International Journal on Advanced Science Engineering Information Technology

Vol.7 (2017) No. 3
ISSN: 2088-5334

A Pattern-Based Password Authentication Scheme for Minimizing Shoulder Surfing Attack

M I Awang[#], M A Mohamed[*], R R Mohamed[#], A Ahmad[#], N A Rawi[#]

[*]*Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, 22200 Terengganu, Malaysia*
E-mail: isa@unisza.edu.my, mafendee@unisza.edu.my, khairani@unisza.edu.my

[#]*Department of System and Networking, Universiti Tenaga Nasional, 43000 Kajang, Selangor, Malaysia*
E-mail: rajina@uniten.edu.my

[#]*Department of Computer Science, National Defence University of Malaysia, 57000 Sungai Besi, Kuala Lumpur, Malaysia*
E-mail: arniyati@upnm.edu.my

***Abstract*— The user usually uses a password to avoid the attacks like a dictionary attack, brute force attack and shoulder surfing attack which is the famous attack nowadays. The shoulder surfing attack is a direct observation technique by watching over the user's shoulder when they enter their password to get information. The most common authentication method used by the user is textual password. But, the textual password has many disadvantages because it is vulnerable to attack as it tends to shoulder surfing attack. In this project, a pattern-based password authentication will develop to overcome this problem. Using this scheme, the user needs to select the type of pattern that they like during registration. To log in to their account, the user needs to enter the password in the form of the textual password in ordering manner based on a pattern that they choose during registration. The text password grid presented with a different style as it filled with random objects whether characters, numbers or images. This method is suitable to minimizing shoulder surfing attack as it can improve the security of user's password and they can efficiently login to the system.**

***Keywords*— user authentication; shoulder surfing; pattern-based; grid selection; recall based**

I. INTRODUCTION

Authentication is the process where the identity of a person or a thing is verified. It is also the way for confirming the truth whether the attribute of data claimed by an entity is valid or not. Some also define authentication as a process in which the proof of identity provided is compared with the file stored the database of users' information within a computing system [1]. During verification, the system compares the stored credential that user chooses during the registration with the credential that they enter during the login session. If the entered credential matches with the one stored in the database, the process completes, and the user gains the authorization to access the system. Simply put, authentication is the process of verifying if the individual is the person that they claimed to be based on the capability of the authentication system. There are three types of authentication technique [2]. The first type of authentication is accepting the proof of identity given by a trusted person who has evidence of the said character the originator. The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. The third type of authentication relies on documentation or other external affirmations [3].

In general, we can categorize user authentication according to three sects that are token-based, biometric-based and knowledge-based as in Fig. 1.

A security token is a small piece of hardware device that one needs to carry with in order to get authorized access to a network service. The device can be in any form such as a key card, smart card or can be embedded into other entity such as a key fob. This token offers an extra level of security via a method called two-factor authentication [4], wherein a user is accommodated with a personal identification number (PIN) that authorizes them as the owner of that specific device. The device displays a number which uniquely identifies the user to the service, allowing one to log in. The identification number for each user is renewed on the predetermined periodical basis. The use of tokens has many benefits compared to traditional methods in that it is self-contained and possesses all the information required for authentication. This is great for scalability as it frees the server from having to store session state. Moreover, using token-based security, we can further refine user access

control. Within the token payload, user roles and permissions can be defined as well as the resources that the user is allowed to access.

Every human fortunately is equipped with unique physiological and behavioural characteristics that distinguish one from another. Biometrics uses these unique characteristics as identifiers to ascertain and verify one's identity. Unique identifiers include distinct features such as fingerprint [5], iris structure [6], retinal patterns [7], facial structure [8] and voice print [9]. All these characteristics are physiological based. In regards to behavioural based, some uniqueness can be extracted from the way one's walk [10], handle the keyboard and mouse [11], write signature [12] and voice tone. Research involving biometric technology has gained attentive footprints and recently being well adapted into standardization.

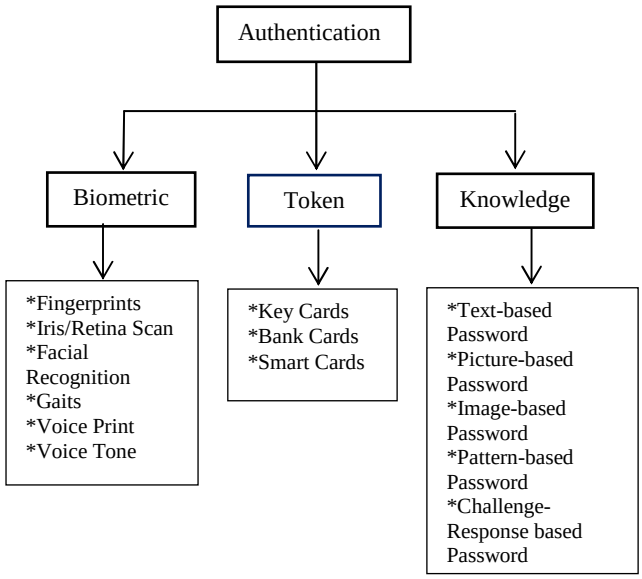

Fig. 1 Taxonomy of user authentication

The ability of a human to memorize is being the basis for knowledge-based authentication [13]. The commonly used tool is a password which can be in various forms such as text, picture, image, and pattern. By and large, it is the most widely used authentication technique due to advantages such as simplicity, convenience, adaptability, mobility, and less hardware requirement. A password is a representation of an entity that is used for user authentication to prove their identity or granted access to a resource [14]. People also use a password to avoid many kinds of attacks such as dictionary attack, brute force attack and shoulder surfing attack [15]. A dictionary attack is a technique for defeating an authentication mechanism by trying to determine the key or word that is used as a password by guessing the possible word based on certain language. Meanwhile, a brute-force attack is a trial-and-error method used to obtain the password via trying every possible combination of characters until succeeded. Unlike the two, shoulder surfing attack is a direct observation technique by watching over the user's shoulder when they enter their password during the login session.

The most common password based authentication method used by the user is via textual-based password [16], [17]. Nevertheless, the textual password is considered as not secure anymore because it has many disadvantages and is vulnerable to attacks especially shoulder surfing attack. In many cases, users frequently choose an easy and straightforward word as their password in order to remember it easily. On the contrary, if the users choose the password which is lengthy which is somehow much secure. However, the long password is difficult to remember. The textual passwords tend to be susceptible to shoulder surfing attack, as it is easy for an attacker to look and hence form the words when users enter their password.

The other method for authentication is via graphical-based passwords [18]-[20]. Similarly, it also has their disadvantages in that it require more time for authenticating and the usability issues. Users who are quickly forgotten what they choose during registration will not be able to login into their account.

There is also a problem with passwords that they do not provide reliable security. This because the attacker can download software or tool from the internet to crack the user password by testing the most combinations of characters for each user on a system thus get their password. In this study, we propose an implementation of pattern-based password authentication scheme for minimizing shoulder surfing attack. We combine two techniques that are grid selection technique during the user registration process and recall based technique during the user login process.

This paper is organized as the following. Section 2 acquaints readers to the related works involving existing pattern-based authentication techniques. Section 3 discusses the methods specifically used within our proposed pattern based authentication applications. Section 4 proposes the design and the development of this new application. Section 5 presents the results and offer some discussions on the matter. Section 6 concludes the findings of this paper.

This section survey numerous techniques that have been proposed by many researchers related to authentication scheme [14], [21]. Based on the literature review of the previous existing article, many theories have been proposed by the researcher for designing authentication schemes. The main reason why authentication is important nowadays is to reduce and avoid from an unauthorized user. Techniques available so far are session password, Draw a Secret (DAS), grid selection technique, recall based technique, recognition based technique and hybrid textual authentication, to name a few. All the techniques that were proposed have their strengths and weaknesses, and each performs the best under selected conditions.

There is a different form of representations used for authentication such as textual password, graphical password, and biometric password. Each of them comes with their advantages and disadvantages [22]. According to [23], the most general authentication methods in computers and other devices usually need the submissions of the users' names and their passwords. This forms the basis of the most common method for authentication that is using textual password [24], [2], [25]. But, the textual password has its disadvantages and drawback. The textual password is vulnerable to eavesdropping, dictionary attacks, social engineering and shoulder surfing attack [2]. Moreover, in [24] pointed out that the textual password has a significant drawback in that if users tend to pick passwords that are

simple and can easily remember, it is easy to guess by an attacker. Whereas, if the password is hard to guess, it often hard to remember by the user. In [25] stated that the main problem of the textual password is the difficulty of remembering those password and users tend to pick the short passwords, as it is easy to remember without knowing that it can be easily guessed and cracked by an unauthorized user and attacker.

The biggest threat nowadays that requires the user to have a password for their account is shoulder surfing attack [26]. Shoulder surfing is an attack which can be performed by the unauthorized user to obtain the authorized user's password by watching over the user's shoulder when he enters his password [24]. This attack is usually effective in crowded places because it is easy to observe someone without been suspicious as they are filling in their password field. The shoulder surfing attack can occur in the events when the user enters their PIN at an automated teller machine or enter a password at a cybercafe, public and university libraries. Besides, shoulder surfing can also be done at a distance using some tools like binoculars or other vision-enhancing devices. Also, some inexpensive and simple devices also can be used to make this attack such as using an illegally installed tiny camera to observe data entry.

The others alternative techniques that are used for authentication are graphical passwords and biometrics. A graphical authentication scheme that was proposed by [27] is a technique, where the user has to identify the pre-defined images to prove user's authentication. During registration, the user needs to select a certain number of images from a set of random pictures. Then, during login phase, the user must identify the pre-selected images for authentication from a set of images. This technique is quite easy to the user as we, human tend to remember images quicker than words. Furthermore, biometrics such as fingerprints, iris scan or facial recognition is pretty secure authentication techniques. Most of the times, it suffers from the need to significantly more time to process the identification, and the device can be quite expensive [2], [25].

In [25] proposed authentication scheme using text and colors for generating session password. Session password is a password that is used only once at a time. Once the session is terminating, the session password is no longer useful because for every login session; users must enter different passwords. Moreover, according to [2], the use of session password is very suitable for Personal Digital Assistants (PDA) because it is resistant to shoulder surfing attack. Session password is generated using grids and colors serve as an alternative authentication technique to reduce the drawback of textual password authentication. During registration phase, the user needs to submit his chosen password consisting of a minimum length of 8 passwords that is called as secret pass. The secret pass must contain an even number of characters because from this; the session passwords are generated. During the login phase, when the user enters his username, an interface that consists of alphabets and numbers in a grid size 6x6 is displayed. The characters are randomly placed on the grid, and the interface will change every time the user want to log in. Then, the user has to enter the password depend on upon their secret pass, and they must consider his secret pass in term of pairs. The first letter in the pair is used to select the row, while the second is used to select the column as the intersection letter is part of the session password. This process is repeated for all pairs of the secret pass until the password is generated. The password that is entered by the user will then be verified by the server to authenticate the user. In a nutshell, although the session password is a new alternative that secured for authentication, it also has some drawbacks like others. In session password, there are some problems such as security of data, files system, backups, network traffic and host security.

Shoulder surfing attack can be minimized using text and color based on graphical password scheme that was proposed by [24]. This method needs the user to choose the length of the password which is between 8 to 15 characters and chooses one color as his pass color from 8 colors that are given by the system. As the seven colors remaining, it will be the decoy colors. As usual, users also need to register an e-mail address for re-enabling his account when he enters a wrong password. The most important things in this scheme are user need to carried the registration process in an environment that is free from shoulder surfing. During the login process, a circle will display which is composed of 8 sectors of equal size when a user sends a login request. The colors of the arcs of each sector are different that can be identified by the color of its arc. Besides, there is a button for rotating the circle clockwise, anti-clockwise, the "confirm" button and the "login" button as well [24]. The user has to rotate the sector which contains the characters of the password and has to move the character in the sector which color is selected by the user until they have their password. As the conclusion, the system that proposed which uses text and color based graphical password is useful to reduce the shoulder surfing attack. Using this authentication method, the user can log in the system without caring about shoulder surfing because they can enter their password without using the physical keyboard. The user can also easily and efficiently login to the system if they use this authentication method as they are familiar with both password scheme that is textual password and color based graphical password.

In [23] proposed a new authentication technique that is a hybrid password authentication scheme based on shape and text. The hybrid password scheme based on the shape that is suitable not only for computers but also can be used in the mobile devices. As overall, this scheme is to make a map that guides the user from shape to text with strokes of the shape and a grid with text [16]. Users may think some personal shapes that the like and its strokes will be their origin password. Then they need to enter the character given in the authentication as the login password. The whole process of this authentication includes two main steps. The first step is password creation or also known as registration phase. The user should click on the grid in the interface following the shapes' stroke sequence that they had chosen early. After that, the system will store the shape and the order with the grid as the user's mapped the text password. The second step is login phase. During this phase, the user needs to enter their text password based on their shapes' stroke sequence. The interface is presented with a different style and filled with a few numbers of the symbols

randomly. The interface will generate another login interface grid if the password entry is not correct. As the strength of this technique, the login interface will be different all the time. So, if the attackers record the text password that user input during login, they would get nothing about the user's original password. This technique also is suitable to reduce the shoulder surfing attack.

In [28] proposed a new authentication technique call "Draw a Secret (DAS)". This system allows the user to create their passwords by drawing something that they want on a given 2D grid. After the user finishes the drawing, the system will then store the coordinates of the grids occupied by the picture. During the login phase, users must re-draw the picture that they had created and chosen during registration. The system verified the authentication if the drawing touches the same grid in the right order, but if not, then the verification is failed. The password space of this scheme is proved to be larger than the full text-based password space and hence is considered as significantly more secure.

II. Material and Method

Testing in this section discuss the two techniques that are to be combined to produce our newly hybridized technique to form the full set of our authentication system. These techniques are grid selection technique which is used during the user registration session and recall-based technique which is used during the user login session.

A. Grid Selection Technique (Registration)

The grid selection technique shown in Fig. 2 is an initially massive, fine-grained grid from which the user selects a drawing grid, a rectangular region which they may enter their password [29]. In our authentication system, grid selection technique is used by the user during the registration phase. There will be an empty grid given for the user to choose their password. The user needs to select the grids as their chosen password. The user can choose whatever pattern or styles they want as they wish [30]. There is no limit for the user to select how many grids they like to choose their password.

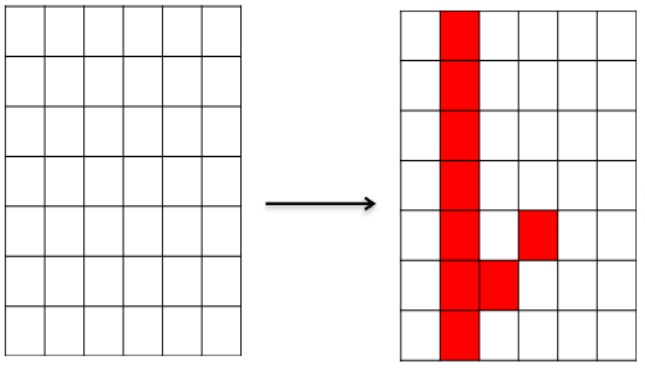

Fig. 2 Grid selection technique

B. Recall Based Technique (Login)

Recall based technique asks the user to reproduce something that user has created earlier during the registration stage [29]. Recall based usually requires the user to interact with the system in some cognitively meaningful manner. The password may be selected in a different type of methods such as from clicking on a collection of images.

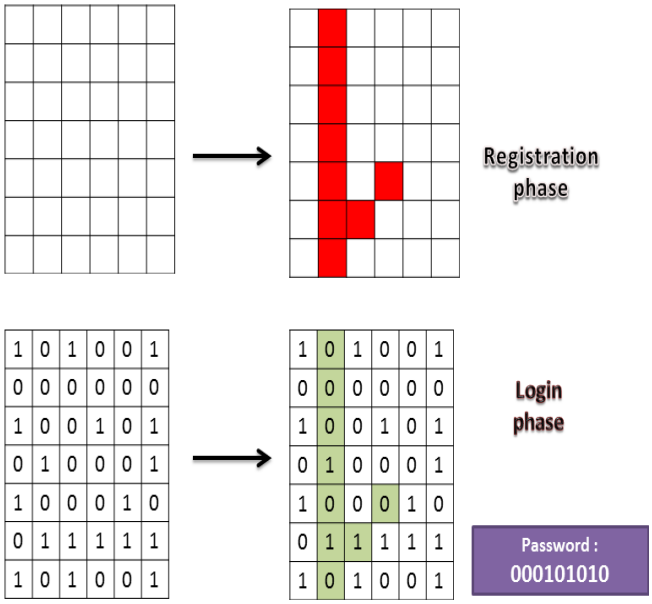

Fig. 3 Recall based technique

Besides, recall based technique also have an implicit order about them, especially during the selection process. The recall based technique can be categorized into two, pure recall based technique and cued recall based technique. Pure recall based technique is an approach where the user needs to reproduce their password without being given any hint or clue. Whereas, the cued recall based technique proposed a framework of reminder, hints, and gesture that help the users to reproduce their password or help users to make a reproduction more accurate.

The recall based technique is normally used during login phase where the user is asked to recall something that he or she created during the registration phase. In this system, as shown in Fig. 3, the user is required to remember their password pattern strokes that they choose during registration. The important things for the user are to remember back the pattern sequence that they choose because, during login, they need to enter the textual password based on their sequence of pattern password. Access to the system is granted only when the users can recall back their pattern password and enter it correctly.

C. Development

Testing In this section, it involves the real development of the authentication system based on the previous phase. To develop the authentication system, the coding will be developed before the system goes through the testing phase using the PHP language. In this authentication system, the grid selection technique and recall based technique will be applied. Besides, by using the waterfall model, the user can continue to suggest the improvement or changes.

The development of this authentication system can be presented through framework and flowchart. Fig. 4 shows the framework for this authentication system. The framework shows the workflow of the whole process for the authentication system. It mainly involves a user as a client

and a server as an authenticator. A new user is required to register and hand in a password that is to be stored in the database.

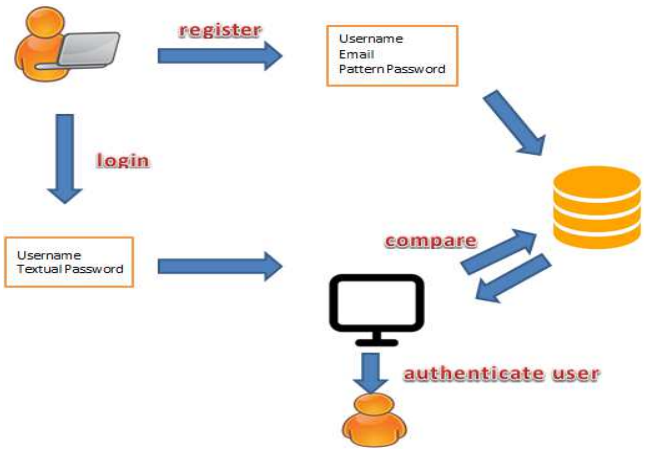

Fig. 4 Framework

For the purpose of getting access to specific resources, this user needs to login to the system by providing the password that supposed to be identical to the one created during the registration process and stored in the database. Failing of doing so will result in the unsuccessful access to the system resources.

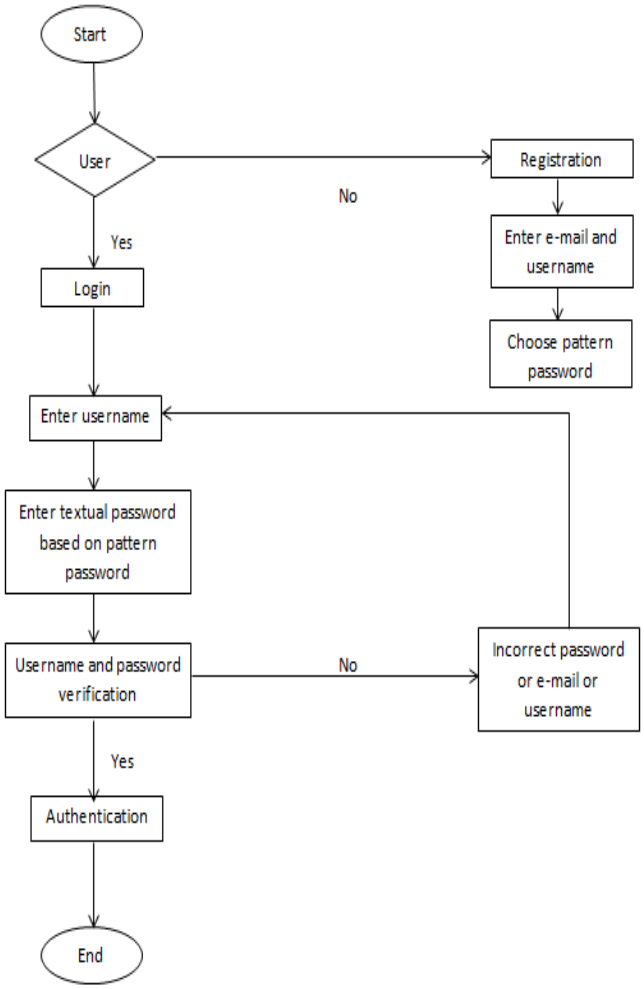

Fig. 5 Flowchart

Fig. 5 shows the flowchart of the authentication system. First, if the user is new to the system and still did not register, he/she is required to do so. During registration, the user needs to enter a username, e-mail and choose the pattern password. All the details then will be saved into the database. Otherwise, if the user has already registered, he can proceed to login into the system. During the login process, the user only needs to enter a username and textual password. Then, the system will compare the username and textual password that is entered by the user and compare it with the one created and stored in the database. If the login is a success as a result of the user entering the correct username and textual password, then the user authentication is successful.

III. Results and Discussion

In this section, we present the result of the implementation of earlier section. In this authentication system, the interface consists of three parts which are home main page interface, registration interface, and login interface. Fig. 6 shows the home page interfaces. In the home page, it will display the button for home, log in, register, and log out. The user can choose which page they want to select and go through.

.

Fig. 6 Main page

Fig. 7 shows the registration page where the user will be directed to if they click on the registration button from the main page. This page is only for unregistered users. The registration page will display the registration form that the user needs to fill up with the required field.

Fig. 7 Registration page

Fig. 8 shows the login interface. The login page will display the login form that is to be filled up by the users with their username and textual password. Somehow, this page is connected to the database where the user credential is stored from registration session.

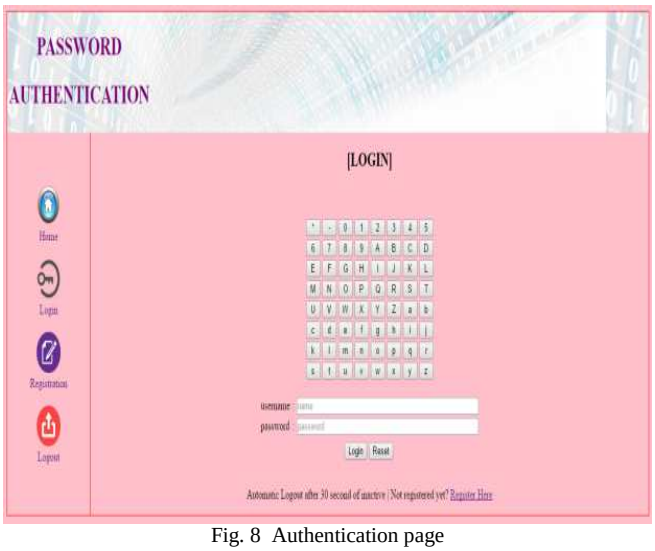

Fig. 8 Authentication page

When the users enter the correct username and password, they will be authenticated as shown in Fig. 9. In this session, the users will be logged out automatically if they remain inactive for more than one minute.

Fig. 9 Result page

Upon completion of any activity, users will be able to log out by clicking on the logout button. If the user wants to perform a new activity, one has to login again.

IV. Conclusion

By this project, it will be a great help indeed to computer users in preventing personal asset from being stolen by their adversaries. Classical authentication techniques are prone to various attacks. The proposed solution caters the issue of shoulder surfing attacks which could easily be conducted when using the text-based password.

References

[1] R. Syahputri and K. S. Chan, "A new pre-authentication scheme for IEEE 802.11i wireless LAN network," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 1, pp. 342-346, 2011.

[2] N. S. Joshi, "Session passwords using grids and colors for web applications and PDA," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, pp. 248-253, May 2013.

[3] S. M. S. Tabatabaeifar, M. Lashkargir, S. Taghizadeh, and H. K. Tafti, "Colour fusion in face authentication system based on visible and near infrared images," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 1, pp. 376-380, 2011.

[4] M. Singhal and S. Tapaswi, "Software tokens based two factor authentication scheme," *International Journal of Information and Electronics Engineering*, vol. 2, pp. 383-386, May 2012.

[5] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proceedings of the IEEE*, vol. 85, pp. 1365-1388, Sep. 1997.

[6] V. Roselin, E. Chirchi, L. M. Waghmare, and E. R. Chirchi, "Iris biometric recognition for person identification in security systems," *International Journal of Computer Applications*, vol. 24, pp. 1-6, Jun. 2011.

[7] M. A. Siddiqui, S. M. H. S. Iqbal, and M. R. Salehin, "Personal authentication through retinal blood vessels intersection points matching," *International Journal of Computer Applications*, vol. 33, pp. 34-39, Nov. 2011.

[8] R. Jafri and H. R. Arabnia, "A survey of face recognition techniques," *Journal of Information Processing Systems*, vol. 5, pp. 41-68, Jun. 2009.

[9] H. Lee and H. Ko, "Voice code verification system using competing models for user entrance authentication," in *Proc. ICCE'05*, 2005, p. 37.

[10] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen, "A lightweight gait authentication on mobile phone regardless of installation error," *Security and Privacy Protection in Information Processing Systems*, vol. 405, pp. 83-101, Jul. 2013.

[11] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, pp. 165-179, Jul. 2007.

[12] D. H. Shah and T. V. Shah, "Signature recognition and verification: The most acceptable biometrics for security," *International Journal of Application or Innovation in Engineering and Management*, vol. 4, pp. 30-36, Aug. 2015.

[13] A. Nayak and R. Bansode, "Analysis of knowledge based authentication system using persuasive cued click points," *Procedia Computer Science*, vol. 79, pp. 553-560, Jan. 2016.

[14] A. Mathur, "Improved password selection method to prevent data thefts," *International Journal of Scientific and Engineering Research*, vol. 2, pp. 239-240, Jun. 2011.

[15] A. H. Lashkari, S. Farmand, D. Zakaria, O. Bin, and D. Saleh, "Shoulder surfing attack in graphical password authentication," *International Journal of Computer Science and Information Security*, vol. 6, pp. 145-154, Dec. 2009.

[16] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A hybrid password authentication scheme based on shape and text," *Journal of Computers*, vol. 5, pp. 765-772, Jan. 2010.

[17] R. Weiss and A. D. Luca, "PassShapes: Utilizing stroke based authentication to increase password memorability," in *Proc. ACM NCHCIBB'08*, 2008, p. 383.

[18] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in *Proc. IEEE ICC'10*, 2010, p. 194.

[19] T. Khodadadi, M. Alizadeh, S. Gholizadeh, M. Zamani, and M. Darvishi, "Security analysis method of recognition-based graphical password," *Jurnal Teknologi*, vol. 72, pp. 57-62, 2015.

[20] V. S. Borkar and P. C. Golar, "Click based graphical password with text password authentication," *International Journal of Computer Science and Network Security*, vol. 15, pp. 76-79, Nov. 2015.

[21] R. B. Joshi, "Highly secure authentication scheme," *International Journal of Computer Applications*, vol. 108, pp. 35-38, Jan. 2014.

[22] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in *Proc. ACM ICAINAW'07*, 2007, p. 467.

[23] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in *Proc. IEEE IWETCS'09*, 2009, p. 90.
[24] S. K. Sonkar, R. L. Paikrao, A. Kumar, and M. S. Deshmukh, "Minimizing shoulder surfing attack using text and color based graphical password scheme," *International Journal of Engineering Research and Technology*, vol. 3, pp. 835-839, Feb. 2014.
[25] N. Dorage and B. Sawant, "Authentication schemes for session passwords using colors," *International Journal of Computer Science and Network Security*, vol. 16, pp. 120-123, Apr. 2016.
[26] T. S. Wu, M. L. Lee, H. Y. Lin, and C. Y. Wang, "Shoulder-surfing-proof graphical password authentication scheme," *International Journal of Information Security*, vol. 13, pp. 245-254, Jun. 2014.
[27] R. Dhamija and A. Perrig, "Deja Vu-A user study using images for authentication," in *Proc. USS'00*, 2000, p. 1.
[28] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proc. USS'99*, 1999, p. 1.
[29] A. H. Lashkari, F. Towhidi, R. Saleh, and S. Farmand, "A complete comparison of pure and cued recall-based graphical user authentication algorithms," in *Proc. ICCEE'09*, 2009, p. 527.
[30] T. S. Nguyen, C. C. Chang, and H. S. Hsueh, "High capacity data hiding for binary image based on block classification," *Multimedia Tools and Applications*, vol. 75, pp. 8513-8526, Jul. 2016.