International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication using Images Sequence

Muhammad Ahsan[1], Yugang Li[2]

[1]Student, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
[2]School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China

---

Abstract - *This paper proposes a new technique of user Authentication that is Graphical Password Authentication using Images Sequence. In existing environment, a very important problem in information security is user authentication. There are many authentication techniques like textual, graphical, biometric, smart card etc. The existing graphical authentication techniques based on images selection are not good enough because in these techniques images are predefined by the system. In this paper, a new technique is proposed. In this method, user will upload images from his/her personal gallery/directory for password selection and images uploaded by one user will not be visible to other user. Graphical password is used as an alternative to textual/traditional alphanumeric password. Traditional alphanumeric password is difficult to memorize and usually forget by users as times passes when user remain unattached from the system, but in case of graphical password there are less chances to forget password because people remember images more easily than text based password. There are also less chances for hackers to steal the graphical based password because hackers will be unable to access the images uploaded by the user as password. We tested this method in a Web-based application.*

Key Words: Biometric authentication, Images based password, Recall based technique, Recognition based technique, Smart card authentication.

1. INTRODUCTION

Data security and user authentication is a basic factor for information security. Internet is providing accessibility to desired information resources across the globe. Every organization, social network, or any other platform try to provide better security to their users which is accurate and more secure for users. Authentication of user is basic component of any information system because it provides the ability to the user to access the system. Old security techniques which are using from a long time, provide less security for authentication than the advance security techniques. In the perspective of information security there may be following main objectives of authentication or security.

- How to keep away an unauthorized user from gaining access to system?
- How to ensure the accessibility of authorized users to the required resources of system?
- How to communicate user with system and with other resources [1]?

As described by the researchers and psychological studies that it is nature of humans that they remember images better than text, therefore the password which is graphical based, can be used alternatively to text based password [2]. Password comprises of data which is used to access to required resources of system. Password is kept secret from other users so that an unauthorized user can't access the resources of system and can't steel the personal information of the authorized users. Authentication can be done through several techniques like Textual/Alphanumeric, Smart Card, Bio-metric, Graphical etc. [3]. Each technique provides its own ability that can be regarded as secure. In this time user authentication regarded as a key feature of information security.

2. PASSWORD TECHNIQUES AND RELATED PROBLEMS

2.1 Textual or Alphanumeric Password Authentication

Textual/Alphanumeric (it can also be called as text based password) is a string or word of combined characters which are used to prove the authorized users [1], [4]. This technique for user authentication is commonly used [1] for a long time because this technique has many advantages but in the advance time there are more chances to steal the password by hackers [5]. To minimize the risk of stealing password, the password should be minimum of eight characters with uppercase, lowercase, special characters and alphanumeric characters. Alphanumeric password should not be meaningful contents like your first or second name, your age, your date of birth, your school name etc. [6].

Lack(s): Text based password is difficult to memorize for user because for a good security, [5] password should be lengthy, alphanumeric and include special characters [6]. If user use his password on daily basis, then password will easily memorize and if user didn't use password for a long time then there is chances to forget password [7]. To minimize the risk of forget password many users save their password in text file in the computer or write down on the paper. Saved password file can also steal by other users. Hackers can break the security which is text based [5]. Attackers use some "Spy" software (Key Listener and Key Logger) which can be easily install in the computer, these soft-ware recorded the key strokes and save in the text file

and these kind of software have also ability to send the saved key strokes to email address or an outside source [1], [8]-[10].

2.2 Smart Card Authentication

This technique is also use for user authentication and this type of authentication is also providing strong security. One of the main advantage of Smart Card Authentication is that it can be combined easily with the other kinds of authentication system. Smart card authentication provides additional security protocol and protection [11]. Smart Card has a small chip. All the information of user is store in the chip of smart card [1]. User swipes his/her smart card into smart card reader for verification of identity.

Lack(s): Smart cards are small in size and can be lost easily [11], [12]. Sometimes user forget his card in his/her office or home. If the card is stolen, then it is difficult to retrieve information from the stolen smart card [7]. This authentication technique can also increase initial cost at the time of deployment.

2.3 Biometric Authentication

Biometric authentication is a technique using individual's physical characteristics [7]. In this technique bio-logical data or bodily elements are evaluated for verification of user identity [7], [12]. Biometric based authentication provides the strongest and foolproof security and protect from unauthorized user to the system than text based, graphical based or smart card authentication [12]. There are no chances for hackers to steal the pass-word which is biometric based [7].

Biometric authentication is mainly implemented in such situations which have critical security requirements. Personal information and biometric data is distinct from each other [12]. Personal information can be stolen but it is very difficult for attackers to steal bio-metric data. Biometric authentication is long term security solution for any company or organization. Bio-metric authentication can be implemented in various ways like DNA Matching, Iris Scan, Retina Scan, Fingerprint Identification, Face Recognition, Hand Geometry Recognition, Signature Recognition and Voice Analysis etc. [1], [7, [10, [12]. Biometric authentication is suitable for those companies or organizations which have critical security requirements.

Lack(s): Biometric authentication is high level security [12] therefore hardware cost for biometric authentication is higher [1] compared to other authentication techniques. Sometimes biometric authentication is not suitable for arthritic persons who have no ability to put hands, eyes or fingers properly on scanner.

2.4 Graphical Password Authentication

Firstly, Graphical Password idea was given by Blonder in 1996, which states that an image should appear on given screen and user should select some regions by clicking on the image, if the selected regions of image are correct then the user will be authenticated [13]. User authentication using graphical technique is now very common. Organizations or companies are trying to adopt this authentication technique. On the web images are also using as re-captcha to know the types of user. Images as re-captcha provide advanced security [14]-[16]. Using images for authentication is easy for human and hard for robots that's why every organization or company try to adopt this technique.

In graphical password authentication images are used by the user for authentication [9], [17] user select some specific regions, select multiple images or create image etc. [8], [13], [18]-[19].

Mainly graphical password authentication based on two different techniques [5], [20]-[21].

I. Recognition Based Technique
II. Recall Based Technique

I. Recognition Based Technique

In this type of graphical authentication technique multiples images are show to user at registration phase [22], images may be in random order. User has to select some images (according to defined condition) for password selection. Selected images as password either in sequence or in random order. At the time of login user has to select images which were selected for password (sequence or randomly).

II. Recall Based Technique

In this technique user has to provide some information at the time of registration i.e. text or handwritten design. Usually it is compatible with touch screen devices, pattern selection, signature, images drawn on 2G grid, hints for password etc. Recall based technique has different categories with different methods and ways, (1) Pure recall based technique which includes Passdoodle, Draw a Secret and Signature technique. (2) Cued recall based technique which include PassPoints, Blonder, VisKey SFR, Pass-Go, Drawing Geometry and Passlogix V-Go technique [5], [10], [20]-[21]. Our research is on graphical authentication using images in sequence that's why our focus is on Recognition Based Technique.

Graphical password authentication has many advantages like it provides more security than the textual password. "Spy" software (Key Listener and Key Logger) can't be used to record images [2]. It provides human friendly interface for user authentication. It is easy to memorize images password and has less attacking chances using dictionary attacks and brute force search [9]-[10]. Biometric

Table 1 shows the comparison between different biometric techniques.

Table -1: Comparison between Different Biometric Techniques

Factors / Techniques	Installation Cost	Security	Required Devices	Reliability	User Acceptance
DNA Matching	Very High	Very High	DNA Testing Machine	Very High	Low
Iris Scanning	High	Very High	Camera	Very High	Medium
Retina Scanning	High	Very High	Camera	Very High	Medium
Fingerprint Identification	Medium	High	Fingerprint Scanner	High	High
Face Recognition	Medium	High	Camera	High	Medium
Hand Geometry	Medium	High	Scanner	High	High
Voice Analysis	Medium	Medium	Microphone	High	Low
Signature Recognition	Low	Low	Touch Panel, Optic Pen	High	Very High

authentication provides very high security but its installation cost is also higher than the graphical password authentication, that's why this technique is more suitable over other authentication techniques.

Lack(s): Graphical authentication technique use images for password that's why it required more storage space [9] than the textual password did. Sometimes in this technique registration phase and login phase is too long and take more time than the textual password. It is easy to guess by shoulder Surfing, it means it can be guess over the user's shoulder due to its graphic nature, when user process information [1], [10], [23]-[27].

3. LITERATURE REVIEW ON GRPHICAL BASED PASSWORD

G. E, Blonder [13] proposed graphical password authentication technique first time. According to introduced technique user can select some click points to choose password from predefined image in the registration phase. At the time of login, user selects those points which were selected in registration phase, if these points matched then user is identified as authorized user.

Nikam [26] proposed a graphical password scheme based on text. During registration phase eight different colors are shown to users. User can select only one color to set password. During login phase a circle having eight sectors with a unique colored arc and 64 letters divided in sectors (each sector with 8 letters) randomly is shown to the user. User can choose the sector which contained letter of password and then user drags it into the sector with colored arc which was selected during registration.

Lashkari [8] proposed a new technique in which authentication of user is done by selection of images throughdifferent size of grids. During registration phase if user selects images to choose password from a 4*4 size of grid then at the time of login phase user selects images to choose password from 3*3, 5*5 or 6*6 size of grid. Size of grid during registration and login is different.

Umar et al. [28] presented a new authentication technique based on images. During registration user selects desire image and then clicks on different points of image. It is necessary for user to remember number of clicked points, order of clicked points and the time interval between two clicked points. During login user clicks on image points which was clicked during registration.

Rane et al. [29] proposed a new draw based graphical password technique in which during login phase images are shown to user. User selects several images in order to choose password. After this user choose one image from selected images and clicks to draw secret. During login phase user draws secret which was in the registration phase. Sequence of clicks is not necessary.

Albayati [30] proposed a new authentication scheme based on decoy image portions. During registration phase user uploads image from mobile gallery regarding image details and choose complexity level of image. During login phase, system shows sub-images which belong to original image and base on complexity level selected during registration phase. System adds decoy sub-images. User choose original sub-images for identification.

Syed, S. et al. [31] proposed new authentication scheme based on images with sound sequence. During registration phase user provides basic information such as id, password, phone number etc. After this user selects

predefined images in desire sequence and then select pixels on images and in the last user selects sound signature corresponding to images as password. In login phase user select pixels from registered images and select sound signature for verification. This technique is more secure but it consumes more time in registration phase and in login phase as well.

Gunde, P. [32] proposed a new graphical authentication technique which based on persuasive click point method. In this technique for registration user select point inside the view port on predefined image. For additional security click point sound is selected by the user. During login, point and sound is selected by user for verification.

Tivkaa, M.L. [33] proposed an authentication technique which based on cryptographic hashing and graphical password (recognition based). During registration user provides login information, password is encrypted and then saved in database. In the second stage user choose an image from image category for password. During login user enter credentials which was provided during registration phase. User is allowed to only two login attempts using text based encrypted password. If login failed, then user select image which was registered during registration phase. Login through image is allow only one time. After one failed attempt by selecting image, user IP will block. Authorized user is force to reset a password by providing registered details.

Chaudhari, D. R. et al. [34] proposed a new authentication technique which based on text based and graphical based as well. During registration user provide information and enter his/her password. Password should contain numbers, letters and special characters, then a circle is shown to user having eight sectors with unique assign number. User is select one sector and he should remember the selected sector. For login system is required password and selected sector by user.

4. INTRODUCED AUTHENTICATION TECHNIQUE

The introduced technique is based on graphical images. In previous techniques user selects a set of images but these images were predefined but in the introduced technique user will upload images from personal directory of computer. Sequence of images is key factor of introduced authentication technique. In this technique user will upload images at the time of registration for the sake of password and for login, user will have to select the images which were uploaded at the time of registration. Figure 1 shows that how this system will run.

4.1 Features of Introduced Technique

There are four main features of proposed technique

i. Valid email

During registration user will provide a valid email address which will be entered during login phase. After entering valid email address system will redirect to next page which will display images selection page.

ii. Number of images

During registration the user will have to select maximum 6 and minimum 4 images which are necessary to be uploaded to complete the registration process. During login phase user will have to select number of images which were uploaded during the registration phase. If the number of selected images is incorrect then user will be unable to login.

iii. Images from personal directory

The user uploads desired images from personal di-rectory. Advantage of this methodology is that, images uploaded from personal directory are easily memorized and these images are not visible to other users. These images are only visible to authorized user.

iv. Sequence of images

Important and key factor of this technique is sequence of images. Sequence of images is stored in database. At the time of login user selects uploaded images in same sequence as the sequence of images was selected during registration phase. If sequence of selected images is incorrect then user will unable to login.

There are two phases in the introduced technique Registration Phase and Login Phase.

4.1.1 Registration Phase

During registration user will registered by providing personal information including email and username. User will have to upload images in desired sequence from personal directory. User will upload at least 4 images and maximum 6 images. It is necessary that user will have to remember the sequence of images that he will upload. Without sequence of images user will be unable to login because our system based on the selection of images in sequence. In our system images sequence is key factor. Figure 2 shows the registration phase of our proposed system.

4.1.2 Login Phase

To ensure the successful login, first of all user will enter valid email address which was provided during registration. If email is valid then system will redirect to next page where 30 different images including user registered images will be shown to user. All images will be shown in random order. User will have to select 4, 5 or 6 images in sequence as a password to access the system. Specific user will select those images which were uploaded at the time of registration. During registration if user uploaded 6 images from personal directory, then he will have to select those 6 images in same sequence which was during registration. If user select incorrect images, incorrect number of images or

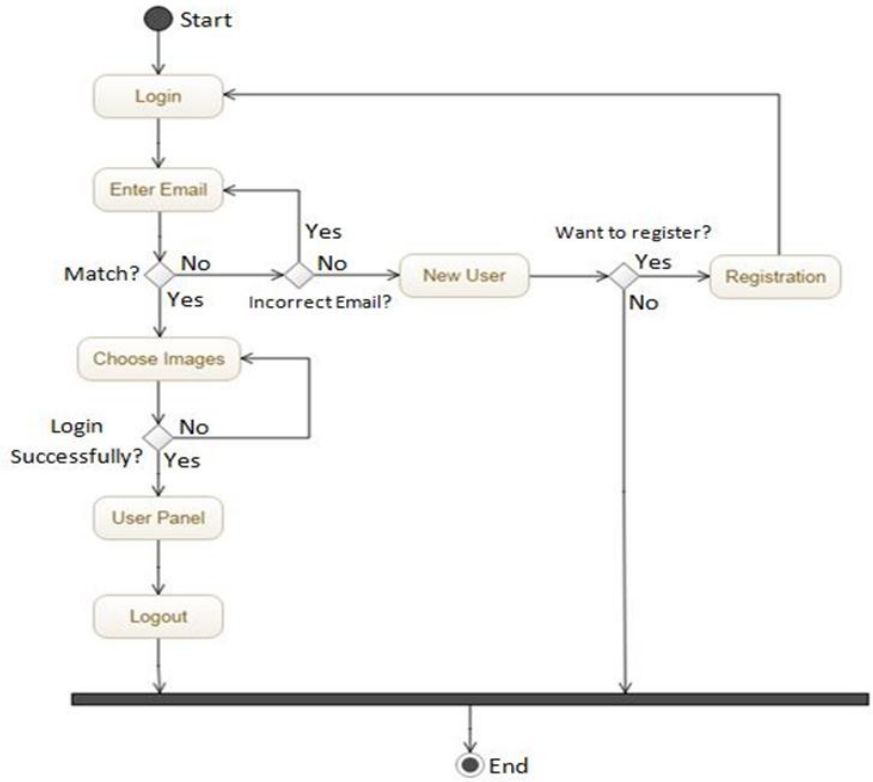

Fig -1: Activity diagram

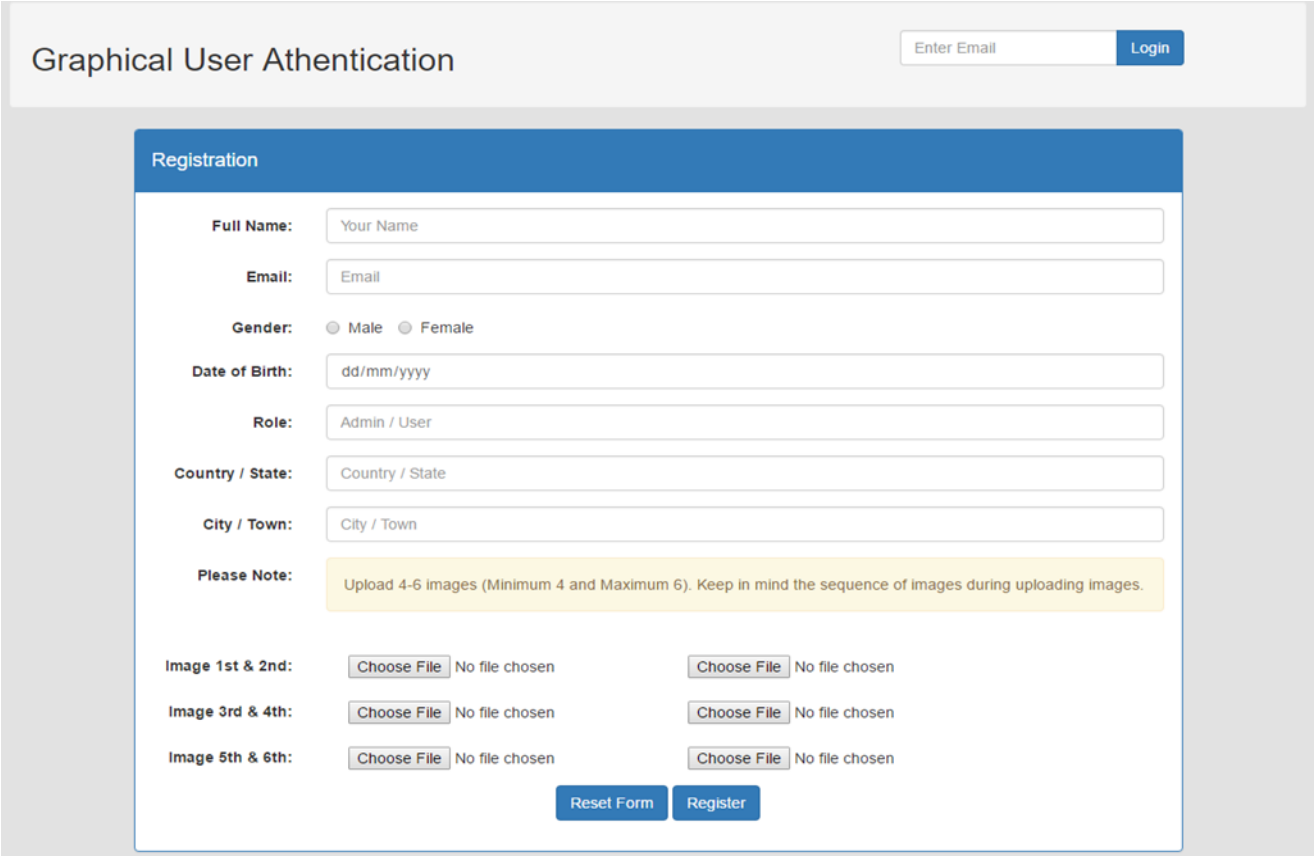

Fig -2: Registration phase

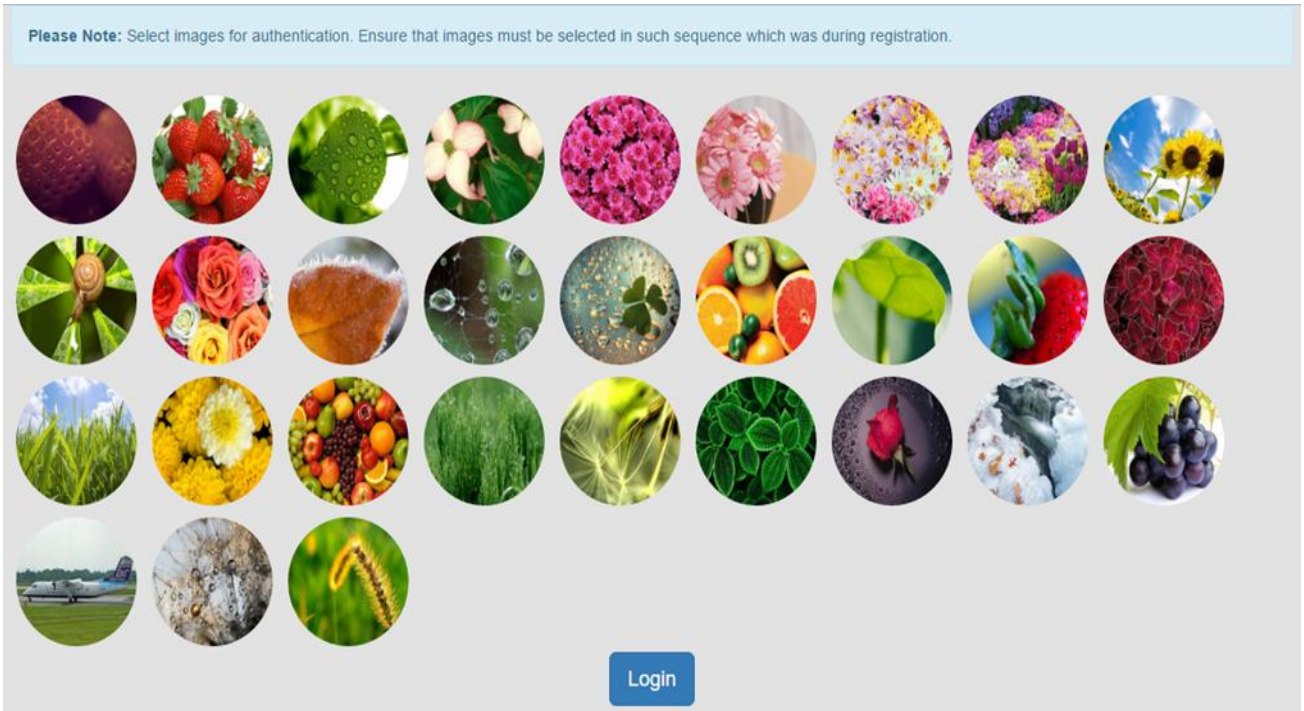

Fig -3: Login phase

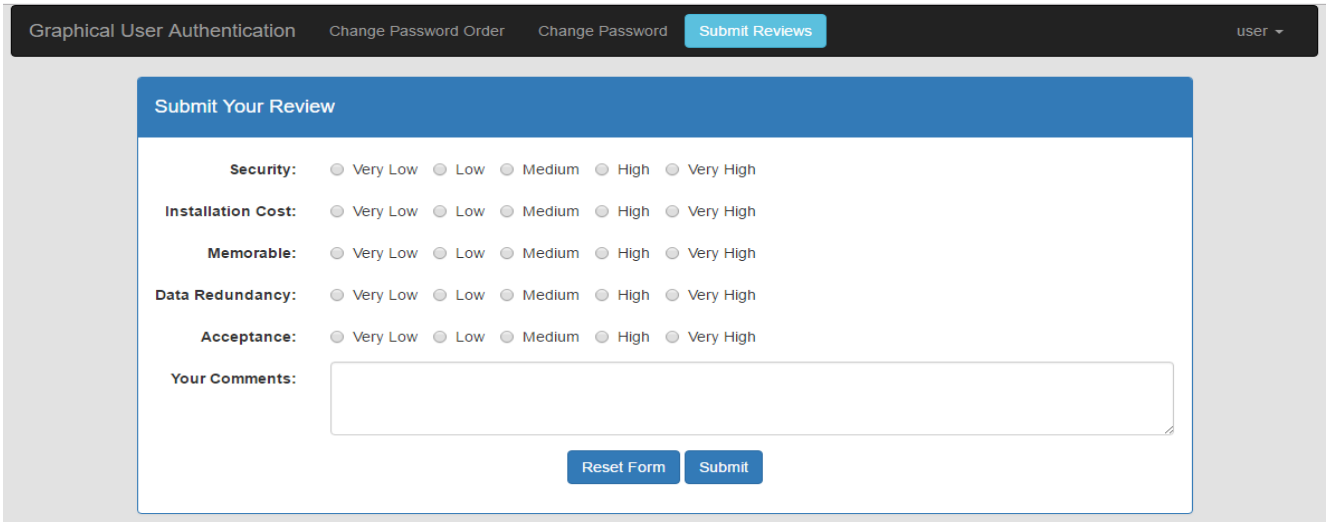

Fig -4: Reviews

in incorrect sequence, then he will be unable to login or access the system. To resist the shoulder surfing, images will be shown in random order. During each time of login order of images will be different from the previous login.

Figure 3 show the login phase of our system, after successful login system will redirect to dashboard of the user.

5. IMPLEMENTATION AND ANALYSIS

Although biometric authentication provides more security but its installation cost is very high. We only compare our system with the textual password technique.

We developed a web-based application using PHP and SQL to test the system and gather the user reviews about our proposed system.

This application was available online on this link http://gua.atestproject.com . The user reviews were gathered in two ways.

I. Online registration and login using above mentioned link.

II. The user provides views about video provide at the link https://youtu.be/y_gLk6o5aDM The link provides detail about the procedure how to login the password authentication technique.

Table -2: Comparison of proposed system with other authentication techniques

Factors / Techniques	Security	Installation Cost	Memorable	Data Redundancy	User Acceptance
Proposed System	High	Very Low	High	Low	Very High
Textual Password Authentication	Medium	Very Low	Medium and High	High	High
Smart Card Authentication	High	High	Low	Low	Low
Biometric Authentication	Very High	Very High	Very High	Low	Very Low

6. RESULTS

The comparison was based on five factors such as Security, Installation Cost, Data Redundancy, Acceptance, and how much easy to memorize. The reviews were collected from different registered users of our system and from YouTube video about the system. Figure 4 shows that how the results were gathered from different users for different factors. Comparison was conducted about user reviews about the proposed sys-tem with the textual/alphanumeric password authentication technique. Table 2 shows the comparison of proposed system and textual/alphanumeric password authentication technique based on user reviews. According to user reviews

- Proposed system is acceptable over textual password.
- It is easy to use.
- Images uploaded from personal gallery are easily memorized.
- Uploaded images are not shown to unauthorized users.

7. CONCLUSION

This paper described about graphical password authentication technique using images sequence. The introduced technique is based on the improvements in previous techniques introduced by the researchers, in this research system has been developed that allows the user to upload 4-6 images from his/her personal gallery or directory. Proposed system followed the sequence of images which were uploaded during registration. Sequence/order of images and number of images are key factor of proposed system. Images uploaded by one user are not visible to other or unauthorized user.

REFERENCES

[1] "Fundamentals of information systems security/access con-trol systems - Wikibooks, open books for an open world," [Online]. Available: https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems. Accessed: Jan. 22, 2017.

[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," 21st Annual Computer Security Applications Conference (ACSAC'05).

[3] M. S. B. Sahu, and A. Singh, "Survey on various techniques of user authentication and graphical Password," International Journal of Computer Trends and Technology, vol. 16, no. 3, pp. 98–102, Oct. 2014.

[4] "Password," in Wikipedia, Wikimedia Foundation, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Password. Accessed: Jan. 24, 2017.

[5] S. Ramanan, and B. J S, "A Survey on Different Graphical Password Authentication Techniques," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, issue 12, pp. 7594–7602, Dec. 2014.

[6] M. Burnett, and D. Kleimann, "Perfect passwords: Selection, protection, authentication," United States: Syngress Media, U.S., 2005.

[7] H. A. Kute, and D. N. Rewadkar, "Continuous User Identity Verification Using Biometric Traits for Secure Internet Services," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, issue. 8, pp. 7352–7357, Aug.2015.

[8] A. H. Lashkari, A. Gani, L. G. Sabet, and S. Farmand, "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids," Scientific Research and Essays, vol. 5(24), pp. 3865–3875, Dec. 2010.

[9] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," Journal of Software, vol. 8, no. 7, pp. 1678–1698, Jul. 2013.

[10] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of graphical Password authentication techniques," International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.

[11] C.-G. Ma, D. Wang, and S.-D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," International Journal of Communication Systems, vol. 27, no. 10, pp. 2215–2227, Nov. 2012.

[12] Y. LI, "Biometric technology overview," Nuclear Science and Techniques, vol. 17, no. 2, pp. 97–105, Apr. 2006.

[13] G. E. Blonder, "Graphical Password," US5559961 A, Lucent Technologies, Inc. (Murray Hill, NJ), Sep. 1996.

[14] P. P. Doke, and S.A Nagtilak, "A survey on CAPTCHA as graphical Password," International Journal of Science and Research (IJSR), vol. 4, no. 12, pp. 2032–2036, Dec. 2015.

[15] Rashmi B J, and B. Maheshwarappa, " Improved Security Using Captcha as Graphical Password," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 5, pp. 352–354, May 2015.

[16] M. Davis, Divya R, V. Paul, and Sankaranarayanan P N, "CAPCHA as Graphical Password," International Journal of Computer Science and Information Technologies, vol. 6(1), pp. 148–151, 2015.

[17] A. H. Lashkari, and S. Farmand, "A survey on usability and security features in graphical user authentication algorithms," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no 9, pp. 195–204, Sep. 2009.

[18] S. Sathish, A. B Joshi, and G. I Shidaganti, "User Authentication Methods and Techniques by Graphical Password: A Survey," International Journal of Computer Applications & Information Technology, vol. 2, issue 3, pp. 1–4, Apr. 2013.

[19] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords*," Journal of Computer Security, vol. 19, no. 4, pp. 669–702, Jun. 2011.

[20] E. E. K. Ugochukwu, and Y. Y. Jusoh, "A review on the graphical user authentication algorithm: Recognition-based and recall-based," International Journal of Information Processing and Management, vol. 4, no. 3, pp. 238–252, May 2013.

[21] D.Aarthi, and Dr. K. Elangovan, "A Survey on Recall-Based Graphical User Authentications Algorithms," International Journal of Computer Science and Mobile Applications, vol. 2, issue 2, pp. 89–99, Feb. 2014.

[22] F. Towhidi, and M. Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms," International Journal of Computer Science and Information Security, Vol. 6, No. 2, pp. 119–127, 2009.

[23] K. Rao and S. Yalamanchili, "Novel Shoulder-Surfing resistant authentication schemes using text-graphical passwords," International Journal of Information and Network Security (IJINS), vol. 1, pp. 163-170, no. 3, Jul. 2012.

[24] Mokal P. H., and Devikar R. N., "A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes," International Journal of Science and Research (IJSR), vol. 3, issue 4, pp. 747–750, Apr 2014.

[25] M. Bendale, N. Singh, S. Baid, and A. Maurya, "A Simple Text Based Graphical Password Scheme to Overcome Shoulder Surfing Attacks," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 3, pp. 364–366, Mar. 2015.

[26] A. M. Nikam, and S. N. Shelke, "Graphical Password Method Based on Text to Protect from Shoulder Surfing.," International Journal of Advance Foundation and Research in Computer (IJAFRC), vol. 1, issue 11, pp. 47–50, Nov. 2014.

[27] Thorawade M.B., and Patil S.M., "Authentication Scheme Resistant to Shoulder Surfing Attack Using Image Retrieval," International Journal of Knowledge Engineering, vol. 3, issue 2, pp. 197–201, Nov. 2012.

[28] M. S. Umar, M. Q. Rafiq, and J. A. Ansari, "Graphical user authentication: A time interval based approach," 2012 IEEE International Conference on Signal Processing, Computing and Control, Mar. 2012.

[29] P. Rane, N. Shaikh, and P. Modak, "Secure authentication using click draw based graphical Password scheme," International Journal of Advanced Engineering Research and Science, vol. 4, no. 1, pp. 1–4, 2016.

[30] M. R. Albayati and A. H. Lashkari, "A new graphical Password based on decoy image portions (GP-DIP)," 2014 International Conference on Mathematics and Computers in Sciences and in Industry, Sep. 2014.

[31] S. Sayed, A. Mohid, M. Pal, and M. Haji, "Graphical Password based authentication system with sound sequence," International Journal of Computer Applications, vol. 138, no. 12, pp. 38–43, Mar. 2016.

[32] P. Gunde, and U. Kokate, "Graphical Password authentication by using persuasive click point method,"

International Journal of Science and Research (IJSR), vol. 5, no. 2, pp. 2138–2140, Feb. 2016.

[33] T. M.L., C. D. N., A. I., and D. Atsaam, "An enhanced Password-Username authentication system using cryptographic hashing and recognition based graphical Password," IOSR Journal of Computer Engineering, vol. 18, no. 04, pp. 54–58, Apr. 2016.

[34] "Shoulder surfing and Keylogger resistance using Two step graphical Password scheme," International Journal of Science and Research (IJSR), vol. 5, no. 6, pp. 2395–2399, Jun. 2016.

BIOGRAPHIES

Muhammad Ahsan is a student of Master in Computer Science and Technology in Beijing Institute of Technology, China. He completed his Bachelor degree in Software Engineering from University of Agriculture Faisalabad, Pakistan.

Yugang Li is Ph.D in School of Computer Science and Technology in Beijing Institute of Technology, China.