COUNT BASED HYBRID GRAPHICAL PASSWORD TO PREVENT BRUTE FORCE ATTACK AND SHOULDER SURFING ATTACK

M. Ezhilarasan[1], D. Dhanabharathi[2], P. Vasanthakumar[3], B. Ayyanar[4]

[1]Professor, Department of Information Technology, Pondicherry Engineering College, Puducherry, India
[2]Final Year Student, Department of Information Technology, Pondicherry Engineering College, Puducherry, India
[3]Final Year Student, Department of Information Technology, Pondicherry Engineering College, Puducherry, India
[4]Final Year Student, Department of Information Technology, Pondicherry Engineering College, Puducherry, India

Abstract

Graphical passwords are more secure and resistant to dictionary attacks when compared to textual passwords, but they are not fully resistant to shoulder surfing and brute force attacks. Usually users tend to set their graphical password short and simple for usability but the problem here is their security is compromised. Another problem in graphical password is most of the graphical passwords contain hotspots and the users are tempted to set the graphical password with the hotspots by which attackers easily guess the password. In this work we have proposed a hybrid graphical password system. In our system, we have increased the password space by proposing count based click point algorithm in recognition based graphical password to make the system resistant to brute force attack. In the recall based graphical password step of our hybrid graphical password, we have included a gesture based password which makes the attacker difficult to record or observe and reproduce it to bypass the security.

Keywords: *Brute force attack, Gesture, Graphical passwords, hotspots, Password space, shoulder surfing attack, textual password*

---***---

1. INTRODUCTION

Authentication is important for every system to make it secure; it plays a major role from high secure applications to less secure applications. It is important to secure the information exchanges from daily transactions to daily user email account. The most critical issue in today's world is providing security in applications such as military and ATM centers which need high security. When it goes to most secure methods, it requires more time and more bandwidth. Applications can be classified as applications which need less security (user held devices) and applications which need more security (ATM centers). Tightening the security for the first type is unnecessary and waste of time for the user and also leaving a weak password for the second type is dangerous.

Popular text based passwords provide security to some extent but they are easily vulnerable to dictionary and brute force attacks though they are short and simple to remember. The biometric authentication system is most secure form of authentication but the cost of the device to authenticate the user is very high. The graphical password came into picture which is more secured than text based graphical password and easy to remember. Most of the system such as mobile devices and latest operating systems use graphical password as a mode of authentication. Pattern lock is the famous example of graphical password in smart phones.

But the most notable problem with graphical passwords is that they are vulnerable to shoulder surfing attack and brute force attack. Many graphical passwords were proposed to eliminate shoulder surfing attack and brute force attack [1] but most of the existing graphical passwords failed to prevent these two attacks.

Shoulder surfing attack [2] is the process of recording or observing the password when the user inputs and reproducing it to break the security system. Since graphical passwords are mostly click type rather than typing it is more vulnerable to shoulder surfing attacks. Graphical passwords are also easier to guess [2], [3]. Most of the graphical passwords that were proposed till now have not eliminated shoulder surfing attack since it can be easily recorded and reproduced or easily guessed.

Existing graphical passwords produce a feedback that indicates the user pattern or user clicks of the graphical password which can be recorded and reproduced, hence our system differs from existing system by using point counts as criteria that is resistant to shoulder surfing attack even if it recorded. And in our system we have increased the password space with that point count to make it resistant to brute force attack.

The key components of our approach are point count and gesture, it is a hybrid system with two steps of graphical password, one with recognition based with point count and the other is recall based graphical password with gesture; so they both combine to prevent brute force and shoulder surfing attack respectively.

Our paper is organized as follows, Section 2 contains the related work, Section 3 contains our Proposed system with module description, Section 4 contains the Methodologies, Section 5 contains the Empirical Results and Analysis and the Section 6 contains the Conclusion and future work followed by the References.

2. RELATED WORK

Increase in use of computers has paved way for many security concerns. Authentication is the major security concern which refers to the process of determining whether someone or something is, originally, who or what it is declared to be.

Authentication Techniques are classified as follows:

- Textual Passwords
- Biometric schemes
- Graphical Passwords

2.1 Textual Password

Textual password is a combination of alphabets and numbers but they are easily guessable [4]. Most frequently used passwords are text based passwords, but they had their own advantages and disadvantages. Textual passwords are advantageous since they are easy to use and faster to input the password. The disadvantages of textual password are, it is weak and not resistant to several attacks such as dictionary attack, spyware, guessing and brute force attack.

2.2 Biometric Password

Biometric authentication is the process of validating the user by the characteristics and traits which include fingerprint, iris, DNA, hand geometry, face and other human traits. Biometric authentication is the foolproof and the most secure form of authentication. But the disadvantage [5]-[7] of biometric is that it involves additional hardware costs and high deployment cost.

2.3 Graphical Password Authentication

A graphical password is an authentication system in which the user is presented with a set of images from which the user selects images or click points in the image, in some order during login phase, and the same points or images in the same order is repeated in the login phase also to authenticate the user. There are two types of graphical password recall based and recognition based. In Recall based password, the user is has to reproduce the same thing he created or selected in the registration phase of the system. In Recognition based password, the user has to identify the things he has done or selected during the registration phase and select the same by identifying in the login phase of the system. Since our work depends on the graphical passwords we will consider some of the notable graphical password techniques and their advantages and disadvantages.

2.3.1 Perrig and Song

Perrig and Song proposed Hash Visualization technique [8] which is recognition based graphical password. In this system the user will be presented with a set of random images and asked to choose them during the registration stage. Later the pictures will be randomized and the user must identify and select those images during the login stage to authenticate. This technique was able to perform better than textual password it is easy to remember this Hash visualization password than text based password. But the problem here is this technique was not able to prevent brute force attack, shoulder surfing attack and guessing attack.

2.3.2 Passface

Passface [9] is a technique similar to hash visualization technique but the difference here is that instead of using some random images Passface used faces. The user has to recognize and pick the registered faces during the registration stage. But this takes longer time than textual password. Advantage here is that faces are easier to remember. Still this technique was not able to prevent brute force attack and shoulder surfing attack.

2.3.3 Sobrado and Birget

Sobrado and Birget [10] proposed a graphical password technique in which the user has to select the pass objects from a large amount of objects available in a frame during the registration stage, during the login stage the objects are randomized to the user and the user has to identify and select them to pass the authentication. This technique was able to prevent shoulder surfing attack by randomizing but the problem is it can be guessed and this technique is vulnerable to brute force attack.

2.3.4 Draw-a-Secret (DAS)

Draw a secret [11] technique is a recall based technique in which user has to draw a symbol or a secret drawing in a grid displayed to the user, and this drawing or symbol has to be reproduced to be authenticated. The password space of DAS is more than textual password, but the problem here is it can be easily guessed and shoulder surfing attack is not prevented in this technique.

2.3.5 Persuasive Cued Click Point (PCCP)

PCCP [12] technique prevents the user from selecting easily guessable spot in the click based graphical passwords known as hotspots [13]-[14]. Only a random block of image is visible to user to set their graphical password. Hence it is difficult to guess the password in this technique. This method is a click based password [15] in which the user clicks points in a block of the picture and the same points must be clicked to authenticate the user. This method is advantageous than other graphical passwords because it is able to prevent guessing attack, but the shoulder surfing attack is not been prevented in this method.

Existing Graphical password limitations:

- Shoulder Surfing Attack and
- Brute force search Attack

We have concentrated in these two attacks because, till now these two attacks have not been eliminated in existing graphical passwords.

3. PROPOSED SYSTEM

Our proposed system is Hybrid graphical password system which is the combination of recognition based and recall based graphical password. We have designed a recognition based graphical password known as Count based click point algorithm in which the user has to click at some points in the picture, each point having a click count, the same process has to be reproduced in the login step to be authenticated. Gesture based graphical password is included in the second step of our system to prevent shoulder surfing attack. In this gesture based graphical password step when the user enters the password, the feedback is not shown in the screen so that it cannot be recorded or observed and reproduced by the attacker.

Our system has two steps, first step which is count based click point algorithm which increases the password space since each point will have any count and hence it prevents brute force attack. Second step which is a gesture based graphical password system in which the feedback is not visible when the user inputs the password and thus preventing shoulder surfing attack. The system design is explained in the below diagram with the modules.

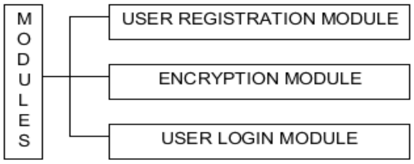


Fig -1: System Design

3.1 Registration Process

Fig. 2 shows the flowchart of registration process. During the registration stage, the user enters the username, and then he should browse a picture. Then the user has to select the tolerance [16] value (approximation of the deviation from the actual point) and also the total point count. Then the user clicks on multiple points in that picture until the total point count is not over with a freedom to click the same point multiple times which the individual point count. The user also has an option to reset the password if the desired password is not set by using the reset button. The position of the click point and the counts of each point are stored in the database. Now the user is mailed with the first step count based click point password with the count of each point and the point on the picture.

Next phase of registration is the gesture based recognition in which the user makes a single stroke gesture and the gesture is stored in a picture format. While the user makes the gesture it is difficult for the attacker or the camera to observe or record it and reproduce it to crack the password. Hence this gesture password addresses the shoulder surfing attack.

In the registration phase of our hybrid graphical password system we have also included an alert mail system. The email id of the user is got at the registration stage itself so that in case of invalid login attempts the user is intimated with the email. And also we have included a password reset feature with the security question that is also got during the registration phase of the Hybrid graphical password system which is asked in the password reset phase to the user.

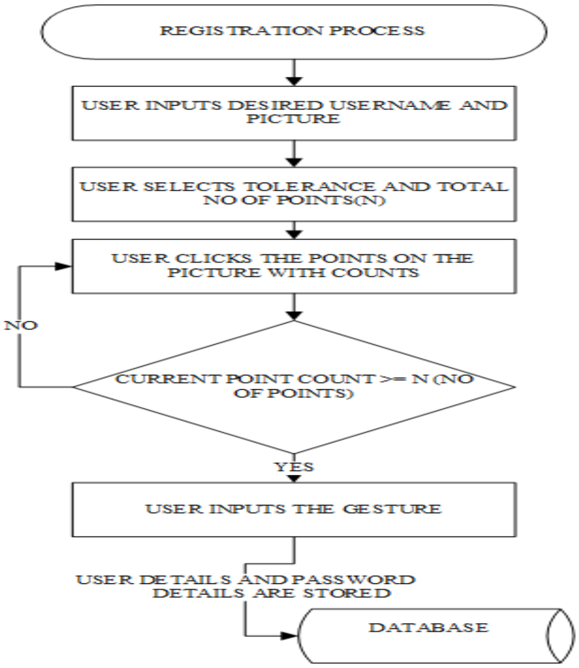

REGISTRATION PROCESS
USER INPUTS DESIRED USERNAME AND PICTURE
USER SELECTS TOLERANCE AND TOTAL NO OF POINTS(N)
USER CLICKS THE POINTS ON THE PICTURE WITH COUNTS
NO
CURRENT POINT COUNT >= N (NO OF POINTS)
YES
USER INPUTS THE GESTURE
USER DETAILS AND PASSWORD DETAILS ARE STORED
DATABASE

Fig -2: Registration flowchart

3.2 Login Process

Fig. 3 shows the flowchart of login process. During the login process the user enters the username and the picture that was set by the user during the registration stage is automatically displayed. Now the user inputs the password by clicking the points on the picture with the count until the password is entered correctly. At any point or the count mismatches the user is taken out of login page and asked to renter. Now the points and the counts are matched with that points and count that has been recorded during the registration process. If they match the user goes to the next phase of login otherwise taken back to login phase again.

In the next phase of the login the user makes the single stroke gesture. Now the gesture is stored in image format. Now this login gesture image is compared with that of the gesture image that was made by the corresponding username during the registration phase. If this matches the user successfully passes the authentication system.

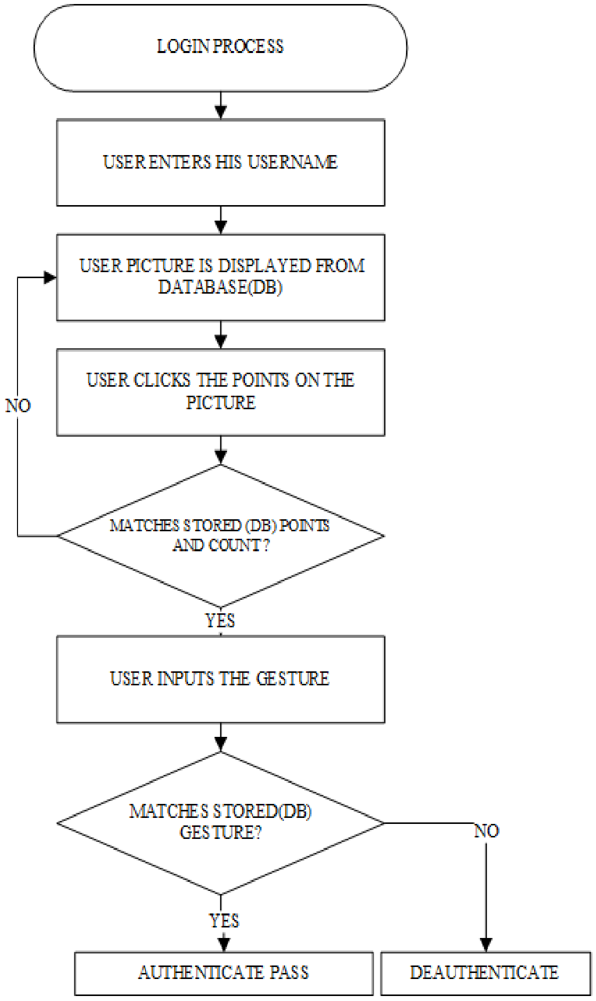

LOGIN PROCESS
USER ENTERS HIS USERNAME
USER PICTURE IS DISPLAYED FROM DATABASE(DB)
USER CLICKS THE POINTS ON THE PICTURE
NO
MATCHES STORED (DB) POINTS AND COUNT?
YES
USER INPUTS THE GESTURE
MATCHES STORED(DB) GESTURE?
NO
YES
AUTHENTICATE PASS
DEAUTHENTICATE

Fig -3: Login flowchart

3.3 Encryption

At the end of the registration process the username and its corresponding click points with their count and the gesture image are encrypted and stored. Then during the login process the above encrypted files are decrypted and matched to authenticate the user.

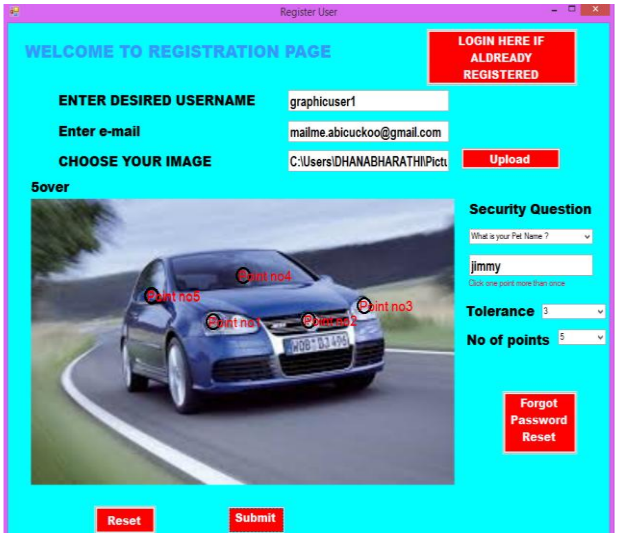
4. METHODOLOGIES

This section deals about the various algorithms and methodologies we have used for the count based graphical password system. This part is classified as three sections which are count based click point algorithm, gesture matching algorithm and encryption algorithm.

4.1 Count Based Click Point Algorithm

This is the first step of our Hybrid graphical password system. This algorithm works as follows: First the user decides the total number of points and then starts to record the points by clicking each point any number of times and till total points is reached. e.g. If total no of points is “5”, the user can click the first point “2” times, second point “2” times, third point “5” times, fourth point “2” times and fifth point “6” times. Then these points are recorded in the database along with the count and these points have to be repeated in the same order and same count during the login stage for the user to be authenticated.

Since the user cannot be accurate in the point of the picture he clicks always, an approximation function called “ClickpointApproximationfunction” has been introduced in which the tolerance can be modified according to the area of usage and the security level that needed.


Register User

WELCOME TO REGISTRATION PAGE

ENTER DESIRED USERNAME graphicuser1

Enter e-mail mailme.abicuckoo@gmail.com

CHOOSE YOUR IMAGE C:\Users\DHANABHARATHI\Pictu

5over

Security Question What is your Pet Name ?

jimmy

Click one point more than once

Tolerance 3

No of points 5

Fig -4: Screenshot of the Hybrid graphical password

Approximation Function for the Click Point Tolerance

```
ClickpointApproximationfunction(Point p0, Point p1)
{
   return (Math.Sqrt(((p00.X - p0.X) * (p00.X - p0.X)) +
   ((p00.Y - p0.Y) * (p00.Y - p0.Y))) <= tolerance);
 }
```

p0 – Point which was recorded during the HGP registration stage
p1 – Point which was recorded during the HGP login stage
X – x co-ordinate of the point
Y -- y co-ordinate of the point
Tolerance – parameter to set the level of approximation (radius of the circle within with the point is accepted) or the tolerance value for that point.

4.2 Gesture Matching Algorithm

This is the second step of our Hybrid Graphical Password system. In this step, gesture recognition is used to authenticate the user. First during the registration stage the user is asked to input a gesture and this gesture is recorded into the database. Then during the login stage the same gesture needs to be reproduced by the user to be authenticated. The gesture of the corresponding user is recorded into the database and during the login stage the recorded gestures in the database is used for authentication. If the gesture is wrong, the user is given an alert message through email stating that there was an illegal or wrong attempt into your account with the time of the wrong attempt was made in our Hybrid graphical password system to the user email address that was got and stored in database during the registration stage.

4.3 Encryption Algorithm

Encryption is necessary because the user details are stored in the database level and if there is a security exploit in the database level the user data is under trouble. Hence we have used TRIPLE DES Encryption algorithm at the database level to secure the data of the user. And also there is an alert system in our system which sends an alert mail to the user for every wrong attempt to his email.

5. EMPIRICAL RESULTS AND ANALYSIS

We considered mainly two parameters when comparing our system with the existing system. One is password space and the other parameter is security percentage with respect to different attacks with the graphical passwords.

5.1 Shoulder Surfing Attack Resistance with Different Tolerance Values

The experiment was carried out with 8 participants with 5 different images into account and considering 5 click points with multiple counts of each point. Different images were consisting of different objects and scenario in it. Each user were allowed to register a graphical password and asked to login. And also when the participant is allowed to enter the login phase, other participants were asked to stand behind them and observe the password which is entered by the participant. This process repeated for other participants too.

Table -1: Resistant To Shoulder Surfing Attack of HGP and PCCP

Sl. No.	Tolerance Value (10^{-1}) cm	Attacker success Rate	Security HGP (%)	Security PCCP (%)
1	5	2/8	75	12.5
2	4	0/8	100	37.5
3	3	0/8	100	62.5
4	2	0/8	100	75
5	1	0/8	100	100

From TABLE I. we can see that the mean success rate by shoulder surfing attack in our hybrid graphical password system is very less when compared to existing graphical passwords and PCCP [12].

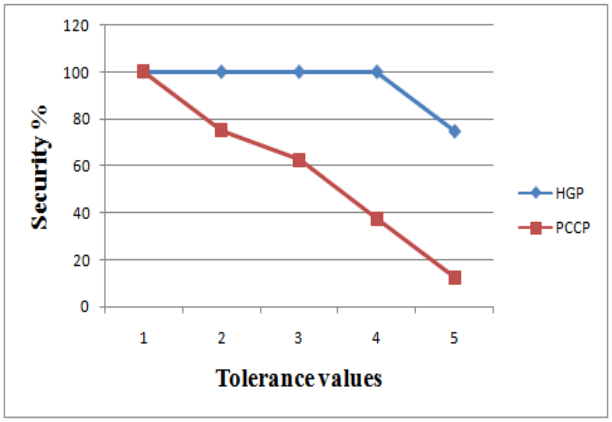


Chart -1: Comparison of security % between PCCP and HGP

Chart-1 shows, in Hybrid graphical password (HGP), the security decreases as the tolerance value increases. The mean Security percentage of our proposed system is 95% which is a significant improvement in the security of our hybrid graphical passwords over the shoulder surfing attack.

5.2 Brute Force Attack Resistance with Increased Password Space

Proposed Hybrid Graphical Password (HGP) shows increased password space when compared to other click based graphical passwords. Other existing graphical passwords showed maximum of N*M*P of click point N and M or dimensions of the picture and P is the picture count. But proposed Hybrid Graphical Password (HGP) System provided increased password space of (N*M) Count where N and M or dimensions of the picture, and Count represents count of each point.

5.3 Guessing Attack Resistance

Guessing attack is difficult to be performed in our proposed system since each point will have a count, even if the attacker figures out or guess the points the participant clicked in the picture he was unable to figure out the point count. Nearly out of 8 participants no one was able to guess the full password even if they were able to guess partial password.

5.4 Social Engineering Resistance

This attack is convincing the user to get the password by verbal description and the attacker re-performs the password to enter the system. Here the verbal description of the password is very tough since the exact point the user has clicked cannot be told verbally with their counts.

6. CONCLUSIONS AND FUTURE WORK

Shoulder surfing attack and brute force attack were the major threat to graphical passwords, and we were able to produce stronger graphical passwords by increasing the password space and using a unique count based click point algorithm. Hybrid Graphical password system was implemented and empirical results were observed and calculated their effectiveness over different attacks using a set of participants. We have obtained most desired results in security and also the usability of the system. Since the password space is improved in our count based hybrid graphical password system and hence our system can also be used for the most secure places like military and ATM applications.

Future improvement of Hybrid graphical password is that instead of using pictures for click points, usage of video will create a better and stronger password with more increased password space. Video consists of objects will vary for the frames which produces more security when compared to picture based graphical passwords.

REFERENCES

[1]. A. Salehi-Abari, J. Thorpe, and P. van Oorschot, “On Purely Auto-mated Attacks and Click-Based Graphical Passwords,” Prof Ann. Computer Security Applications Conf. (ACSAC), 2008

[2]. 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

[3]. P. C. van Oorschot and J. Thorpe. Exploiting predictability in click-based graphical passwords. Journal of Computer Security, 2011

[4]. J. Yan, A. Blackwell, R. Anderson, and A. Grant, “The Memorability and Security of Passwords,” Security and Usability: De signing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O‟Reilly Media, 2005

[5]. L. Jones, A. Anton, and J. Earp, “Towards understanding user perceptions of authentication technologies,” in ACM Workshop on Privacy in Electronic Society, 2007

[6]. L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication,”Proceedings of the IEEE, vol. 91, no. 12, December 2003

[7]. A. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” Transactions on Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125–143, 2006

[8]. 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

[9]. T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998

[10]. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002

[11]. P. Dunphy and J. Yan, “Do background images improve Draw a Secretgraphical passwords?” In 14th ACM Conference on Computer and Communications Security (CCS), October 2007

[12]. 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

[13]. S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. European Symp. Re-search in Computer Security (ESORICS), pp. 359-374, Sept. 2007

[14]. Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp. 2007

[15]. A. Salehi-Abari, J. Thorpe, and P. van Oorschot, “On purely automated attacks and click-based graphical

passwords," in Annual Computer Security Applications Conf. (ACSAC), 2008

[16]. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005

BIOGRAPHIES

Dr. M Ezhilarasan is the Professor, in the Department of Information Technology, Pondicherry Engineering College, Puducherry, India. He has completed his PhD and his Area of Specialization includes Multimedia Data Processing and Coding, MultiBiometrics

D Dhanabharathi is Final Year Student, in Department of Information Technology, Pondicherry Engineering College, Puducherry, India. His areas of interest includes Database, security, and data structures

P Vasanthakumar is Final Year Student, in Department of Information Technology, Pondicherry Engineering College, Puducherry, India. His areas of interest includes Database, security, and data structures

B Ayyanar is Final Year Student, in Department of Information Technology, Pondicherry Engineering College, Puducherry, India. His areas of interest includes OOPS, security, and data structures