Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices

Partha Pratim Ray

Department of CSE, Surendra Institute of Engineering and Management
Siliguri, West Bengal, India

***Abstract*— Passwords provide security mechanism for authentication and protection services against unwanted access to resources. One promising alternatives of textual passwords is a graphical based password. According to human psychology, human can easily remember pictures. In this paper, I have proposed a new hybrid graphical password based system. The system is a combination of recognition and pure recall based techniques and that offers many advantages over the existing systems and may be more convenient for the user. My approach is resistant to shoulder surfing attack and many other attacks on graphical passwords. This scheme is proposed for smart hand held devices (like smart phones i.e. PDAs, ipod, iphone, etc.) which are more handy and convenient to use than traditional desktop computer systems.**

***Keywords*— smart phones, graphical passwords, authentication, network security**

I. Introduction

Security system plays an important role in the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. In order to that computer systems and the information associated to them should also be protected. Computer security systems should consider the human factors such as ease of a use and accessibility, in this context. Current secure systems suffer because they mostly ignore the importance of human factors in security (Dhamija 2000). An ideal security system considers all four items such as security, reliability, usability, and human factors. Passwords are simply secrets that are provided by the user upon request by a recipient. They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists (Authentication 2011). Passwords are the most common means of authentication which do not require any special hardware. Typically passwords are strings of letters and digits (alphanumeric). Such passwords have the disadvantage of being hard to remember (Sobrado 2002). Weak passwords are vulnerable to dictionary attacks and brute force attacks where as Strong passwords are harder to remember. To overcome the problems associated with password based authentication systems, the researchers have proposed the concept of graphical passwords and developed the alternative authentication mechanisms. Graphical passwords (GP) systems are the most promising alternative to conventional password based authentication systems. GP use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters (Elftmann 2006). The idea of GP was originally described by Greg Blonder in 1996 (Blonder 1995). An important advantage of GP is that they are easier to remember than textual passwords. As human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration (theoretically until brain is strong). In this way graphical passwords provide a means for making more user-friendly passwords while increasing the level of security.

Besides these advantages, the most common problem with GP is the shoulder surfing problem: an onlooker can steal user's graphical password by watching in the user's vicinity. Many researchers have attempted to solve this problem by providing different techniques (Xiayuan 2005). Due to this problem, most GP schemes recommend small hand held devices (PDAs) as the ideal application environment. Another common problem with graphical passwords is that it takes longer to input graphical passwords than textual passwords (Xiayuan 2005). The login process is slow and it may frustrate the impatient users. The exploitation of smart phones like ipod, iphone and PDA's is increased due to their small size, compact deployment and low cost.

In this paper, considering the problems of text based password systems, I have proposed a novel graphical password scheme which has desirable usability for small hand held devices. My proposed system is new GP based hybrid system which is a combination of recognition and pure recall based techniques and consists of two phases. During the first phase called Registration phase, the user has to first select his username and a textual password. Then a number of objects are shown to the user to select from them as his graphical password. After selecting few objects, the user has to give digits (0-9) as same number as of the objects selected (one for each object). During the second phase called Authentication phase, the user has to give his username and textual password and then give his graphical password by selecting the objects shown and providing the digits in the same way as done during the registration phase. If digits are entered correctly the user is authenticated and only then he/she can access his/her account. For practical implementation of our system we have chosen i-mate JAMin smart phone which is produced by HTC, the Palm Pilot, Apple Newton, Casio Cassiopeia E-20 and others which allow users to provide graphics input to the device. It has a display size of 240x320 pixels. The implementation details are out of the scope of this paper.

The structure of my paper is organized as follows. In section II, the classification of all existing authentication methods is described. In section III, all existing GP based schemes are classified into three main categories. Section IV reviews existing research and schemes which are strongly related to our work. In section V my proposed system is described in detail. In section VI we have compared our proposed system with existing schemes by drawing out the flaws in existing schemes. Finally section VII concludes the paper.

II. Classification of Authentication Methods

Authentication has become mere important for an organization to provide an accurate and reliable means of authentication (Khan 2007). The authentication methods can be divided into three major parts, such as Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication (Approaches 2011).

A. *Token Based*

It is based on "Something You Possess". For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allow them to fetch a specific resource - without using their username and password. After obtaining the token, the user can offer the token - which in turn offers access to a specific resource for a time period - to the remote site (Token 2011), while some use knowledge based techniques to enhance security (Approaches 2011). Two types of token based authentication methods are as follows.

- Passwords
- Pin number

B. *Biometric Based*

Biometrics is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits (Biometric 2011). It uses physiological or behavioral characteristics like fingerprint or facial scans and voice recognition or iris to identify users. A biometric scanning device takes a user's biometric data, such as fingerprint scan, and converts it into digital information a computer can interpret and verify. Biometric identification depends on computer algorithms to make a yes/no decision. The different types of biometric authentication methods are as below.

- Contact metric technologies
  - Finger print
  - Hand/Finger geometry
  - Dynamic signature verification
  - Keystroke dynamics
- Contact less technologies
  - Facial recognition
  - Voice recognition
  - Iris scan
  - Retinal scan

C. *Knowledge Based*

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords (Approaches 2011). Knowledge-based authentication (KBA) is based on "Something You Know" to identify you, such as Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question (Knowledge 2011). KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval and offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics (Kba 2011). It can be divided into three sub types as follows:

- Recognition based systems
- Recall based systems
- Cued recall based systems

III. Classification of GP Based Systems

GP schemes can be broadly classified into four main categories. Detailed classification of systems involved in these four categories as follows:

A. *Recognition Based System*

which are also known as Cognometric Systems or Searchmetric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. The proposed works in this regards are summarized as below:

- Cognitive authentication (Weinshall 2006)
- Use your illusion (Hayashi 2008)
- Story (Davis 2004)
- Déjà vu (Dhamija 2000)
- PassFace (Realusr 2011, Passfaces 2011)
- VIP (Angeli 2005, Moncur 2007)
- Photographic authentication (Pering 2003)
- Convex Hull Click (Wiedenbeck 2006)
- GPI/GPS (Bicakci 2009)
- Picture Password (Jasen 2003)

B. *Pure Recall Based Systems*

which are also known as Drwanmetric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Few works are given below:

- Android screen unlock (Tafasa 2011)
- GrIDsure (Gridsure 2011)
- PassShapes (Weiss 2008)

- DAS (Jermyn 1999)
- BDAS (Dunphy 2007)
- PassGo (Tao 2006)
- YAGP (Gao 2008)
- Haptic Password (Orozco 2006)
- Passdoodle (Goldberg 2002, Varenhorst 2004)

C. *Cued Recall based systems*

which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Several works are as below:

- Jiminy's scheme (Renaud 2004, 2001)
- Suo's scheme (Suo 2006)
- PassPoints (Wiedenbeck 2005, 2005, 2005)
- PassFace (Realusr 2011, Passfaces 2011)
- CCP (Chiasson 2007)
- PCCP (Chaisson 2008)
- Inkblot authentication (Stubblefield 2004)
- 3D scheme (Alsulaiman 2006)
- Passlogix (Passlogix 2011)

D. *Hybrid systems*

which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes. The scheme is studied by researches as below:

- CDS (Gao 2010)
- Two Step Authentication (Oorschot 2009)
- GP based systems for small mobile devices (Khan 2011)
- My proposed system: Ray's Scheme

IV. Related Work

(Khan 2011) proposed a scheme for small mobile devices which takes drawing as input in authentication phase. The input is given by mouse or stylus according to the objects (pictures) selected by user priori in registration phase. (Gao 2010) proposed and evaluated a new shoulder-surfing resistant scheme called Come from DAS and Story (CDS) which has a desirable usability for PDAs. It requires users to draw a curve across their password images (pass-images) orderly rather than click directly on them. This scheme adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users to draw a curve across their password images (pass-images) orderly rather than click directly on them. The drawing method seems to be more compatible with people's writing habit, which may shorten the login time. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shoulder surfing.

(Oorshot 2009) proposed a hybrid authentication approach called Two-Step. In this scheme users continue to use text passwords as a first step but then must also enter a graphical password. In step one, a user is asked for her user name and text password. After supplying this, and independent of whether or not it is correct, in step two, the user is presented with an image portfolio. The user must correctly select all images (one or more) pre-registered for this account in each round of graphical password verification. Otherwise, account access is denied despite a valid text password. Using text passwords in step one preserves the existing user sign-in experience. If the user's text password or graphical password is correct, the image portfolios presented are those as defined during password creation. Otherwise, the image portfolios (including their layout dimensions) presented in first and a next round are random but respectively a deterministic function of the user name and text password string entered, and the images selected in the previous round.

V. Rays' Scheme: My Proposed System

I have proposed a hybrid system for authentication and have given the name Ray's scheme. This hybrid system is a mixture of both recognition and recall based schemes. Ray's scheme is an approach towards more reliable, robust, user-friendly and secure authentication. I have also reduced the shoulder surfing problem to some extent.

Working of Ray's Scheme: My proposed system comprises of 3 steps out of which steps 1-2 are registration steps and step 3 is the authentication step. Graphical representation of my scheme is shown in Figure 1.

- *Step 1:* The first step is to type the user name and a textual password which is stored in the database. During authentication the user has to give that specific user name and textual password in order to log in.
- *Step 2:* In this step, objects are displayed to the user and he/she selects minimum of four objects from the set and there is no limit for maximum number of objects. This is done by using one of the recognition based schemes. Specific digits (0-9) are to be selected then by the user according to the objects selected, which are stored in the database with the specific username. The user needs to select same number of digits as the objects. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Examples are shown in Figure 2.
- *Step 3:* During authentication phase, the user recalls pre-selected objects and related digits as his password on a touch sensitive screen (or according to the environment) with a mouse or a stylus. This will be done using the pure recall based methods.

During registration, the user selects the user name and a textual password in a conventional manner and then chooses the objects as password. The minimum length for textual password is Ln=6. Textual password can be a mixture of digits, lowercase and uppercase letter. After this the system shows objects on the screen of a hand held device (PDAs, ipods, iphones) to select as a graphical password. After choosing the objects, the user puts digits (0 to 9) on a screen with a stylus or a mouse or by hand. Digits given input by the user are stored in the database with his/her username. In object selection, each object can be selected any number of times as like for digits. Flow chart of registration phase is shown in Figure 3.

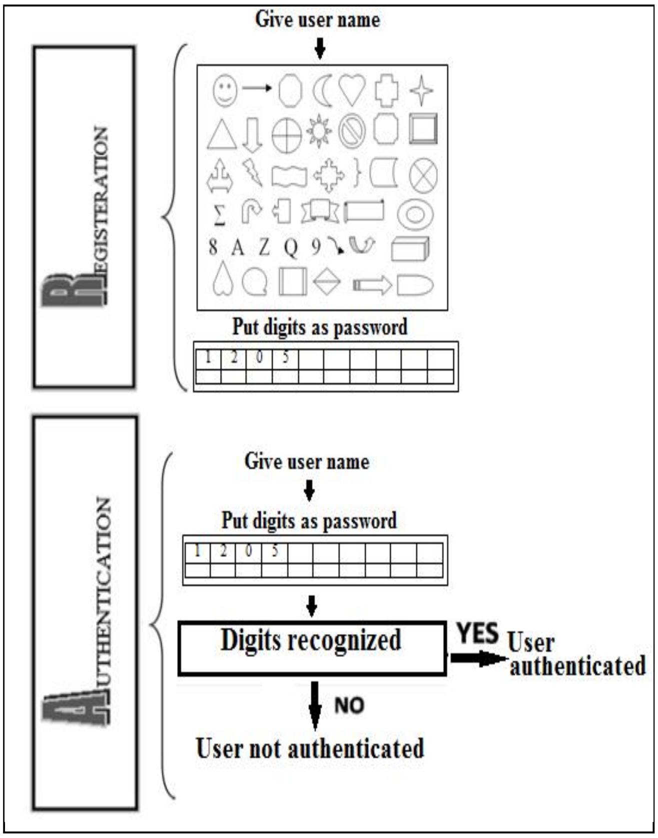

Fig. 1 Graphical Representation of Ray's Scheme

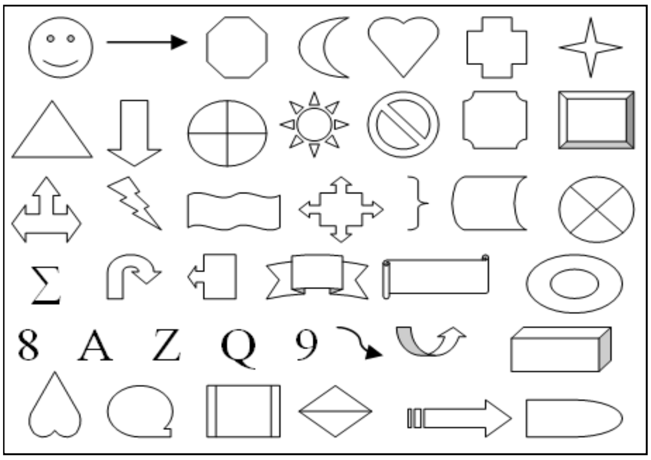

Fig. 2 Some examples of objects shown to the users

During authentication phase, the user has to first give his username and textual password and then put digits pre-selected. These digits are then matched with the digits stored in the database. Flow chart of authentication phase is shown in Figure 4.

VI. COMPARISON OF RAY'S SCHEME WITH EXISTING SYSTEMS

My system offers many advantages over other existing systems as discussed below:

Comparing to the "Passface" system (Passface 2011), Ray's scheme can also be used for those who are face-blind. I have used objects instead of human faces for selecting as password because later on during the authentication phase, the user has to put digits as his/her password and it is a much more difficult task to draw human faces than simple digit putting. Also I believe that as compared to human faces, objects are easier to remember which are in daily use. Ray's scheme has eliminated the problems with grid based techniques where the user has to remember the exact coordinates which is not easy for the user. Our system just compares the digits put by the user during authentication.

Ray's scheme is less vulnerable to Brute force attack as the password space is large. It is also less vulnerable to online and offline dictionary attacks. Since simple hand touch is used, it provides ease to the user for putting digits and also it will be impractical to carry out dictionary attack. Ray's scheme is better than Man et al scheme (Man 2003). This is because in his scheme the user has to remember both the objects and string and the code. In our method the user has to remember the objects he selected for password and also the digits he has put corresponding to objects during registration.

Comparing to Van Oorschot's approach (Oorschot 2009), my system is more secure since users not only select graphical password but also put digits as their password, making it difficult to hack. In my proposed system, even if the textual password is compromised, the graphical password cannot be stolen or compromised since the user is putting digits corresponding to objects as password. Ray's scheme proposed system differs from CDS (Gao 2010) in that the user has to first select a textual password and then a graphical password, making it more secure. Comparing to Two Step Authentication system, our proposed system works in the same way as Two Step Authentication system i.e the user has to choose a textual password before choosing a graphical password but difference is that in our system during authentication, after giving the username and textual password, the user has to put digits as his numerical password which is matched with its stored string drawn by the user during the registration phase. This approach protects from hacking the password and prevents them from launching different attacks. Thus my system is more secure and reliable than two step authentication system. As with all graphical based systems, Ray's scheme system will also be slow. The normalization and matching will take time.

When comparing to Khan's approach (Khan 2011), Ray's scheme proves itself much smarter and simpler in all the way of designing and implementation. Khan's approach takes textual username and password as the parameters in authentication phase similar to my scheme. But it differs, when Khan’s system asks the user to draw the objects he selected priori in registration phase than just put digits corresponding to objects in my scheme. Drawing is complex procedure in terms of user ability, though it can be minimized by experience; but it is very difficult to implement in practical systems which when occur increases expenses and complexity of systems. In my scheme, user only need to put digits according to the selected objects from the pane, which is very simpler and easier in every aspect of user usage and practical implementation.

The possible attacks on graphical passwords are Brute force attack, Dictionary attacks, Guessing, Spy-ware, Shoulder surfing and social engineering. Graphical based passwords are less vulnerable to all these possible attacks than text based passwords and they believe that it is more difficult to break graphical passwords using these traditional attack methods. My System is resistant to almost all the possible attacks on graphical passwords.

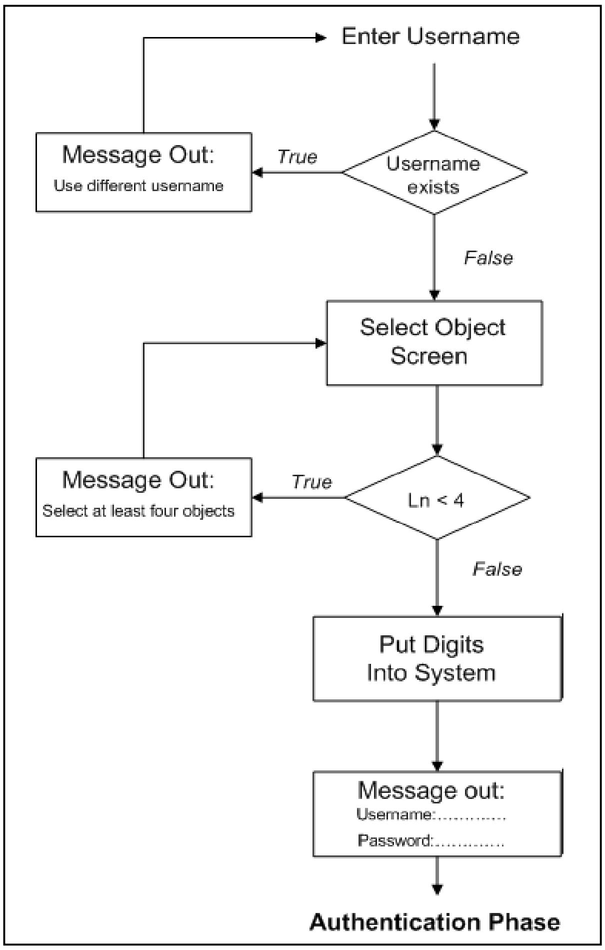

Fig. 3 Flow chart of registration phase

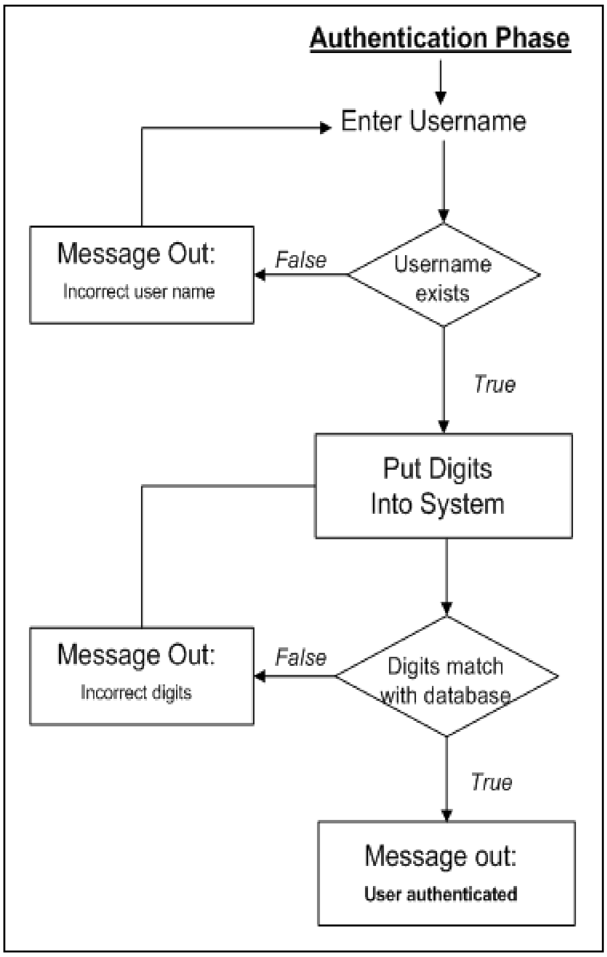

Fig. 4 Flow chart of authentication phase

VII. Conclusion

The main element of computational trust is user identity. Currently lots of authentication methods and techniques are available but each of these has its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, I have proposed authentication system which is based on GP schemes. Although my system aims to reduce the problems with existing GP schemes but it has also some limitations and issues like all other graphical based password. I have proposed an authentication system which takes digits as password as selected for the pictures (objects) priori. Currently I am heading on implementation of my proposed system. In future, I will investigate the performance issues and user adaptability.

REFERENCES

[1] Dhamija, R., Perrig, A. (2000), Deja Vu: A User Study. Using Images for Authentication. *9th USENIX Security Symposium.* Authentication (2011), http://www.objs.com/survey/authent.htm.

[2] Sobrado, L, and Birget, J C. (2002), Graphical Passwords, *The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research*, vol 4, http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[3] Elftmann, P. (2006), Diploma Thesis, Secure Alternatives to Password-Based Authentication Mechanisms.

[4] Blonder, G, E. (1995), Graphical password, U.S. Patent 5559961, Lucent Technologies, Inc.

[5] Suo, X, Zhu, Y, Scott. Owen, G. (2005), “Graphical Passwords: A Survey”, *Annual Computer Security Applications Conference.*

[6] Khan, H, Z, U. (2007), Comparative Study of Authentication Techniques, *International Journal of Video & Image Processing and Network Security,* Vol: 10 No: 04.

[7] Approaches to Authentication (2011), http://www.e.govt.nz/ plone/ archive/ services/ see/ see-pki-paper-3/ chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html.

[8] Khan. W. Z., Aalsalem. A. Y., Xiang. Y. (2011), A graphical password based systems for mobile devices. *Internation Journal of Computer Science and Issues,* Vol. 8, Issue 5, No. 2, 145-154.

[9] Token Based Authentication (2011), http://www.w3.org/ 2001/ sw/ Europe/ events/ foaf galway/ papers/ fp/ token_based_authentication/.

[10] Biometric Authentication, (2011), http://www.cs.bham.ac.uk/ ~mdr/ teaching/ modules/ security/ lectures/ biometric.

[11] Knowledge based Authentication. (2011), http:// searchsecurity.techtarget.com/ definition/ knowledge-based-authentication .

[12] Knowledge Based Authentication. (2011). http://csrc.nist.gov/archive/ kba/index.html.

[13] Weinshall, D, (2006), Cognitive authentication schemes safe against spyware, (short paper). *IEEE Symposium on Security and Privacy.*

[14] Hayashi, E., Christin, N., Dhamija, R.,and Perrig, A. (2008), Use Your Illusion: Secure authentication usable anywhere, 4th *ACM Symposium on Usable Privacy and Security (SOUPS).*

[15] Davis, D., Monrose, F., and Reiter, M. (2004), On user choice in graphical password schemes, 13th *USENIX Security Symposium.*

[16] Dhamija, R., and Perrig, A. (2000), Deja Vu: A User Study. Using Images for Authentication, 9th *USENIX Security Symposium.*

[17] Real User. (2011), www.realuser.com.

[18] Passfaces Corporation. (2011), The science behind Passfaces, White paper, http:// www. passfaces. com/enterprise/resources/white_papers.htm.

[18] Angeli, A., D., Coventry, L., Johnson, G., and Renaud, K. (2005), “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”, *International Journal of Human-Computer Studies,* **63**(1-2):128-152.

[19] Moncur, W., and Leplatre, G. (2007), Pictures at the ATM: Exploring the usability of multiple graphical passwords, *ACM Conference on Human Factors in Computing Systems (CHI).*

[20] Pering, T., Sundar, M., Light, J., and Want. R. (2003), Photographic authentication through untrusted terminals, *Pervasive Computing,* 30-36.

[21] Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J. (2006), Design and evaluation of a shoulder-surfing resistant graphical password scheme, *International Working Conference on Advanced Visual Interfaces.*

[22] Bicakci, K., Atalay, N. B. , Yuceel, M. , Gurbaslar, H., and Erdeniz, B. (2009), Towards usable solutions to graphical password hotspot problem, *33rd Annual IEEE International Computer Software and Applications Conference.*

[23] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R. (2003), Picture Password: A Visual Login Technique for Mobile Devices, *NISTIR.*

[24] Tafasa. Patternlock, (2011), http://www.tafasa.com/patternlock.html.

[25] GrIDsure. GrIDsure (2011), corporate website: http://www.gridsure.com.

[26] Weiss, R., and Luca, A., D. (2008), PassShapes-Utilizing stroke based authentication to increase password memorability, *NordiCHI,* 383-392.

[27] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. (1999), The design and analysis of graphical passwords, *8th USENIX Security Symposium.*

[28] Dunphy, P., and Yan, J. (2007), Do background images improve Draw a Secret graphical passwords?, *14th ACM Conference on Computer and Communications Security (CCS).*

[29] Tao, H. (2006), Pass-Go, a New Graphical Password Scheme, Master Thesis, University of Ottawa.

[30] Gao, H., Guo, X., Chen, X., Wang, L., and Liu, X. (2008), YAGP: Yet another graphical password strategy, *Annual Computer Security Applications Conference.*

[31] Orozco, M., Malek, B., Eid, M., and Saddik, A. E. (2006), Haptic-based sensible graphical password, *Virtual Concept.*

[32] Goldberg, J., Hagman, J., and Sazawal, V. (2002), Doodling our way to better authentication, (student poster), *ACM Conference on Human Factors in Computing Systems (CHI).*

[33] Varenhorst, C. (2004), Passdoodles: A lightweight authentication method, MIT Research Science Institute.

[34] Renaud, K., and Angeli, A. D. (2004), “My password is here! An investigation into visio-spatial authentication mechanisms”, *Interacting with Computers,* **16**(4):1017-1041.

[35] Renaud, K., and Smith, E. (2001), Jiminy: Helping user to remember their passwords, Technical report, School of Computing, University of South Africa.

[36] Suo, X. (2006), A design and analysis of graphical password, Master's thesis, College of Arts and Science, Georgia State University.

[37] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. (2005), Authentication using graphical passwords: Basic results, *11th International Conference on Human-Computer Interaction (HCI International).*

[38] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. (2005), Authentication using graphical passwords: Effects of tolerance and image choice, 1st *Symposium on Usable Privacy and Security (SOUPS).*

[39] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. (2005), PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, **63**(1-2):102-127.

[40] Chiasson, S., van Oorschot, P. C., and Biddle, R. (2007), Graphical password authentication using Cued Click Points, In *European Symposium On Research In Computer Security (ESORICS),* LNCS 4734, 359-374.

[41] Chiasson, S., Forget, A., Biddle, R.,and van Oorschot, P. C. (2008), Influencing users towards better passwords: Persuasive Cued Click-Points, *Human Computer Interaction (HCI),* The British Computer Society.

[42] Stubblefield, A., and Simon, D. (2004), Inkblot Authentication, MSR-TR-2004-85, Technical report, *Microsoft Research.*

[43] Alsulaiman, F., and Saddik, A. El. (2006), A novel 3D graphical password schema, *IEEE International Conference on Virtual Environments: Human-Computer Interfaces and Measurement Systems.*

[44] Passlogix graphical password system. (2011), www.passlogix.com.

[45] Gao, H., Ren, Z., Chang, X., Liu, X, Aickelin, U. (2010), A New Graphical Password Scheme Resistant to Shoulder-Surfing, *International Confer-ence on CyberWorlds.*

[46] Oorschot, P. C. V., Wan, T. (2009), TwoStep: An Authentication Method Combining Text and Graphical Passwords. *4th International Conference, MCETECH.*

[47] Man, S., Hong, D., Mathews, A. (2003), A shoulder surfing resistant graphical password scheme, *International conference on security and management.*

AUTHORS PROFILE

Partha Pratim Ray obtained Bachelor of Technology in computer science and engineering from the West Bengal University of Technology, Kolkata, West Bengal, India in the year 2008. He has recently completed Master of Technology in electronics and communication engineering with specialization in embedded systems in 2011 from the same University. The author has already published 6 research papers in various national and international journal and conference proceedings. He is currently an assistant professor in Computer Science and Engineering Department in Surendra Institute of Engineering and Management, Siliguri, Darjeeling, India. His interest includes in embedded systems and software, pervasive computing and wireless sensor network.