Authentication using Persuasive Cued Click Points (PCCP) with Improved Advanced Encryption Standard (IAES)

Vasudha Kalra
Department of Computer Engineering, Student, HMRITM Delhi

Karishma Ahlawat
Department of Computer Engineering, Student, HMRITM Delhi

Ravinder Beniwal
Department of Computer Engineering, Asst. Prof. HMRITM , Delhi

***Abstract*-- Security of information and hence the authentication is the major concern in today's era of digital communication. Knowledge based authentications are the most widely used authentication techniques which include both text-based and graphical-based passwords. The text-based authentication has been shown to have significant drawbacks. For example, masquerading, eavesdropping, dictionary attack etc. Hence Graphical passwords becomes an important means of authorization of any type of application in both online and offline categories. The persuasive cued click point provide the graphical password feature in which the user need to click on the images to authenticate them. If the click point area of the image is seen by the attacker then he/she can enter into the system. A persuasive cued click point with improved advanced encryption standard provides the graphical password system as well as security to the database system also. Keeping these things in mind, this research is focused on password system with dual security feature. The PCCP and IAES features are implemented together for graphical password system. Hence in current research the PCCP with improved AES features is implemented for graphical password system and performance is explored.**

Keywords—Authentication, Graphical Passwords, Persuasive Cued Click Points, Improved Advanced Encryption Standard

I.INTRODUCTION

A. Why PCCP??

As text-passwords are easy to remember and easy for attackers to guess. So, graphical passwords provide us an alternative to text-passwords. Graphical passwords primarily based on pass points, password is a sequence of five click points on a given image. But in this, there is a problem of security. So, to reduce security impacts of hotspots, an alternative click based graphical password strategy called Cued- Click Points (CCP) is used.

In CCP, rather than clicking on five points on one image, CCP helps to click on one click point on each of a sequence of five images. The next image displayed is based upon the previously entered click-point. But in CCP, usability problem occurs because users are selecting click points anywhere in the image. So, in this way attacker can easily see the click-points.

To overcome the problem of CCP, PCCP is implemented. Persuasive Technology help the user to choose more strong and secure passwords. In PCCP all the five click-points are hotspots. When user start creating the password, the image that appeared in front of user is slightly shaded except random portion of viewport. In this, viewport is positioned randomly to avoid the hotspot problem. Users are requested to select the highlighted portion of viewport but they cannot select outside the viewport. If the user want to change the position of viewport, it can do this by clicking on the shuffle button. The highlighted viewport and shuffle button is present only during the password creation process. At the time of login and password conformation, there is no shaded portion present in the image and the users are free to click anywhere in the image.

B. PCCP With Added Authentication

Persuasive Technology was first articulated by Fogg [6] as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology guide and encourage users to select stronger passwords, but do not impose system generated passwords. In other words, the persuasive elements must not be ignored and the resulting passwords must be memorable. PCCP achieves this by making the task of selecting a weak password more monotonous and time consuming. The major drawback remained with the PCCP was shoulder surfing attack. Persuasive Cued Click Points did not remove the shoulder surfing attack. The next issue remains with the persuasive cued click points, it was difficult for the user to remember different images. [2] This implies there was a need of an additional authentication with PCCP. Some of the authentication techniques with PCCP are described below:

1)Persuasive Cued Click Points (PCCP) with Image Scrambling: Image scrambling (i.e., encryption) technologies are very useful tools to ensure image security by transforming the image into an unintelligible image [4]. Scrambling makes the image unrecognizable to prevent eavesdroppers from decoding the true form or meaning of the image using the human visual system or a computer system. Image scrambling [4] is a useful approach to secure the image data by scrambling the image into an unintelligible format. The most basic guessing attack against PCCP is a brute force attack, with expected success after exploring half of the password space (i.e., with a theoretical password space of 243, success after 242 guesses). However, skewed password distributions could allow attackers to improve on this attack model. We now consider how these could be leveraged in guessing attacks. Pass Point system hotspots of small number

of users can be collected and an attack dictionary can be formed, with the use of server-side information. Then this dictionary details can be used for the guessing of the click point in an image. But this does not work in PCCP with Image scrambling scheme, because the view port is entirely changing during the scrambling phase., and so it does not include the hot spot in almost all cases. If the attackers gain the access to hash table entry of the passwords, they cannot correctly predict the original password, which are kept in a different database, which can be encrypted also using any of the strongest encryption scheme[3].

2)Persuasive Cued Click Points (PCCP) With Sound Signature: In PCCP, user clicks on the viewports that are difficult to remember. So, with the help of sound signature user can easily remember the password that are difficult to remember. PCCP with sound signature, user is asked to select a sound signature corresponding to each click point. With the help of sound signature, user can easily recall the click points on an image. With the combination of both, system showed better performance in terms of speed, accuracy and ease of use. It also reduces the Brute Force attack. This system is more helpful when user is logging in the system after a long time.[5]

3)Persuasive Cued Click Points(PCCP) with Advanced Encryption Standard (AES): In order to overcome the shoulder surfing attack and to provide the security on the click points of the user's password, AES algorithm is applied on the click points. In case of PCCP, the image is divided into 16 different grids by the system on which users are allowed to choose click points. After clicking on the image first time that particular grid will be expanded and displayed in the front of the user like this the image will be divided till the third click by the user. The selected image can be from the system and from the server too. The registration process will also ask for a text password which too is encrypted with the help of AES. The x and y coordinates of the grid in the image selected by the user is taken by the system and the values of x and y are encrypted using Advanced Encryption Standard algorithm. The encrypted values of x and y are then stored into the database for authentication purpose. [2]

4)Persuasive Cued Click Points (PCCP) with Improved Advanced Encryption Standard (IAES): By adding the features of Persuasive Cued Click Points with Improved Advanced Encryption Standard achieves the better results in authentication system as compare to the PCCP & Advanced encryption standard. Graphical authentication scheme is better to remember for the user. As user has to choose only one image for the authentication purpose it is easier for the user to remember and difficult for the attacker to attack because it is difficult for the attacker to see at click points area of the image. The complexity of the PCCP with IAES is increased but the combinations to attack on the system also increases. As in this, system are providing two ways for the image selection by the users, so one more new option can provide to the users to use web cam to capture his/her own pictures at the time of registration. The PCCP-IAES system can be used for the following systems. In the following given system, the combinations of text as well as graphical passwords can be applied together.

- Banking Applications
- Storage Area Network
- Redundant Array of Independent Disk
- Hospital Management System
- Student Resource Sharing System

The PCCP-IAES can be applied on the above listed applications and by which the more security can be provided to the system. [1]

This paper describes the design, implementation and the evaluation of Persuasive Cued Click Points(PCCP) with Improved Advanced Encryption Standard(IAES).

II.PERSUASIVE CUED CLICK POINTS(PCCP) WITH IMPROVED ADVANCED ENCRYPTION STANDARD (IAES)

Symmetric Key Cryptography is a type of cryptography in which same key is used for encryption and decryption. Advanced Encryption Standard(AES) uses symmetric key cryptography [6][7]. The key data for AES is 128 bits/ 192 bits/ 256 bits. Size of key of AES is same as the seize of data of AES. The rounds for the execution of AES technique are 10, 12, 14 for 128 bits, 192 bits and 256 bits respectively. AES 128 bits is used in this research with improved features of AES.

A salt key is added with the AES key for enhancement in AES which in turn increases the combinations of password. For example: consider data size of 128 bits, salt key of 8 bits. So, earlier the combinations of password for AES were 2^128 bits and after adding the salt key to the AES now the combinations of password will become 2^ (128+salt key).

Hence, the results after adding the salt key will automatically get improved and hence called improved advanced encryption standard(IAES).

IAES is used for encrypting the text as well as graphical passwords of the users in which salt key is used. In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password. The primary function of salts is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks.

For each password, a new salt is randomly generated [8], [9]. The salt and the password are combined and are processed with a cryptography hash function and the resulting output is stored with the salt in the database.

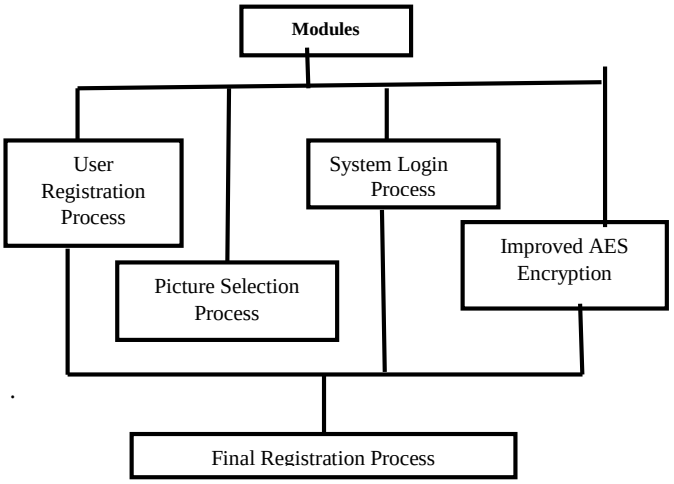

Fig 1 System Architecture Of PCCP and IAES

Figure 1 display the system architecture of PCCP &AES. There are five modules that help the user to successfully entered into the system to access the data.
First module, user registration process, user has to register themselves by providing appropriate details in order to get entry into the system. Second module, picture selection process, in this module user has to select image and user can select the image from system as well as server. After this user has to select three click points on the image so that they can register them successfully. Third module is System login process, now user has to login into the system by providing text as well as image password. The IAES Encryption is applied to the both text and image password so in this way user data is stored securely into database.
The Final module and last module is final registration process, it is the combination of entire four steps and after completion of all the four modules, last module gets completed, which is known as Final Registration Process.

III. DESIGN METHODOLOGY

Persuasive Cued Click Points uses technique of Knowledge based Authentication (KBA). The graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

*A) Registr*ation Process: In user registration process, the user has to enter the user name, email id, contact number and text passwords. After filling all the required data in the registration form the user is successfully registered for the system. The user interface of registration process is shown in the figure 2

B) Login Process: Figure 3 displays the flow of system working under PCCP with IAES technique. There are total five steps to complete the process of system. In first process user has to enter his/her email Id for entering into the system. The second process, user has to enter the text password. In third step user has to select images for password for this system provides two way for selecting images passwords, the one is system image and other is server image. So, user has choice to select image from the system or from the server. If the user is more comfortable with his/her system's images then he/she can select from the system's images. So, in this way it become difficult for the attacker to know which image is selected by the user. The fourth step is to click on the images selected by the user, then user has to click on the images at any three positions. The last and fifth step is Authentication. In this step user has to click on three parts of the images at the same position as he/she clicked at the time of registration. If there is match occur between the click points of login with the click points of registration then "Authenticated".

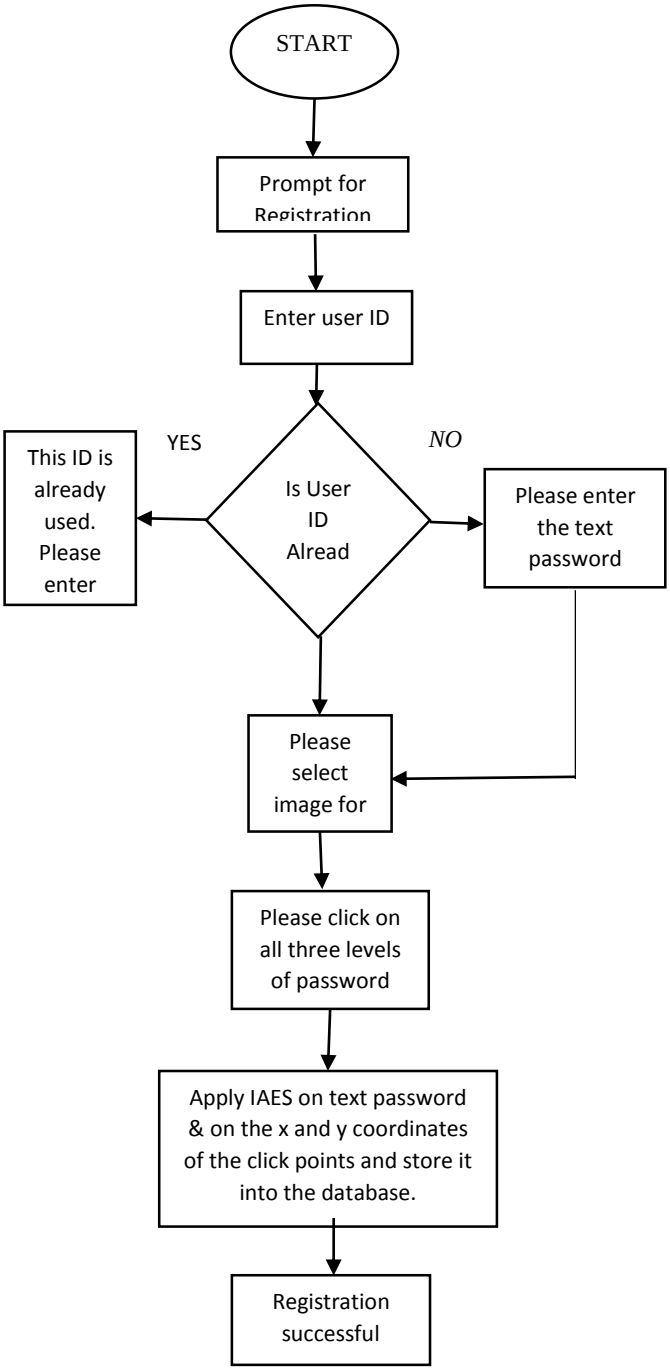

Fig 2. Registration Process

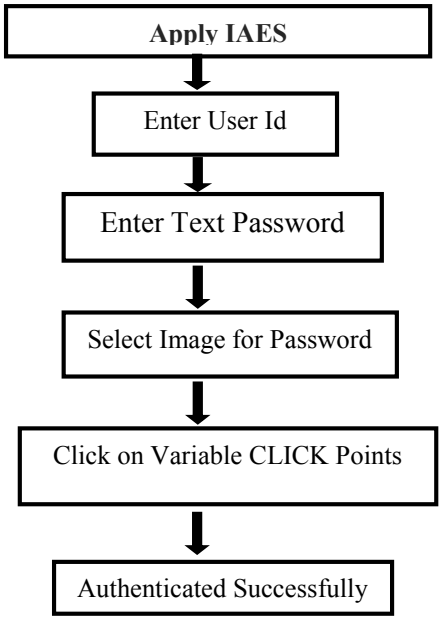

Fig.3.Flow of System

IV. IMPLEMENTATION

A) User Interface Module: Figure 4 displays the registration process of the PCCP-IAES system in which user has to enter some fields as per the instructions and click points as per their choice. The maximum click points are allotted is three (3). The default click points are 3. As per the security concern user can choose less or maximum 3clickpoints.

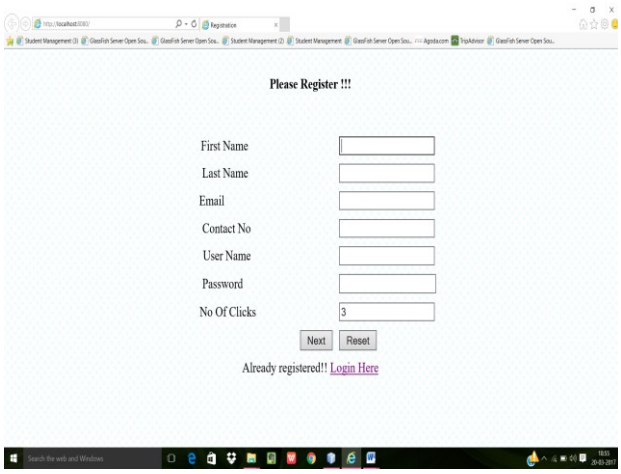

Figure 4: Registration page of PCCP-IAES

B) Server Image Selection: The image shown in figure 4 is the image selected by the user which is available on the server. The user can choose the images from the server for his passwords.

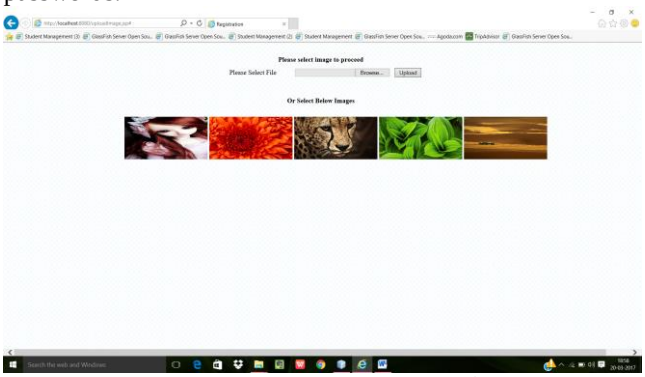

Figure 5: Server Image selection page of PCCP-IAES

C) System Image Selection: The figure shown in Figure3 image selected by users which is available on the system. For comfortably with the user's own known images make them as a password will be easy for him/her to remember it. The list of images are present in system. It means user can choose his/her favorite image from their system in which he/she is comfortable with.

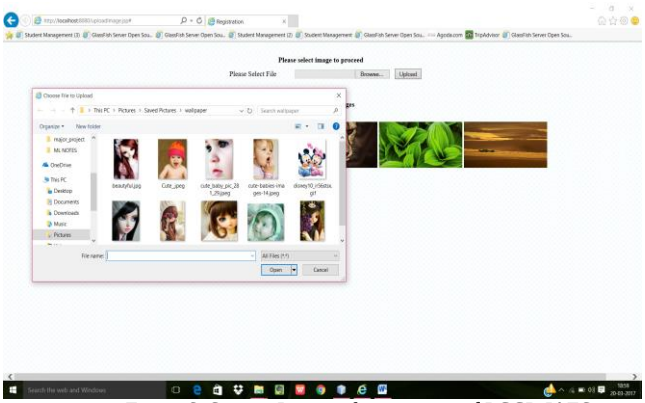

Figure 6: System Image selection page of PCCP-IAES

D) Click on the Image to Select 3 Click Points: The figure shown in Figure 7 shows the image selected by the user. The user need to select three click points on the image. These three click points would be used further in order to login. The User need to remember the click points in order to complete the login process further.

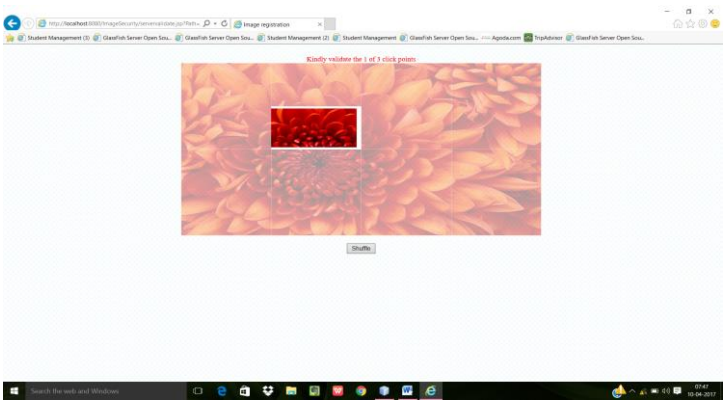

Figure 7: Select click points on selected image of PCCP-IAES

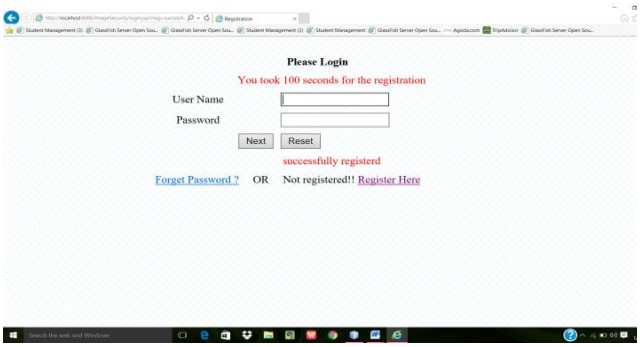

Figure 8: Login Page showing time taken for registration

E) Login Process: The following Figure 9 shows the login process in PCCP-IAES system. User has to enter his/her user name and password which they had already entered while registration into the system. After clicking on next button one image will displayed in front of user and user has to click on the image thrice.

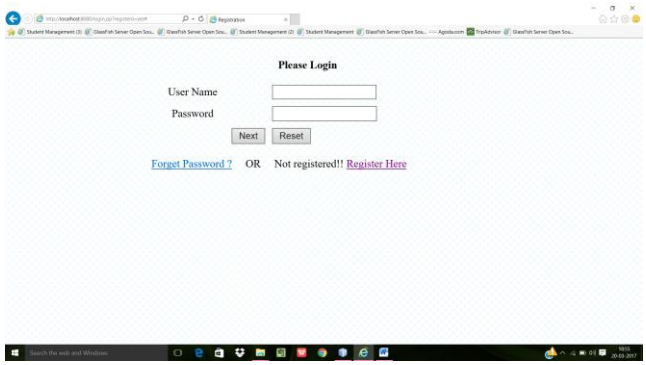

Figure 9: Login Page of PCCP-IAES

F) IAES Is Applied to Encrypt Text Password: Figure 10 shows the encrypted text password and the encrypted x and y coordinates of the click points.

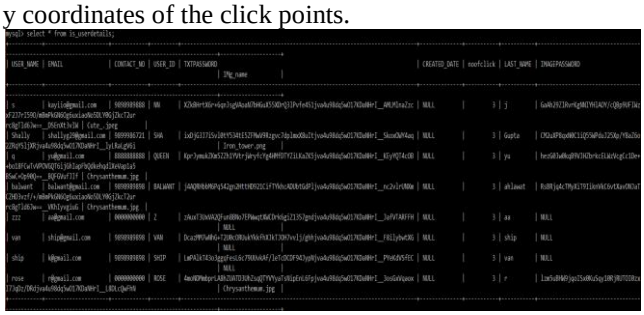

Figure 10

V. RESULTS

The Table1 shows the comparative study of PCCP, PCCPAES and PCCP-IAES. Login time of PCCP is more as compared to PCCP-IAES. By adding the salt key with AES the number of combinations of attack get increases. Login time of PCCP is less as compared to PCCPAES. As the AES is difficult to apply on images it is taking more time to apply on image. PCCP with Improved AES is taking 30.9 milliseconds for login in the system. Instead the PCCP takes 31.9 seconds for login. Approximately 1.0 milliseconds less time taken by the PCCP-IAES. As the time taken by the PCCP-IAES is 1.0 milliseconds less than the PCCP. This system also provides the more complex combination to attack on the system. The complexity increases approximately 8.6769e+40. It means user has to try 8.6769e+40 times more trials to attack on the system. PCCP with Improved AES is taking approximately 11 milliseconds less time than the existing PCCP technique. The total time for password authentication is 82.6 milliseconds in PCCP but in PCCP-IAES it is 71.1 milliseconds.[1]

Table1 Comparison of PCCP, PCCPAES and PCCP-IAES

Methods / Time (ms) →	Create Time	Login Time	Confirm Time	Total Time
PCCP	50.7	16.2	15.7	82.6
PCCP + AES	24.2	22.1	12.4	58.7
PCCP + IAES	40.2	15.9	15	71.1

VI. CONCLUSION

By adding the features of Persuasive Cued Click Points with Improved Advanced Encryption Standard achieves the better results in authentication system as compare to the PCCP & Advanced encryption standard. Graphical authentication scheme is better to remember for the user. As user has to choose only one image for the authentication purpose it is easier for the user to remember and difficult for the attacker to attack because it is difficult for the attacker to see at click points area of the image. The complexity of the PCCP with IAES is increased but the combinations to attack on the system also increases. As in this, system are providing two ways for the image selection by the users, so one more new option can provide to the users to use web cam to capture his/her own pictures at the time of registration.[1]

VII. REFERENCES

[1] Smita Chaturvedi, Rekha Sharma, "Securing text & image password using the combinations of Persuasive Cued Click Points with the help of Improved Advanced Encryption Standard, International Conference on Advanced Computing Technologies and Applications(ICACTA-2015).

[2] Smita Chaturvedi, Rekha Sharma, "Securing text and image password using the combinations of Persuasive Cued Click Points with Advanced Encryption Standard" (2014,Aug).

[3] BINITHA .V .M. ," Persuasive Cued Click Based Graphical Password with Scrambling For Knowledge Based Authentication Technique with Image Scrambling " IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 2 (Jul. - Aug. 2013), PP 14-24 www.iosrjournals.org

[4] Dimitri Van De Ville, W.P., Rik Van de Walle, Ignace Lemahieu, Image Scrambling Without Bandwidth Expansion. IEEE Transactions on Cirsuits and Systems for Video Technology, 2004. 14.

[5] Jisha Anna Alex, Sheena Anees, A.Neela Madheswari," User Authentication Based On Persuasive Cued Click Points with Sound Signature", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 3, No.5, October 2013.

[6] Hamdan. O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. AI-Nabhani , "New Comparative Study Between DES, 3DES and AES within Nine Factors," Journal of Computing,vol.2, no.3,pp.1003-4085,2010.

[7] http://security.stackexchange.com/questions/48000

[8] http://security.stackexchange.com/questions/48000

[9] http://en.wikipedia.org/wiki/Salt_%28software%29

[10] S. Chiasson, Elizabeth Stobert, Alian Forget, Robert Biddle, and P.C. van Oorschot, "Influencing users towards Better Passwords: Persuasive Cued Click Points," InProceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction,vol.1,pp.121-130,2008.
[11] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle,"Multiple password interference in text and click-based graphical passwords," in ACM Computer and Communications Security ,2009.
[12] Davis, Darren, Fabian Monrose, and Michael K. Reiter, "On User Choice in Graphical Password Schemes," In USENIX Security Symposium, vol.13,pp.11-11,2004
[13] Paul C van Oorschot Amirali Saheli-Abari and Julie Thorpe,"Purely Automated Attacks On Passpoints Style Graphical Passwords,"IEEE Transaction On Information Forensics and Security,Vol.5,No.3,pp 393-405,2013.
[14] P.R. Devale Shrikala M. Deshmukh, Anil B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme,",2013.
[15] S.Chiasson, P. Van Oorschot, and R. Biddle,"Graphical Password Authentication Using Cued Click Points," Pro c.European Symp. Reseacrh in Computer Security ESORICS, pp.359-374,2007.
[16] E. Stobert ,A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," In Proceedings of the 26th Annual Computer Security Application Conference,pp.79-88,2013.
[17] S. Chiasson , A. Forget, R. Biddle, and P.C. avn Oorschot , "User interface design affects security: Patterns in click-based graphical passwords," International Journal of Information Security Springer, vol.11, no.6, pp.387-398,2009.
[18] J.Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in Security and Usability: Designing Secure Systems That People Can Use, L.Cranor and S. Garfinkel, pp.129-142,2005.
[19] L.O' Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol.121, no.12,pp.2021-2040,2003.