorithm in Cued Click Point Authentication typically involves the following steps:

Step1: The user is presented with a grid of images, and is asked to click on a specific point within one of the images. This point serves as the "cue".

Step 2: After the user clicks on the cue, the system prompts them to click on specific points within other images in a predetermined sequence.

Step 3:If the user clicks on the correct points in the correct sequence, they are granted access to the system.

The CCP algorithm can improve the security of Cued Click Point Authentication systems by making it more difficult for attackers to guess or crack passwords. It also has the advantage of being more memorable and easier to use for users, since they only need to remember the sequence of images and clicks, rather than a complex alphanumeric password.

## IV. EXPERIMENTS AND RESULTS

The main objective of Cued Click Points (CCP) authentication is to provide a more secure and user-friendly alternative to traditional alphanumeric passwords. The method aims to address the limitations of traditional passwords, such as weak passwords, password reuse, and password guessing attacks, by using images and predefined points as authentication factors. CCP aims to make authentication more secure by creating a unique sequence of clicks on images that only the user knows, making it difficult for attackers to guess or brute-force the password. Additionally, CCP is designed to be easy to use, even for non-technical users, with a simple and intuitive interface. Overall, the objective of CCP is to provide a more secure and user-friendly authentication method that can be easily adopted by a wide range of users

### *A 1. Simulation Environment*

The Django web framework is a free, open-source framework that can speed up development of a web application being built in the Python programming language.

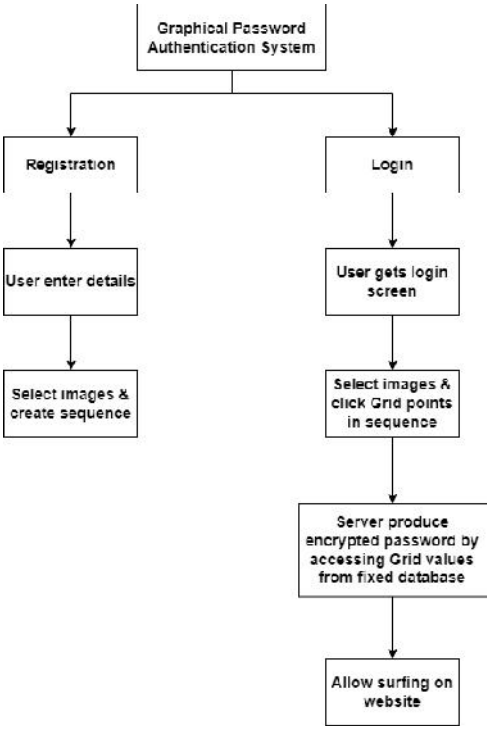
**Make database management more Python-like:**Starting a Django project allows you to build your application's entire data model in Python without needing to use SQL. Using an object-relational mapper (ORM), Django converts traditional database structure into Python classes to make it easier to work within a fully Python environment. Django Web Framework offers a shortcut to full integration with your application's database. It provides CRUD (create, read, update, delete) functionality, HTTP Response and cross-site scripting, supplies user management capabilities, offers software administration features and more.

**Create dynamic pages with templates:** The Django application produces that dynamic HTML with a built-in templating engine called the Django template language (DTL). An HTML template allows Django developers to combine static elements (including design elements such as colours, logos, or text) with data (such as user names or locations) to create a new web page on the fly.

**Enhance security:** Web apps are frequent targets of hackers, especially applications that store user login information or financial data. Django offers features to help protect your application and your users. One of the biggest risks for sites that accept user-entered data is that a malicious user will inject code with their data that can have a disastrous effect on your system. To protect against attacks like these, Django templates automatically escape common HTML characters in any user-entered field.

**Scaling Django:** Django web framework makes scaling easy. Because a Django app can manage your user sessions, you can add more instances of your application and transfer the user's experience across the instances without losing data.

### *A 2. Architecture diagram*


Graphical Password Authentication System
Registration
Login
User enter details
Select images & create sequence
User gets login screen
Select images & click Grid points in sequence
Server produce encrypted password by accessing Grid values from fixed database
Allow surfing on website

Architecture Diagram

The overall system design consists of following modules

1. Login Authentication
2. New User Registration
3. Cued click Point Module

### 1. Login Authentication

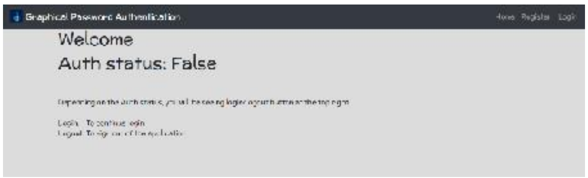
Login validation is utilized to check whether the client is an approved individual to utilize the framework. For each client have been new username and secret word with one-of-a-kind number is given through graphical framework which they can access and checking their confirmation subtleties of clients. In this undertaking can get to the client should give the right username and secret key dependent on graphical pictures.

### 2. New User Registration

The enlistment login module handles standard client enrolment and login usefulness. In the enrolment stage the new understudy can enlist the subtleties and get the administration, if there is any new client they can make the new login id, in enrolment the new client must give full insights regarding the name, email, portable number, at long last they will get the client's name and secret word graphically.

### 3. Cued click point Module

By selecting all click point on single image introduces hotspots creation. In CCP user have to select different five images instead of selecting click point on same image. For every image user have to select only one click point. When user click on a correct position on image, then next image will display. In CCP address of next image is stored in previous click point. if a user enters an incorrect click-point during login, the coming image will also be incorrect. Unknown or hacker is who was saw an unrecognized image will 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.

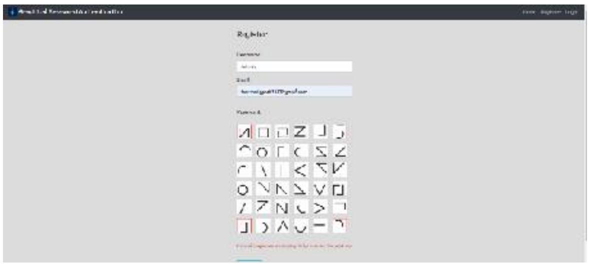


Welcome
Auth status: False

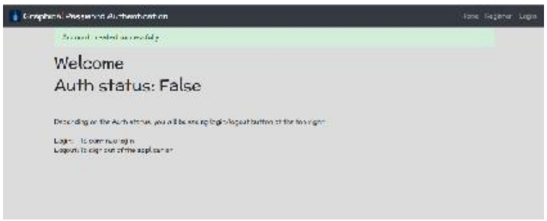
Depending on the auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Home Page



Users sign up page



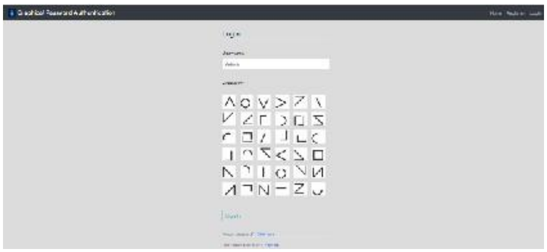
Account created successfully

Welcome
Auth status: False

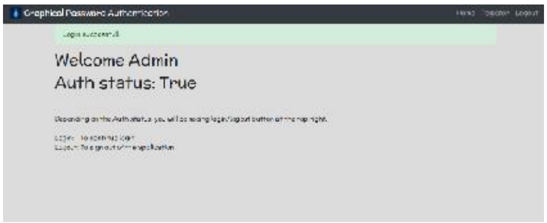
Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Successfully user complete the registration



Login page



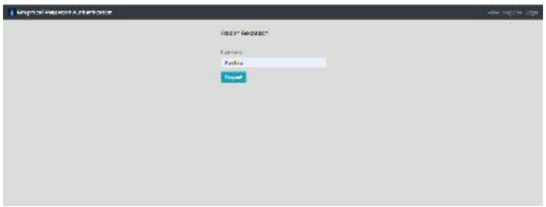
Login successful

Welcome Admin
Auth status: True

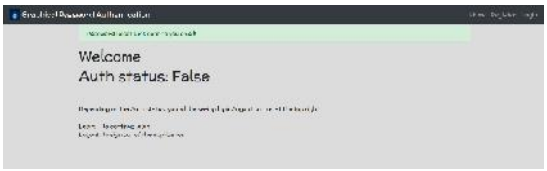
Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

After successfully login

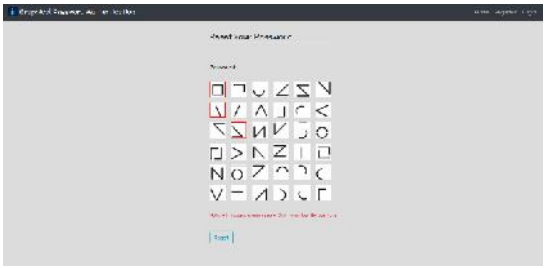


Reset password



Welcome
Auth status: False

Reset link sent to registered email



Password Reset

*A 3. Performance Metrics*

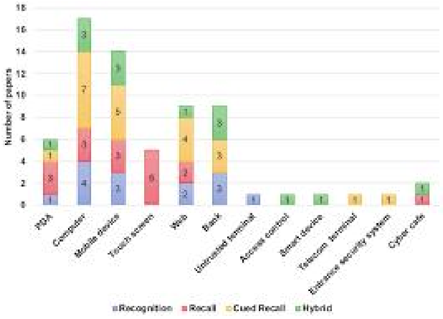
The Cued Click Point (CCP) algorithm can also be evaluated for its performance in Cued Click Point Authentication systems. Here are some common performance metrics for the CCP algorithm in Cued Click Point Authentication:

**Accuracy:** This metric measures how often users are able to correctly authenticate using the CCP algorithm. Accuracy is typically reported as a percentage of successful logins over the total number of login attempts.

**Time to authenticate**: This metric measures the time it takes for a user to successfully authenticate using the CCP algorithm. A shorter time to authenticate indicates better usability and user experience.

**Memorability:** This metric measures how easily users can remember their clicks on the cue and subsequent images. A memorable click sequence is more likely to be used by users and less likely to be forgotten or written down, reducing the risk of security breaches.

**Security:** This metric measures the effectiveness of the CCP algorithm in preventing unauthorized access. A more secure system will have lower rates of successful attacks or guesses.
User satisfaction. By evaluating these performance metrics, designers and researchers can better understand the strengths and weaknesses of the CCP algorithm in Cued Click Point Authentication systems and make improvements to enhance usability, security, and user experience.



Cued click point metrices

## V. DISCUSSION AND CONCLUSION

Through the proposed Cued Click Point Authentication system, we overcame the limitations of the existing text-based passwords. The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Thus, Cued Click Point Authentication is quite user friendly and secure as compared to other authentication methods. Random image selection, making slight modification to images for each user and shuffling them renders most of the widely used cyber-attacks useless. Efficient image compressing techniques also make this type of authentication suitable for offline authentication systems as well as devices with low memory.

## VI. FUTURE SCOPE

In future it has great scope. It can be used everywhere instead of text-based password. We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication systems but they have their own advantages and disadvantages. Cued Click Point authentication has become increasingly popular as an alternative to traditional alphanumeric passwords due to its perceived security and usability benefits. However, there is still room for improvement and enhancement.

Here are some future enhancements that could be implemented in Cued Click Point authentication.

**Multi-factor authentication:** One possible future enhancement is to add additional layers of security to Cued Click Point Authentication, such as multi-factor authentication. This could involve combining graphical passwords with other authentication methods, such as biometric authentication or one-time passwords.

**Machine learning algorithms:** Another future enhancement is to incorporate machine learning algorithms to improve the security and usability of graphical passwords. These algorithms could analyse user behaviour and usage patterns to identify potential security threats and adjust authentication requirements accordingly.

**Gamification**: Gamification could also be used to enhance Cued Click Point Authentication. This could involve turning the password creation process into a game or challenge that encourages users to create more complex and secure passwords.

**Dynamic authentication:** Another possible future enhancement is to make the Cued Click Point Authentication process more dynamic. This could involve using a dynamic image database that changes regularly, making it more difficult for attackers to guess the password.

**Virtual reality authentication:** As virtual reality technology becomes more advanced and widespread; it could be used as a new way to authenticate users. Virtual reality could provide a more immersive and engaging authentication experience thatis both secure and user-friendly.

## REFERENCES

[1] “Graphical Passwords: A Survey”, Xiaoyuan Suo Ying Zhu G. Scott. Owen Department of Computer Science , Georgia State University.

[2] The Shoulder Surfing Resistant Graphical Password Authentication Technique,Mrs.Aakansha,S.Gokhalea, Prof.Vijaya S.Waghmareb, 7th International Conference on Communication, Computing and Virtualization 2016

[3] GPAS - Graphical Password uthentication System for Software Privacy Protection S.Geetha, N.Thilagavathi, A.Nivedha shree, M.Subalakshmi, April 2016.

[4] Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[5] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[6] Graphical Password Authentication Vishal Pednekar, Sayli Tawhare, Arundhati Pradhan, Nidhi Shettigar, Bharati Singh, Amisha Sahu Department of Computer Engineering.

[7] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[8] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[9] A. Gilbert, "Phishing attacks take a new twist," in CNET News.com, May 04, 2005.

[10] A. Jain, L. Hong, and S. Pankanti, Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000. [8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[11] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[12] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest

[13] Renaud. “Evaluating authentication mechanisms”. In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.

[14] D. Florencio and C. Herley. “A large-scale study of WWW password habits”. In 16th ACM International World Wide Web Conference (WWW), May 2007.

[15] Xiaoyuan Suo, Ying Zhu, G.Scott. Owen, “Graphical Passwords: A Survey”, Department of Computer Science Georgia State University.

[16] Kirkpatrick. “An experimental study of memory”. *Psychological Review*, 1:602-609, 1894.

[17] S. Madigan. “Picture memory”. In J. Yuille, editor, *I*magery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[18] A. Paivio, T. Rogers, and P. C. Smythe. “Why are pictures easier to recall than words?” *Psychonomic Science*, 11(4):137-138, 1968.

[19] R. Shepard. “Recognition memory for words, sentences,and pictures”. *Journal of Verbal Learning and VerbalBehavior*, 6:156-163, 1967.\

[20] Graphical Password Authentication System Akshay Karode, Sanket Mistry and Saurabh Chavan Computer Department, Mumbai University, Mumbai.

[21] .Liew Tze Hui; Housam Khalifa Bashier; Lau Siong Hoe; Goh Kah Ong Michael; Wee Kouk Kwee - Conceptual framework for high-end graphical password - 2014 2nd International Conference on Information and Communication Technology (ICoICT)

[22] R. Shepard. “Recognition memory for words, sentences,and pictures”. Journal of Verbal Learning and VerbalBehavior, 6:156-163, 1967.

[23] S. Madigan. “Picture memory”. In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[24] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[25] Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.