Providing a Secure Hybrid Method for Graphical Password Authentication to Prevent Shoulder Surfing, Smudge and Brute Force Attack

Faraji Sepideh

***Abstract*—**Nowadays, purchase rate of the smart device is increasing and user authentication is one of the important issues in information security. Alphanumeric strong passwords are difficult to memorize and also owners write them down on papers or save them in a computer file. In addition, text password has its own flaws and is vulnerable to attacks. Graphical password can be used as an alternative to alphanumeric password that users choose images as a password. This type of password is easier to use and memorize and also more secure from pervious password types. In this paper we have designed a more secure graphical password system to prevent shoulder surfing, smudge and brute force attack. This scheme is a combination of two types of graphical passwords recognition based and Cued recall based. Evaluation the usability and security of our proposed scheme have been explained in conclusion part.

***Keywords*—**Brute force attack, graphical password, shoulder surfing attack, smudge attack.

I. Introduction

SMART devices are common in our daily lives. They have become an integral part of our day-to-day activities and people store private information, such as contact details, documents, personal images, PIN numbers, and financial information in their smart devices. A consumer report in the USA found that 34% of all smartphone owners either have no security mechanism in place or use a simple code to lock the screen of their smartphones. At the same time, only 36% of smartphone users use a basic 4-digit PIN to lock their phones [1]. User authentication is crucial for protecting data that are stored on smart devices. Many authentication schemes are proposed in the literature, e.g., public key infrastructure, biometrics-based, smart cards-based, and password-based and so on [2]. The most common type of authentication is password-base and text-based password is more common than others. It is a combination of alphabets, digit and special symbols since it is easy to memorize and can be converted to a unique number for key exchange protocols [3]. Text-based password is difficult and inefficient in the smart device because of the limited screen size. As a result, people use smaller password, which makes them more vulnerable to attack [4]. In addition, if the password is complicated people write it down. And people use one password for multiple devices [5]. However, text-base is vulnerable to various attacks, such as brute force attack, dictionary attack, social engineering attack, guessing attack and many others [6].

A graphical password has been proposed as a possible alternative to a text-based password. According to psychological studies, pictures are generally easier to remember or recognized than text [7]. The graphical password technique is developed by Blonder in 1996 [8]. The purpose of this system is increasing the security space and avoiding the weakness of conventional password [9]. However, existing graphical password schemes are also vulnerable to various attacks, among which shoulder surfing, smudge attack, and brute force are the most prominent [10]. Shoulder-surfing, using direct observation techniques, such as looking over someone's shoulder or CC cameras and video recorders to get passwords, PINs and other sensitive personal information is a serious problem. One of the possible problems is catching password by a malicious observer during entering password by user using traditional input device like keyboard, mouse … [11]. Nowadays touch screens are more common rather than hardware keyboards due to providing conversant experience. But hacker can catch the password due to smudge remains on screen. Remaining smudge is one of the side effects of touch screens. Latent smudges and frequently touched areas of the screen may be used to infer a form of information leakage [12]. The other famous attack is the brute force which aims to systematically check all possible secrets until the correct one is found. Most of the graphical password schemes fail to tackle attacks. Therefore, finding a solution to prevent these attacks remains an active research issue. In this paper, we propose a secure graphical password scheme, which is protected from these three attacks: shoulder surfing, smudge, and brute force attack. This scheme is a combination of two types of graphical password recognition based and cued recall-based which are detailed in the next section.

II. Background

There are three types of graphical password:

1- Recognition based
2- Recall based
3- Hybrid scheme

A. Recognition Based Technique

In registration phase user selects some images from some random images. In login phase the user should select images based on selected images in registration phase. The user has to recognize those preselected images in a correct sequence [13].

Sepideh Faraji is with Science and Research Branch of Islamic Azad University Iran (phone: 0+989122591451; e-mail: sepidehfaraji2000@gmail.com).

This scheme is vulnerable to attacks such as shoulder surfing, smudge, and brute force attacks. In the scheme which was explained in 2006, about 1000 objects are displayed on the screen and a user has to select multiple objects in such a manner that they must form a triangle. The motivation behind displaying this huge number of images on the screen is to introduce redundancy on the display. As a result, shoulder surfing attacks become less effective. Although this scheme prevents shoulder surfing attacks to a certain degree, it suffers from smudge attacks. Moreover, this approach is inconvenient for people with weak vision because there are too many images shown on a small screen [14]. Another scheme is called pass-face which is developed on a conjecture that people can memorize human faces over other images. In pass-face, a user has to select various human faces as a sequence of k images to create a story for authentication. To authenticate, users have to pick out their assigned faces, one at a time, from successive groups of faces. This scheme provides strong two-way authentication; however, it is susceptible to shoulder surfing and brute force attacks [15]. The other scheme is the Image-Pass technique which was explained in 2011. In this, 30 images with a 6*5 grid are presented to user and user selects some images and creates his password. In the next phase, a new combination of 12 real and decoy images are presented to the user and he has to select his password in order. Position of images will vary at every login. But because of grid size and fixed password images position this method is at the risk of shoulder surfing attack [16].

B. Recall Based Scheme

Recall based scheme is divided into two categories:

1- Pure recall-based
2- Cued recall-based

In pure recall base technique, the user has to repeat a registration draw. Users need to reproduce their passwords without being given any reminder. Some examples of this technique are: Draw-A-Secret (DAS) is one such pioneer graphical authentication scheme. In DAS, instead of entering an alphanumeric password, users use a set of gestures drawn on a grid to authenticate themselves. Although this scheme is meant to improve both the security of the scheme and the ease of verification by the user, it is vulnerable to both shoulder surfing and smudge attacks [17]. One of the unique methods of graphical passwords is the signature technique, because the user signature is individual so there is no need to memorize and it is hard to sign instead of the others. But using available devices such as mouse to signing is hard and also alternative devices such as pen-like input are expensive [18].

In cued recall-based technique user unlocks a device by tapping on multiple pre-selected points on the screen. This scheme provides a balance between recalling something from memory and recognizing an image. In this technique, a clue is provided to the user to recall a password, registered during the registration phase. This technique provides hints to a user to memorize the password hence easier than pure recall based technique. This type of graphical password-based scheme is introduced by Blonder in 1996 [8]. Some examples of this technique are: Pass Point technique: In this, any natural picture/painting is used, which helps the user to remember the click points. Predefined click points is not needed here unlike the Blonder technique which was explained in 1996 [8]. In this method which was explained in 2005 for the first time, an image is presented to user in registration phase and he can select any place on the image and the tolerance around each selected area is calculated. At authentication phase, the user has to click within tolerances of chosen click points in a correct sequence. Here, the password is easily created but the users can have more difficulty in learning their passwords than textual passwords. Also, login time is larger than a textual password [19]. Passlogix V-Go technique: Passlogix Inc. is a commercial security company located in New York City, The USA. This method is also called “Repeating a sequence of actions” that it means creating a graphical password by using sample objects in the house, garden or others; e.g. In the kitchen, the user can prepare a meal by selecting cooking ingredients, take fast food from the fridge and put it in the microwave oven, select some fruits and wash it in the washbasin and put it in the clean bowl. But password space is very small so password can be predictable or guessable [20].

C. Hybrid Scheme

A hybrid scheme is a combination of two or more schemes. There are some schemes which are a combination of recognition and recall scheme. A hybrid graphical password scheme is proposed in [2]. It combines a vibration code with a modified pattern locking system. It built an authentication graphical system named Vibration-And-Pattern (VAP) to neutralize the effects of shoulder surfing, smudge, and brute force attacks. To pass the authentication step, the user must select the same number of cells and feel the same number of vibration code as he had done in the registration phase. Their pattern lock has more flexibility in comparison to Android pattern lock; for instance, one cell cannot be selected two times in a password pattern in Android systems. This creates a higher password space and makes the brute force attacks less applicable. Considering shoulder surfing attacks, it is to mention that they can still be challenged as picture passwords come with a vibration code that users must sense it. There are some obscure parts that cannot be properly determined by the observers. Conversely if the phone is placed on a table or somewhere flat or woody, vibration might be heard by close observers and can disclose the vibration code. Smudge attacks are tough to be mounted as one cell can be selected several times by a user. Timing attacks get harder due to its randomized vibration code for several authentication observations but it might add to the total timing of the authentication process. The other technique was proposed in [13]; they combined the two well-known types, recognition-based and recall-based, to produce a password that is immune to two steps of authentication. In the enrollment phase, users as their first phase of authentication should choose some images from a set of 25 pictures. And after those users are presented with 3 questions and they should select 3 points ROA (region-of-answer). Users should select correct images respectively in the first phase of authentication then they should select three regions of the preselected pictures as for the next step. In step two, the system utilizing a cued recalled-based method helps users to remember them easier. It should be mentioned here that in this step, the system randomizes the questions' numbers in a three-digit format to make it difficult for bystanders to memorize the relationship between questions and points. The two step authentication model uses randomization in both steps to make it harder for bystanders; however, it is not yet resistant to people with sharp eyes and a razor-sharp mind because the system would gradually be vulnerable to those people. Furthermore, this system is vulnerable to malicious software which has the intention to take screenshot and record mouse clicks. In the second phase, users should do their best to recollect what the related questions were, for example, 324. This number indicates the questions' numbers in a different order each time but the relevance of these numbers to the question list might somewhat be forgetful. In this case, although it is time-consuming, users can go back to the registration form to see what the questions' numbers were.

As a result of the above discussion, it is evident that most of the graphical password scheme fails to tackle attacks. Therefore, finding a solution to prevent these attacks remains an active research issue. In this paper, we propose a hybrid graphical password scheme, which is protected from shoulder surfing, smudge and brute force attacks. This scheme combines two types of graphical password: recognition based and pure recall based password. The details of our scheme are presented in the next section.

III. Proposed Scheme

In this paper, we proposed a hybrid graphical password scheme. It combines Recognition and Cued recall base. By doing so, our scheme provides better resilience against shoulder surfing, smudge, and brute force attacks. Our scheme is made of two main phases: registration and login. Details are presented in the following section:

A. Registration Phase

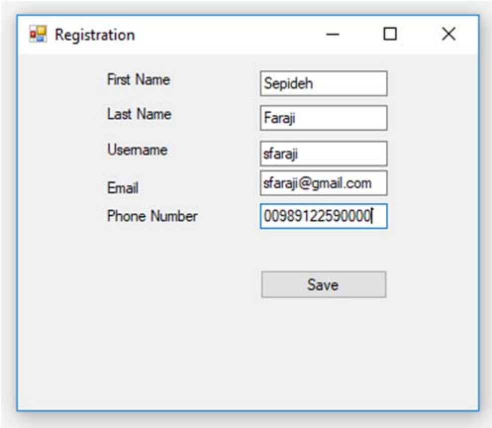
1-1 User creates his profile by entering personal details and username. The information we need is shown in Fig. 1.

1-2 Then it shows a 5*5 grid with 25 cells and the system randomly puts a set of 25 images into those cells. Users can use these images or choose any images from the stored images in the database.

1-3 In the next step user has to select three images from the grid. These three images will use a password, so it is important to remember those images. The minimum number of images in the password should be 3. The images selected by the user are displayed in the down in order to be selected by the user. Then the user selects next button. This step is illustrated in Fig. 2.

1-4 Then the other 5*5 grid will be shown and the user has to draw a pattern that will use in the login phase. To design this pattern user must select cells next to each other.

1-5 The registration phase will complete if the user draws his pattern and click on the complete button. This step is illustrated in Fig. 3.


Registration

First Name: Sepideh
Last Name: Faraji
Username: sfaraji
Email: sfaraji@gmail.com
Phone Number: 00989122590000

Fig. 1 Registration information

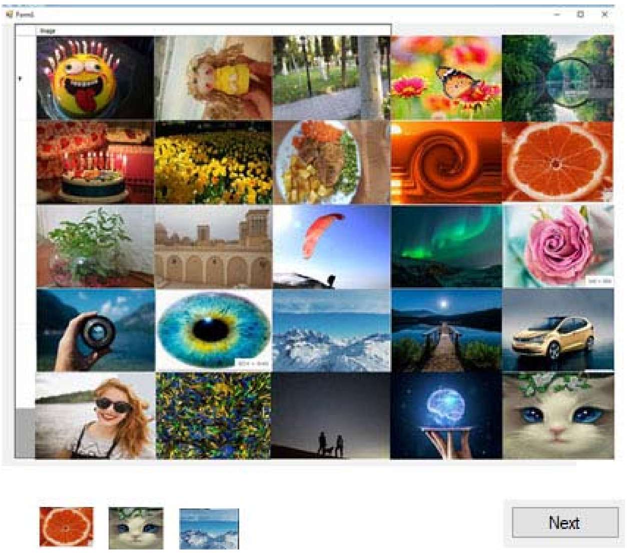


Fig. 2 Registration phase, images selection

B. Login Phase

1. The login step is based on recognition-based method and the user is asked for a username. If the user enters the correct username, step2 of the login phase will be shown to the user.
2. Then, if username is correct, the graphical password will be entered. In this step, it shows a 5*5 grid with 25cells and the system randomly puts a set of 25 images into those cells. The image position will vary at every login.
3. In this step user must select image according to his pattern. He remembers his pattern and selects images based on it. Instead of selecting the previous registered password images, the ones matched with his pattern should be chosen. This step is based on the cued recall base method.
4. The user has to select password images in the order he selected in the registration phase. Then the user clicks on

the login button and is allowed to log in. These steps are shown in Fig. 4. Selected images as a graphical password in registration phase were orange, cat and mountain, as illustrated in Fig. 4. In login step the user selects flower, butterfly and sky instead of them. The images' positions will vary at every login, so the images which the user selects will be changed in every selection due to image position and his pattern.

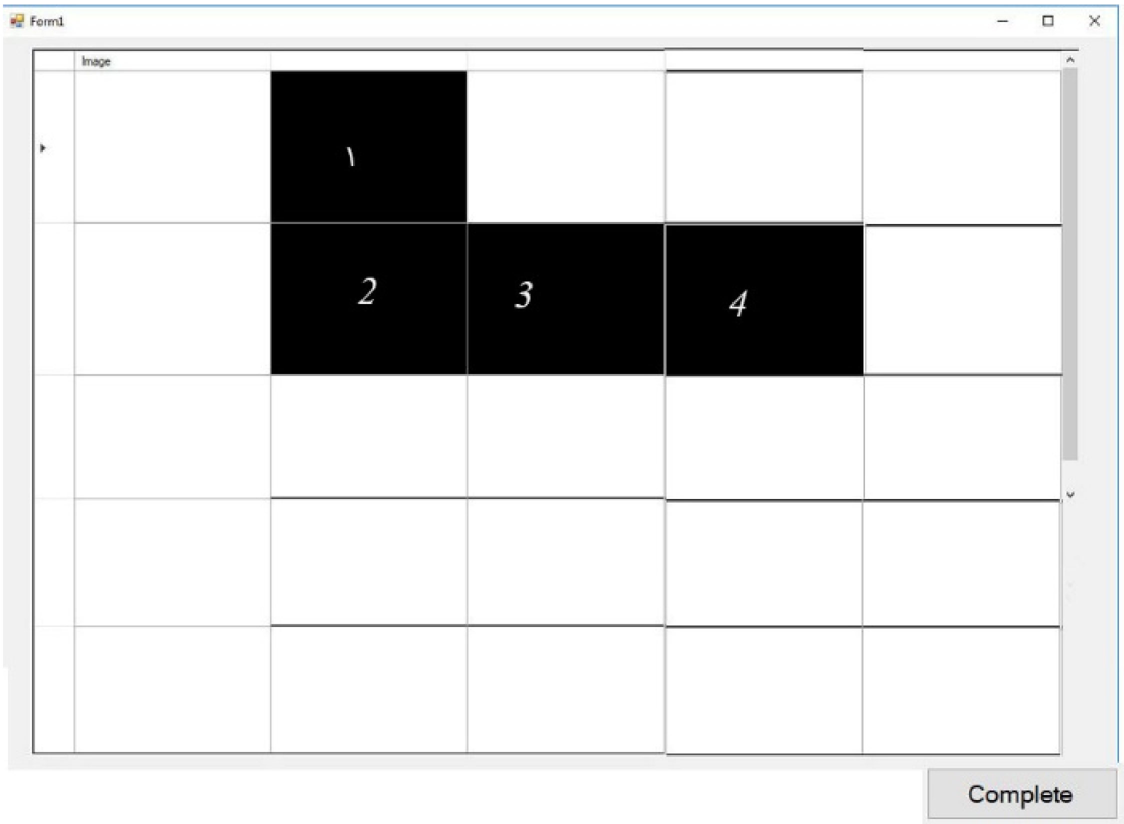


Fig. 3 Design a pattern by cells selection

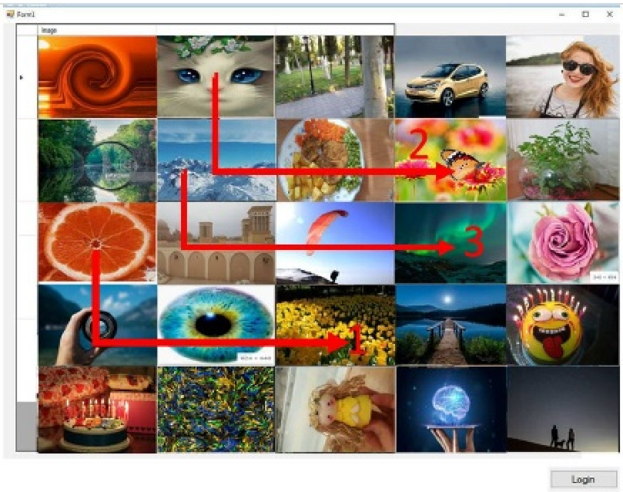


Fig. 4 Login phase, image selection based on user pattern

IV. Analysis of the System

It is observed that most of the graphical passwords are vulnerable to shoulder surfing, smudge and brute force attack but our system provides strong security against all of them.

Shoulder surfing attack: this attack refers to using direct observation techniques, such as looking over someone's shoulder to get information about users' input. It is particularly effective in crowded places, as it is relatively easy to observe somebody without being noticed. It is also a challenge for the most existing graphical passwords such as PassPoint, DAS and CCP [21]. In our proposed scheme the positions of the images will vary at every login, so the images which user selects will be changed in every selection due to image position and his pattern. So it is a strong way to prevent shoulder surfing attacks. In other words, if a man sees your screen while you are entering your password, he sees the fake images which are not your password images and also you select different images in each login.

Smudge attack: Screens are touched, so oily residues, or smudges, remain on the screen as a side effect. Latent smudges may be used to infer recently and frequently touched areas of the screen – a form of information leakage [22]. Instead of selecting the real password images, the other cells should be chosen and if the attacker captures screen, they find fake cells and also they capture different cells in each login.

So our proposed scheme prevents smudge attack.

Brute force attack: this attack aims to systematically check all possible secrets until the correct one is found. In our method, the password space is calculated as: The number of possible passwords, taken at least 3 images out of 25 images will be: C (25, 3) = 25! /3!*22! = 2300 passwords. However, the random passwords are possible to be: 2300*25! = 3.5*1028 > 1028. And also the minimum number of pattern that user can use by selecting two cells as a pattern will be: C (25, 2) = 300. So available password space is: 3.5*300*1028 > 1031.

There is a compression of the password space of several password schemes. For traditional text-based passwords with length 8 over a 64 character alphabet, the relevant password space is 2.81*1014, while the password space can be enlarged to 1.17*1016 with length 8 over 102 printable characters. For another well-known graphical password PassPoint, the password space is 4.22*1016 with 6 click points [23]. It is seen that the password space is much larger than both traditional text-based passwords and PassPoint as a graphical password. Thus scheme has a very large password space so it provides strong security against the brute force attack.

V. Conclusions

A graphical password is developed as an interesting alternative to traditional text-based passwords. In this paper, we presented an authentication mechanism and method for a graphical password which is resilient against shoulder surfing, smudge, and brute force attack. Our system is a combination of recognition and a cued recall-based approach. It is more secure from previous graphical password methods.

References

[1] Herb Weisbaum, Most American don't secure their smartphones. April 26,2014, url: http://www.cnbc.com/2014/04/26/ most-American-don't-secure-their-smartphones.html

[2] Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N. ... & Zain, J. M. (2017). VAP code: A secure graphical password for smart devices. Computers & Electrical Engineering, 59, 99-109.

[3] Xiong, H., Chen, Y., Guan, Z., & Chen, Z. (2013). Finding and fixing vulnerabilities in several three-party password authenticated key exchange protocols without server public keys. Information Sciences, 235, 329-340.

[4] Michael cooney, 10 common mobile security problem to attack. Pc world, url: https://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

[5] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). ACM.

[6] Janczewski, L. J., & Fu, L. (2010, October). Social engineering-based attacks: Model and New Zealand perspective. In Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on (pp. 847-853). IEEE.

[7] Cranor, L. F., & Garfinkel, S. (2005). Security and usability: designing secure systems that people can use. " O'Reilly Media, Inc.".

[8] Blonder, G. E. (1996). U.S. Patent No. 5,559,961. Washington, DC: U.S. Patent and Trademark Office.

[9] Chaturvedi, S., & Sharma, R. (2015). Securing text & image password using the combinations of persuasive cued click points with improved advanced encryption standard. Procedia Computer Science, 45, 418-427.

[10] Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19.

[11] Kumar, M., Garfinkel, T., Boneh, D., & Winograd, T. (2007, July). Reducing shoulder-surfing by using gaze-based password entry. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 13-19). ACM.

[12] Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. Woot, 10, 1-7.

[13] Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498.

[14] Wiedenbeck S, Waters J, Sobrado L, Birget J. Design and evaluation of a shoulder-surfing resistant graphical password scheme. Proceedings of the international working conference on advanced visual interfaces (AVI); 2006.

[15] Passfaces Corporation. Passfaces: two factor authentication for the enterprise. Url: http://www.realuser.com/ last accessed in June 2015.

[16] “ImagePass - Designing Graphical Authentication for Security” Martin Mihajlov E- business Department Faculty of Economics Borka Jerman-Blazi Jožef Stefan Institute Ljubljana, Marko Ilievski Seavus Group 2011.

[17] Jermyn I, Mayer A, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. Proceedings of the 8th USENIX security symposium; 1999.

[18] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[19] Susan Wiedenbeck, Jim Waters, Jean - Camille Birget and Alex Brodskiy, Nasir Memon. PassPoints, “Design and longitudinal evaluation of a graphical password system”, International Journal of Human-Computer Studies, 63(1-2): 102-127, July 2005.

[20] Passlogix,http://www.passlogix.com,Accessed on February 2007.

[21] Meng, Y., & Li, W. (2013, July). Enhancing click-draw based graphical passwords using multi-touch on mobile phones. In IFIP International Information Security Conference (pp. 55-68). Springer, Berlin, Heidelberg.

[22] Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. Woot, 10, 1-7.

[23] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Passpoints: Design and Longitudinal Evaluation of A Graphical Password System. Int. J. Hum.-Comput. Stud. 63(1-2), 102–127 (2005)

S. Faraji, Tehran/Iran, Aug 16th 1989, Master student of information technology at Science and Research Branch of Islamic Azad University Iran. She received bachelor's degree in computer science from Kashan University 2011, Iran. She is technical manager of Energy Exchange Settlement System, Tehran/Iran. She was Software Developer of Stock Market Systems.