

Implementation of Authentication Mechanism Using Image Segmentation for Web based Applications

Sana Ansari¹, Prof. Avinash Shrivastava²P.G. Student, Department of Computer Engineering, Vidyalankar Institute of Technology, Wadala, Mumbai, India¹Assistant Professor, Department of Computer Engineering, Vidyalankar Institute of Technology, Wadala, Mumbai,
India²

ABSTRACT: Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as “the weakest link” in the authentication chain. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to different attacks. Attackers can observe directly or use external recording devices to collect users’ credentials. To overcome this problem, we proposed an authentication mechanism based on segmenting the images. The images can be user defined and its breaks down in numerous fragments to draw a pattern on it. The system detects the suspicious attack based on the log in history and sends an alert mail to the authentic user. Proposed prototype is going to provide data security on web as well as database in an encrypted and decrypted format. Also facilitates password recovery through email systems where the parts of segmented image are sent to the authorized user and he/she authenticates by clicking the actual segmented image.

KEYWORDS: authentication; images; graphical passwords; segmentation.

I. INTRODUCTION

In recent years, information security has been formulated as an important problem. Main area of information security is authentication which is the determination of whether a user should be allowed access to a given system or resource. In this context, the password is a common and widely authentication method. A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and those wishing to gain access are tested and are granted or denied the access based on the password according to that. The disadvantages of text-based passwords are well known. Password guessing is possible because users keep it simple for remembrance. The attackers are smart enough to guess easy passwords. System Generated passwords are difficult to remember. Text-based passwords are commonly in use but have usability and security issues.

There have been many rising usages of web-based applications as compared to 15 years ago. This is mainly due to several merits of web applications is provided over traditional software [based on the article (LumJia Jun, Brandon) [11].

- Compatibility with devices, web browsers & operating systems
- Capable of performing tasks which were done using host-based software
- Development of new web technologies, languages and procedures have given way to the development of new dynamic applications (i.e. AJAX)
- Easy to use and are more presentable and attractive
- Does not require any additional hardware or software (installation, etc.)
- Configuration and as well as security.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

There are many defencelessness and attack virus for web-based application. This includes both web-specific (i.e. Cross-Site Scripting), as well as generic (i.e. Password Sniffing), all of which leave the user susceptible to being victims of identity theft means the security issue is much greater problem in on the network some solution will be research or find but it's not sufficient such as SSL may fully protect an application due to the introduction of new web concepts such as cloud computing and the growing complexity of attack vectors.

II. LITERATURE SURVEY

Graphical based password techniques have been proposed to solve the limitations of the conventional text based password techniques, because pictures are easier to remember than texts. It is referred as "Picture superiority effect".

Recognition Based Systems.

Recognition-based systems are also known as cognometric systems [10]. These systems generally require that users must memorize the portfolio of images during the process of password creation, and when logged in, the users must recognize their images from decoys. Exceptional ability of humans to recognize images previously seen made the recognition based algorithms more popular. Various recognition based systems have been proposed using different types of images, mostly like faces, icons, everyday objects, random arts, etc.

Recall Based Systems.

Pure recall-based graphical password systems are also referred to as drawmetric systems because users recall an outline drawing on a grid that they created or selected during the registration phase. In these types of systems, users usually draw their password either on a grid or on a blank canvas. Memorability is difficult in case of recall is a difficult as retrieval is done without any reminders or cues. The first graphical password system proposed in this category was Draw-A-Secret (DAS) [09]. In this, Users are asked to draw their password on a 2D grid through a stylus or mouse. The drawing can consist of one continuous pen stroke or preferably, several strokes separated by "pen-ups" that continue the next stroke in a different cell. To successfully log in, users must redraw the same path through the grid cells.

Hybrid Schemes

Zhao and Li [11] proposed a Textual-Graphical Password Authentication scheme (S3PAS) to resist the shoulder surfing attacks. This scheme combines advantages of both textual and graphical passwords and is resistant to shoulder-surfing, spyware and hidden-camera attacks. At the time of registration, user has to select a string k as the original textual password. Password length may vary on different environments and for different security requirements. During login, user has to find the original password in the login image and then click inside the invisible triangles, called "passtriangles", created by the original password.

Various Attacks on the System.

Some common methods that attackers use for discovering a victim's password include:

- Guessing
- Online Dictionary Attack
- Offline Dictionary Attack
- Offline Brute Force Attack
- Shoulder Surfing Attack

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

TABLE I. Analysis of various schemes with respect to different attacks

Table 1. summarizes the security of the different graphical password schemes we analyzed. ‘Y’ means Yes, that it is

Category of Schemes	Scheme	Attacks				
		Dictionary Attack	Guessing	Shoulder Surfing	Spyware	Social Engineering attack
Recognition Based	Passfaces	Y	Y	Y	N	D
	Cognitive	Y	Y	Y	Y	D
Recall Based	DAS	N	N	N	Y	M
	PassDoodle	N	N	N	Y	E
Cued Recall Based	Passpoints	N	Y	N	N	D
	CCP	N	N	N	N	D
Hybrid Schemes	CAS	Y	N	N	Y	D

resistant to that form of attack. ‘N’ means No that the scheme is open to attack. In Social engineering attack, ‘E’ indicates Easy as the attack is highly effective. ‘M’ denotes Middle that difficulty has increased. ‘D’denotes the attack is difficult.

III. IMAGE SEGMENTATION

Image segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as super pixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze.

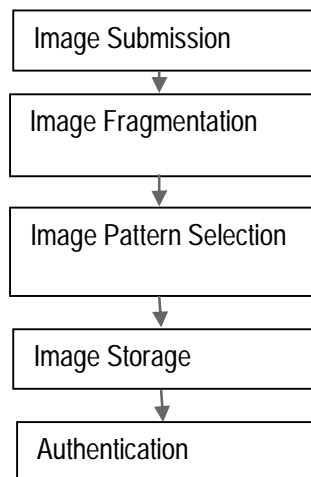


Figure 1: Flow of the System

The proposed system is a combination of image passwords as well textual passwords for providing more secure authentication. It has two main modules: first module is the registration process and second module is the login process.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

In the registration process the user registers through providing basic details and username with even entering a textual password. Further the user selects number of the images he requires for authentication. The more the number of images he selects more secures his/her authentication will be.

Further user, selects the grid size in which the image gets segmented into blocks and small segments. These segments are further stored in the database which are send to the server side and it gets shuffled accordingly. The shuffled fragmented images are presented to the user on which user selects the patterns depending on his will, he/she can either select some or all the segmented images.

The second module is the login module where the user logs in with the username then the first segmented image appears and user draws a pattern on it. If the pattern on the first image appears to be right, then the user is redirected to second image which he/she selected during registration process. If user selects the wrong pattern, then the user will be directed to random images for further authentication. If this process happens twice then an alert mail to authenticate user will be sent by the administrator.



Figure 2: Basic modules of Authentication System.

IV. IMPLEMENTATION

Proposed System includes various aspects during implementation which can be expressed as:

- **Registration of User:**

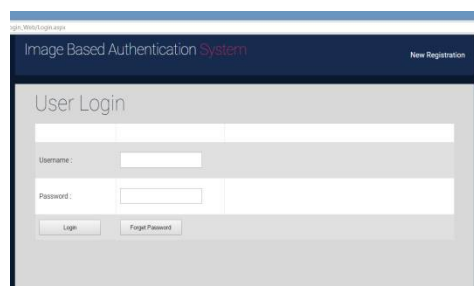


Figure 3: User Login Form

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

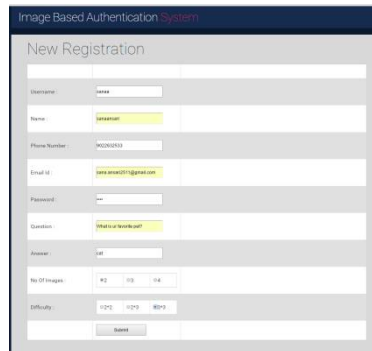


Figure 4: User Registration Form

In this module the user registers before it gets access to the system by entering the basic details and providing correct email-id and phone number for future verification as an authentic user and which will be useful to the administrator if any suspicious act will be taking place or someone is trying to attack or login.

- **Selection of Images:**

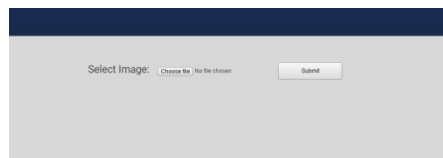


Figure 5: Image Selection Form

In this module the user selects an image then selects the level of difficulty so the image gets stored in the database which further gets segmented using image segmentation technique and can do this process thrice for secure authentication.

- **Segmentation of image:**

In this module the image is stored in the database and gets segmented depending upon the grid size. The segmentation can be division of the images based on the difficulty level for example an image can be segmented into matrix of 3X3 or 6X6 or even 9X9.



Figure 6: Image Segmentation

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

- **Submission of Image:**

The image gets stored in the database and different segments are stored differently. Whenever user logs in the image segments appear in a disordered form and the user selects based on the pattern selected during registration.

- **User Authentication:**

User logs in after registration the segmented images gets displayed to the user and then user selects the desired pattern which he has provided during registration. If user forgets password so the different types of segmented image is send to the desired email id and user verifies by selecting one of them so the password can be retrieved. If the user selects the wrong pattern on the segmented image an alert mail and message is send to the authentic user's email id which comes to know that something suspicious is happening.

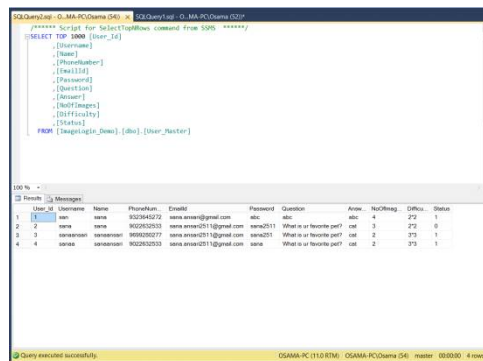


Figure 7: Database Status bit set to 1 or 0

- **Data Security:**

This module is going to consider security aspect of the proposed system. We are going to secure the System by implementing encryption and decryption of data for the authentic user's data. Further the data cannot be retrieved by any hacker as it will be in encrypted form.



Figure 7: Files Stored in Encrypted Form

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

V. CONCLUSION

Our work is one step forwarding the paradigm of using segmentation and patterns for security. Of reasonable security and usability and practical applications Thus the proposed system will be more effective authentication system that provides more security to data and protection against different attack. The authentication system is based on graphical password which segments the image based on various difficulty levels.

For successful login user selected the segmented image in the same pattern which is chosen by user during a registration and this system also provides alert message and email which provides more security to data.

REFERENCES

- [1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. IEEE TRANSACTIONS ON INFORMATION FORENSIS AND SECURITY, VOL.9, NO 6, June 2014.
- [2] Hossein Nejadi, Ngai-man Cheung, Ricardo Sosa and Dawn C.I.Koh. DeepCaptcha: An Image CAPTCHA Based on Depth Perception. ACM digital Library, March 2014.
- [3] Hady Ellis. The Science behind Passfaces. www.realuser.com, Feb 2012.
- [4] De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128-152, 2005.
- [5] P.R. Devale Shrikala, M. Deshmukh and Anil B. Pawar. Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme. International Journal of Soft Computing and Engineering, Volume-3, Issue-2 May 2013.
- [6] Iranna A M and Pankaja Patil. Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol.2, Issue 7, July 2013.
- [7] Nilesh Kawale and Shubhangi Patil. A Recognition Based Graphical Password System. International Journal of Current Engineering and Technology, Vol.4, No.2, Apr 10, 2014
- [8] Darryl D'Souza Phani, C. Polina, Roman V and Yampolskiy. AvatarCaptcha: Telling Computers and humans apart via face classification. IEEE, 2012.
- [9] Robert Biddle, Sonia Chiasson and P.C. van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.
- [10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system". International Journal of Human-Computer Studies, 63 (1-2): 102-127, 2005.
- [11] J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens". In USENIX 4th Workshop on Offensive Technologies, 2010. In NordiCHI, pp.383-392. ACM, October 2008.
- [12] H.C. Gao, L.C. Ma, J.H. Qiu and X.Y. Liu, "Exploration of a Hand-based Graphical Password Scheme", Proceedings of the 4th international conference on Security of information and networks, 2011.
- [13] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., "A Novel Cued-recall Graphical Password Scheme", In sixth International Conference on Image and Graphics (ICIG), pp.949-956, 2011
- [14] M. S. Umar, M. Q. Rafiq, and J. A. Ansari, 'Graphical user authentication: A time interval based approach', IEEE Transaction, vol. 2, pp. 856-861, June 2012.