Cued Click Points Password Authentication using Picture Grids

[1] R. Shantha Selva Kumari, [2] S.Viji

[1] Professor and Head, Department of Electronics & Communication
Mepco Schlenk Engineering College, Sivakasi, India

[2] PG Student, Department of Electronics & Communication
Mepco Schlenk Engineering College, Sivakasi, India

Abstract – The main issues of knowledge-based authentication is Users tend to choose memorable passwords that are easy for attackers to guess but strong passwords are difficult for users to remember. An important usability goal for authentication system is to support users in selecting better passwords, thus increasing security by expanding the effective password space. This paper proposes Picture passwords, which are an alternative to alphanumeric passwords, in which users click on images/grids to authenticate themselves. Users click on one point per image for a sequence of images. The next image will be based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. We suggest that Cued Click Points (CCP) provides greater security because the number of images increases the workload for attackers. While increasing the number of images and number of grids the security and efficiency will be very high.

Keywords - *Password, Pass Points, Click Points, Image, Picture Password, Cued Click Point (CCP).*

1. Introduction

People always select predictable passwords. This occurs with text based and graphical passwords. There are two types of difficulties of remembering text passwords. They are easy to remember and hard to guess. If the password is easy to remember, it will be easy to guess. On the other hand, if the password is hard to guess, it will be hard to remember also Users tend to write passwords down or use the same passwords for different accounts [1]. Other methods are also available nowadays, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raises the privacy concerns and smart cards usually need a PIN because cards can be lost. Hence, passwords are still dominant and are expected to continue to remain so for some time. Many problems of users with alphanumeric passwords are related to memorability of secure passwords. To create more unforgettable passwords, graphical password systems have been devised. Graphical password authentication is based on clicking on the image rather than typing alphanumeric strings. we proposed a new click-based graphical password scheme called Cued Click Points [8]. A password consists of one click-point per image for a sequence of images. The next image displayed is based on previous click point so users receive immediate implicit feedback as to whether they are on the correct path or not, when they are logging in. Users had high success rates, could quickly create and re-enter their passwords, and very accurate when entering their click-points.

A preliminary security analysis of this new scheme is also presented. Hotspots (i.e. areas of image that users have to select) are a concern in click-based passwords, so CCP uses a large set of images that will be difficult for attackers to obtain. The hotspot analysis requires proportionally more effort by attackers, as each image must be collected and analyzed separately. CCP appears to allow greater security; the work load for attackers of CCP can be randomly increased by augmenting the number of images in the system. As with most graphical passwords, CCP is not planned for environments where shoulder-surfing is a serious threat.

The following section briefly describes the need of Picture Password, Types of Picture password, Other method of Recognition based Techniques, Password Authentication using Picture Grids, how to improve security in Picture Password System and Security. Finally we provide the discussion of results.

2. Problems in Text Passwords

Text passwords are the most predominant user authentication method, but have security and usability problems [2] [3]. A user can forget a password that is not used regularly, as the memory is not “refreshed” or “activated” sufficiently often. When users have different passwords, today practically a universal condition, interference becomes a possibility. The user may either shuffle the elements of the different passwords or remember the password but confuse which system it corresponds to.

Users normally manage with password memory problems by decreasing the complexity and number of passwords, thereby reducing the security of password. A secure password should be 8 characters or longer, random, with upper case and lower case characters, symbols and digits. Such passwords lack meaningful content and can be learned only by habitual memorization or by a weak way of remembering. Generally, users ignore such password recommendations, using instead tiny, simple passwords that are relatively easy to track down using dictionary attacks [10] or attacks based on the knowledge of user.

3. Proposed Work

3.1 Password Authentication using Pictures

Why Picture Password: Recent surveys have shown that users often choose, short, alphabetic only passwords consisting of personal names of family or friends, pet names, and even the word “password”. Users typically write down their passwords, share their passwords with others, and use the same password for multiple systems, sometimes with a single digit added on the end. While hard password practices may be largely attributed to memory problems, there are other factors as well. Hence Picture password systems have been devised.

Most picture password systems are based on either recognition or cued recall. In recognition-based systems the user must recognize the image that is previously chosen from a larger group of distracted images. In cued recall password systems users must click on the areas of previously chosen in an image, cued by viewing the image. Both types of systems may have memory advantages compared to alphanumeric passwords. Alphanumeric passwords are based on pure recall method. Furthermore, psychological studies show that images are recognized with very high accuracy after two hours delay, which gives more accuracy than words and sentences.

3.2 Types of Picture Password

Pass Points system (see fig.1): In Pass Points [4], a password consists of a sequence of five click-points on a given image. Users may select any grid as click-points in an one image for their password. To log in, users should repeat the sequence of clicks in the correct order on that image. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build dictionary attack and more successfully guess Pass Points passwords.

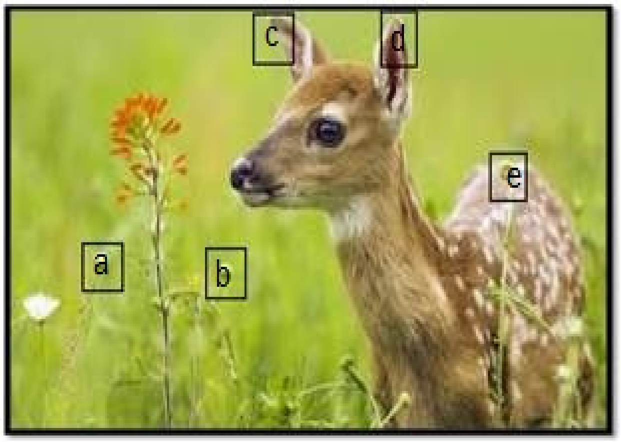


Fig.1. Pass Points in Picture

A dictionary attack consists of using a list of potential passwords and trying each on the system in turn to see if it leads to a correct log in for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

Other method of Recognition based Techniques (see fig.2): To create a password the user chooses nine images of human faces from a large of faces. When log in, the user sees a 3x3 grid with nine faces, consisting of one face previously chosen by the user and nine decoy faces. The user must recognize and click anywhere on the previously selected face. This procedure will be repeated with different target and decoy faces, for a total of four rounds. Only if the user chooses all three or four correct faces, according to our settings, will he or she successfully log in. However, the drawbacks of all such passwords are based on image recognition, which displays only small number of images, e.g., nine images, one of which is a selected image.

To get security similar to that of 8-character alphanumeric password, 15 or 16 rounds with more faces each would be required. This could make the log in slow and tedious.

Fig. 2: Other method of Recognition based Techniques

4. Password Authentication using Picture Grids

Rather than five click-points on one image (Pass Point systems), Cued Click Point (CCP) uses one click-point on five different images [5]. The next image will be displayed which is based on the location of the previously entered click-point (see Figure 3), creating a path through a set of images. Users select their images only to the extent that their click-point determines the next image. To create new password users uses the different image sequence with different click-points.

The claimed advantages are that password entry becomes a method of true cued recall type, wherein each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is not a requirement on user, as the system presents the images one at a time. CCP also provides a feedback of implicit, which is claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

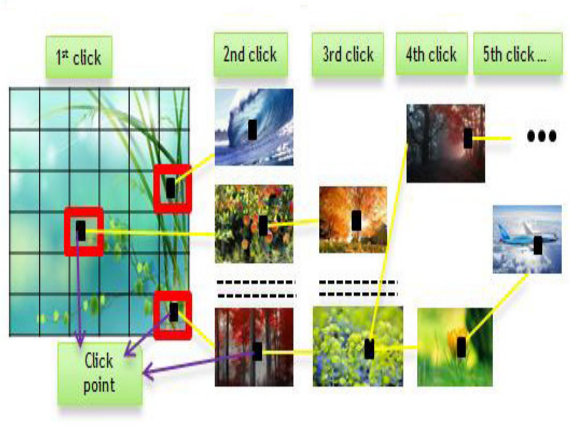


Fig. 3: Password Authentication using Pictures

4 .1 System Module

The designed system consist of two modules such as picture selection module and system log in module (see Figure 4)

In picture selection phase there are two ways for selecting the picture.

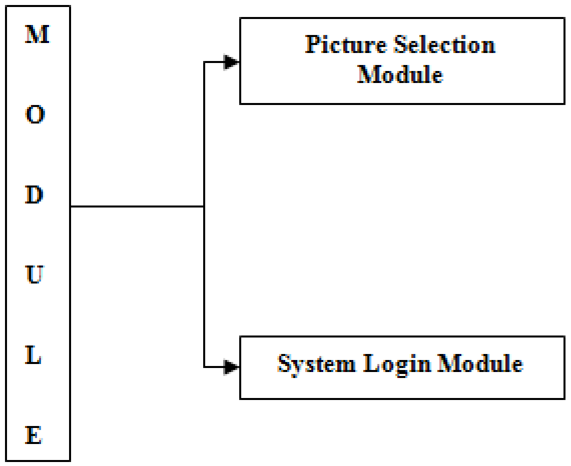


Fig. 4: System Module

1. User defined pictures: Pictures or images are selected or derived from hard disk or user supported devices.
2. System defined pictures: Pictures are selected by the user from the database of the password system.

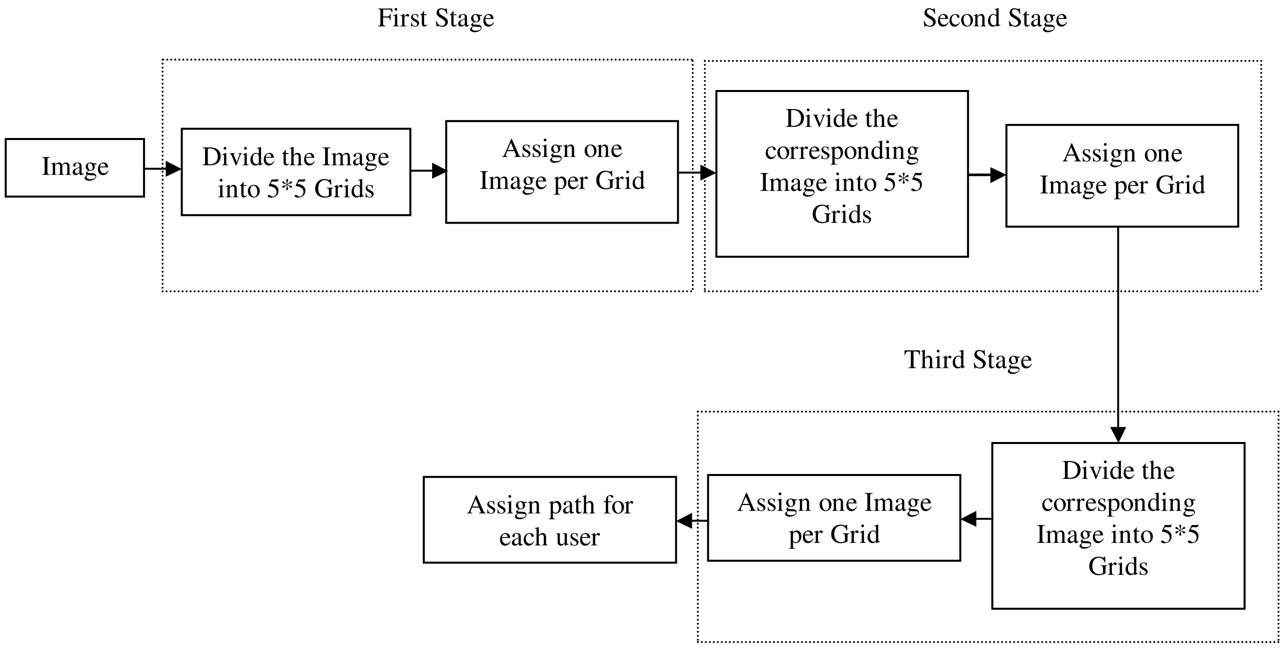

First Stage
Second Stage
Image
Divide the Image into 5*5 Grids
Assign one Image per Grid
Divide the corresponding Image into 5*5 Grids
Assign one Image per Grid
Third Stage
Divide the corresponding Image into 5*5 Grids
Assign one Image per Grid
Assign path for each user

Fig. 5a: Block Diagram for Picture Selection Module

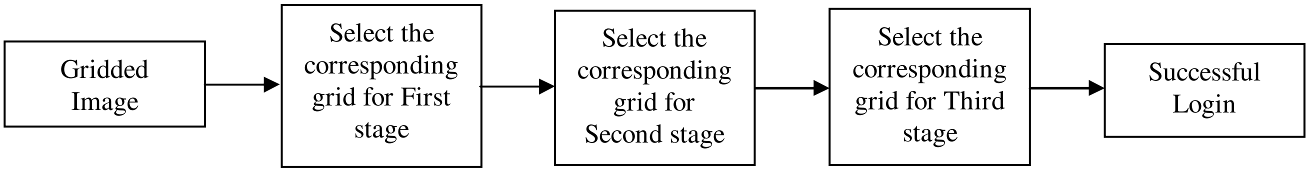

Gridded Image
Select the corresponding grid for First stage
Select the corresponding grid for Second stage
Select the corresponding grid for Third stage
Successful Login

Fig. 5b: Block Diagram for Picture Selection Module

In picture selection phase (Fig.5a & 6a) user select sequence of images and select one click-point on each image for password settings. Users must select a click-point within the view port. The requirement level of Security (*K)* defines the number of images used for the authentication. For the first image, it is split into specified number of grids then the image is assigned for each and every grid. This process will be repeated until the requirement level of Security (*K*) has been achieved. Then the path will be assigned for each user as password.

During system log in (See Fig. 5b & 6b), the images are displayed normally, without shading or viewport, and repeat the sequence of clicks in the correct order, within an original click-point grid.

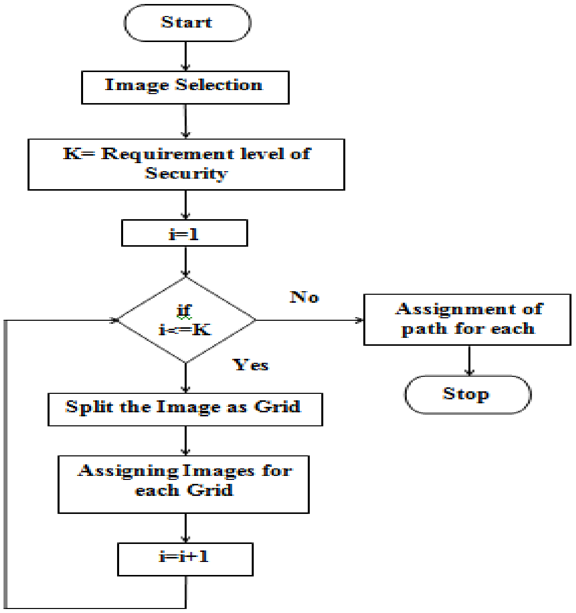

Start
Image Selection
K= Requirement level of Security
i=1
if i<=K
No
Yes
Assignment of path for each
Stop
Split the Image as Grid
Assigning Images for each Grid
i=i+1

Fig. 6a: Flow Chart for Picture Selection Module

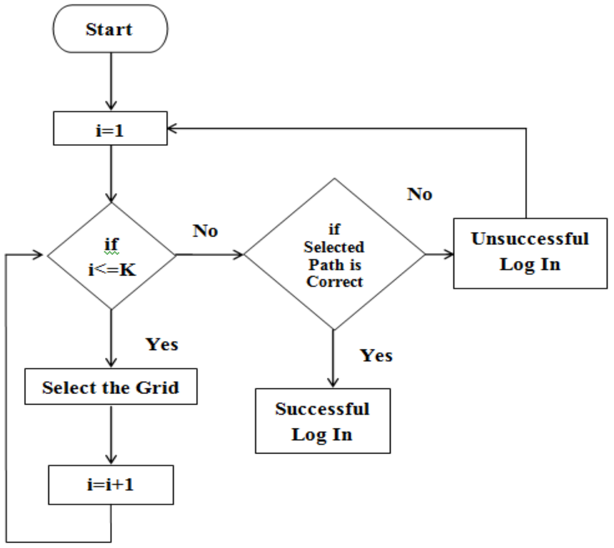


Fig. 6 (b): Flow Chart for System Log In Module

4 .2 Procedure

Step 1: Select the image sequences and divide each image into equal number of grids (equal number of rows and columns) for password settings.

Step 2: Assign different images for each grid and divide it by number of grids.

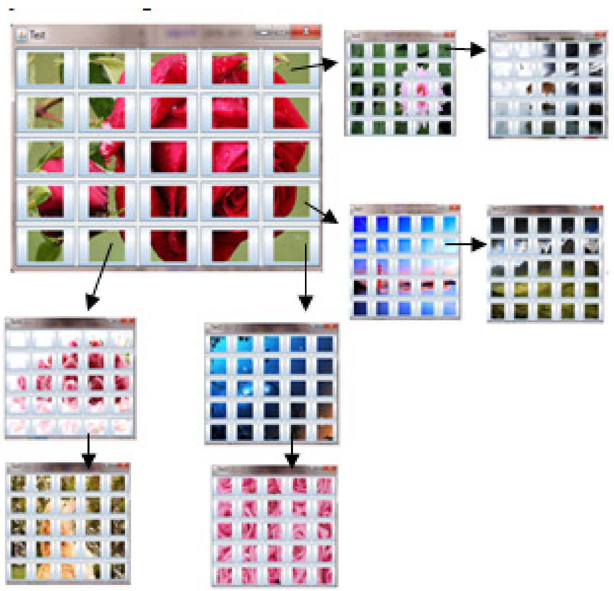


Fig. 5: Image sequences for each grid

Figure 5 combines step1 and step 2. The first image is divided into 25 equal of grids and image sequences are arranged for each grids are shown. Figure 5 shows image sequences are arranged for 5th, 20th, 22nd and 25th grid for first image. Similarly image sequences are arranged for all the grids.

Step 3: Assign correct path for successful log in
Step 4: Also assign remaining path for unsuccessful log in

5. Result

The proposed method for the Click based Password Authentication using Picture Grids for computers was implemented using Java. The Input image (figure 6) is first splitted into equal number of rows and columns for password settings. Here the image is splitted into 5 rows and 5 columns. Here we have created the password for 25 users.

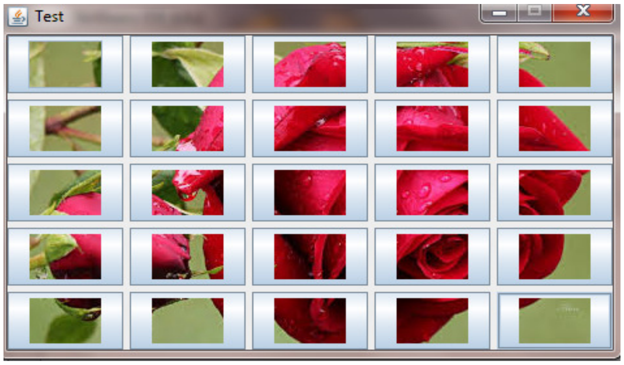
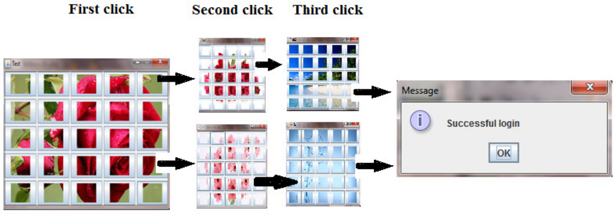


Fig. 6: Splitted image

To log in, there are 3 click points. That is one click point for each image. To create password for 25 users we have to select separate path for each user.

Assign image path for each grids for three steps. Sequentially there are 3 images. Here the figure 7 and 8 shows passwords for 2 users. Two users have different path to log in successfully. Also, each image split into 5*5. Figure 7 show the correct path to log in successful

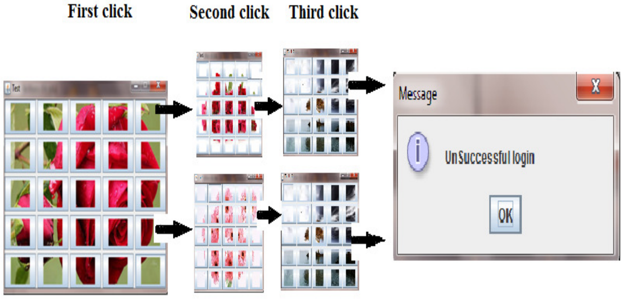


Successful login

Fig. 7: correct path to reach destination

Figure 7 shows the password settings for 5th and 20th users. That is here we have assigned each grid for each user (grid 1 for 1st user, grid 2 for 2nd user, and so on). 5th user have to select 5th grid in the first image (first click), 10th grid in the second image (second click) and 20th grid in the last image (third click) to log in successfully. Similarly, 20th user have to select 20th grid in the first image (first click), 20th grid in the second image (second click) and 15th grid in the last image (third click) to log in successfully. If they select wrong grid (path) he/she cannot log in correctly.

Figure 8 show that when an unauthorized user access the system he cannot log in correctly.



UnSuccessful login

Fig. 8: Incorrect path

Figure 8 shows the wrong path for the same users (5th and 20th users). Here 5th user has selected 5th grid in the first image (first click), 15th grid in the second image (second click) and 10th grid in the last image (third click). Hence they cannot log in correctly. Similarly, 20th user has selected 20th grid in the first image (first click), 10th grid in the second image (second click) and 15th grid in the last image (third click). From this we inferred that, even we select the wrong grid it will not terminate the path. It just go up to last image and finally it shows “unsuccessful login”. Hence attackers cannot identify the correct path.

Table 1: Comparison between No. of users and their Efficiency and Security Level

Number of Users	Number of Image Sequences	Efficiency in %	Computation Time	Efficiency
10	5	95	5 Sec	Low
15	6	98	6 Sec	High
25	8	100	8 Sec	Very High

The table 1 shows, while increasing the number of users and number of image sequences, the security level will be very high but time more consuming. Also, time consuming depends on various users. If their operating time is high, their consuming time will be low. Otherwise, it takes long time to log in. Also, it depends upon the system speed.

6. Make Picture Password System More Secured

a. The security of this system depends on the number of grids. As the number of grids increases, we can choose several paths. Thus, making the system highly secured.
b. Avoid hotspots on the picture while selecting click point.
c. Choose minimum 3 pictures or maximum 5 pictures of this password system. As no. of pictures increases, the password becomes that tight.

7. Conclusion

Picture passwords are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e. it is easy to remember & it is hard to guess. By the solution of the shoulder surfing problem, it becomes more secure & easier password scheme. By implementing encryption algorithms and hash algorithms for storing and retrieving pictures and points, one can achieve more security Picture password is still immature, more research is required in this field. While increasing the number of images and number of grids the security will be very high and the efficiency will be 100%.

References

[1] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[2] L. O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[3] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[4] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int"l J. Human-Computer Studies, ol. 63, nos.1/2, pp. 102-127, 2005.

[5] Iranna A M, Pankaja patil, " graphical password authentication using persuasive cued click point ", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEI), Vol. 2, Issue 7, July 2013.

[6] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), July 2008.

[7] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April 2012.

Authors Profile

R. Shantha Selva Kumari received her BE degree in Electronics and Communication Engineering from Bharathiyar University, in 1987 and MS degree in Electronics and Control from Birla Institute of Technology, Pilani, in 1994. She completed her PhD degree in Biosignal Processing in 2008 from Manonmanium Sundaranar University, Tirunelveli. She has 28 years of teaching experience and is currently working as Professor and Heading the Department of Electronics and Communication Engineering at Mepco Schlenk Engineering College, India. Her current research interest includes signal processing, wavelets and its applications, neural networks. She is a life member in ISTE, FIETE and CSI.

S. Viji received her BE degree in Electronics and Communication Engineering from Kalasalingam Institute of Technology, in 2013 and doing ME in Communication Systems from Mepco Schlenk Engineering College (2014-2016).