

TWO LEVEL IMAGE BASED AUTHENTICATION SYSTEM

C.Thenmozhi, S.Sathvi, B.Thamotharan

School of Computing, SASTRA University, Thanjavur.

thenmozhi.kct@gmail.com, sathvisubramanian@gmail.com, balakrishthamo@gmail.com

Abstract:

Authentication plays an important role in protecting resources against unauthorized use. But currently many user authentication systems suffer from drawbacks and security threats. Simple text based passwords are not secure enough and are a burden on the users to remember. The biometric authentication systems which are used for high security systems need additional hardware and software supports and hence are much expensive and difficult to maintain. For certain applications, research suggests that the use of images may be more effective. This is because humans are far better at recognizing images that they have previously seen than they are at remembering passwords. Hence in this paper, we propose user authentication by using image as passwords (PassImages). Though some systems use images for authentication, it still has some drawbacks which are prone to password attacks. On Analysis of the drawbacks of existing password systems, we have proposed solutions that overcome the vulnerabilities and improve the user authentication system.

Key words: *Authentication, Image-based-authentication, PassImage,*

1. Introduction:

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then user is said to be authorized otherwise the user is not authorized. Authentication is needed to let the system perform some tasks for the user. According to the report prepared by Deloitte's Canadian Technology, Media & Telecommunications arm, "More than 90% of user-generated passwords have been proved to be vulnerable to hacking. Even those passwords traditionally considered strong with combination of letters, numbers and symbols are at risk" [5]. It is also predicted that, with the increase in the value of the information protected by passwords, there is also an increase in the number of hack attempts. This eventually leads to an increase in demand for additional forms of authentication by various high-value sites.

2. Existing System:

2.1 Text-Based Passwords

- ◆ In recent years, the inadequacies of the traditional text-based password have been clearly demonstrated. The users of password often aren't much aware of the security. They habitually use similar words as their password and make it guessable. They need to use alphanumeric uppercase, lowercase to set a strong password which is difficult for the users to remember [1]. Sometimes it leads to brute force attack. The password which is typed using keyboard or mouse can easily identified using key stroke, mouse movement and shoulder movement.

2.2 Biometric Security System

In case of the biometric security system the disadvantages are:

- ◆ Iris Recognition and retinal scan needs additional hardware support and are very expensive.
- ◆ Fingerprint and Hand geometry needs scanner and these techniques are futile for dirtiness, injury, arthritis rheumatics and roughness.
- ◆ In the Facial recognition the accuracy is low and it needs camera as additional device.
- ◆ While considering the signature recognition, we need optical pen and touch panel. The accuracy is very less for signature recognition since the signatures are changeable and easy signature is hackable.
- ◆ In case of the voice recognition system, it needs additional devices but the accuracy is medium. It creates problem because voice is changeable due to age, cold, noise, etc.

Other than these disadvantages the biometric passwords create threats as follows:

If the computer with the biometric information is connected to the web, the data may be easily retrieved. The biometric information copy can also be fabricated. It is more expensive hence it is not economically an advantageous technology. Hence the social acceptance of these techniques are medium-low. [4]

The solutions for these problems are to set images as password which is easy to remember and less vulnerable to password attacks. But currently the system that uses images for authentication is also not well premeditated.

Hence it also leads to some password hacks. The static image which is kept to set PassImage leads to mouse movement, shoulder movement and key attack. The password length constraint may cause brute force attack. But these problems can be avoided by using image for authentication purpose.

3. Proposed System- 'T-IBA-S'

This paper proposes the experimental authentication system 'T-IBA-S' - Two Level Image Based Authentication System, which is designed to avoid the problems that are faced by the existing password authentication systems. Two levels of authentication have been designed to avoid the vulnerabilities of current employed systems. Hence the design is made up of two main stages:

3.1 Registration Stage

At the registration stage, the users are required to fill their details such as username, e-mail address and any other detail marked with *. The type of PassImage such as co-ordinate selection, multiple image selection, upload image. Once the user selects the type of PassImage, they will be transferred to the corresponding page to set the password.



Fig 3.1.1 Registration Stage

- ◆ In the Co-ordinate selection, the user has to select any image from the list and choose a co-ordinate position in that image. Here, an image and its corresponding co-ordinate are saved as PassImage.

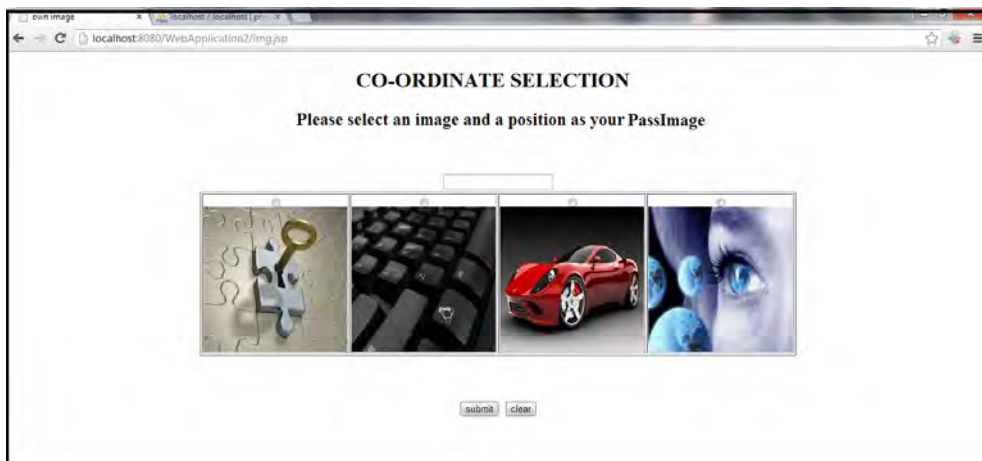


Fig 3.1.2 Co-ordinate Section Registration

- ◆ In the Multiple Image selection, the images are displayed in the grids with the changing of position for every turn and refresh. The user can select any number of images as their PassImage and they are saved as the PassImage.

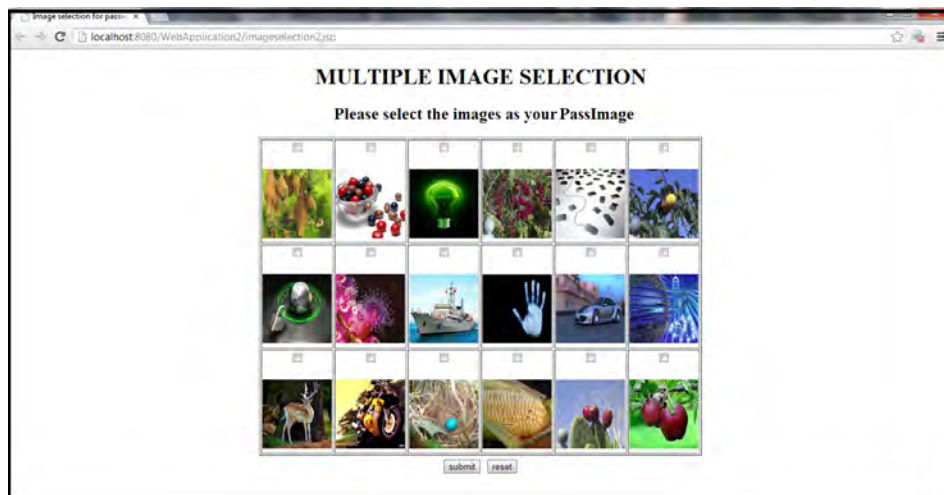


Fig 3.1.3 Multiple Image Selection Registration

- ◆ In the Upload Image, the user is required to upload an image into the system and he can choose a co-ordinate position on that image. Here, the uploaded image and its corresponding co-ordinate are saved as PassImage.



Fig 3.1.4 Upload Image Registration

3.2 Login Stage

In the login Stage, the user needs to enter the correct username, PassImage Type. The selection of correct PassImage type forms the first level of authentication.

And the selection of correct PassImages forms the second level of authentication.

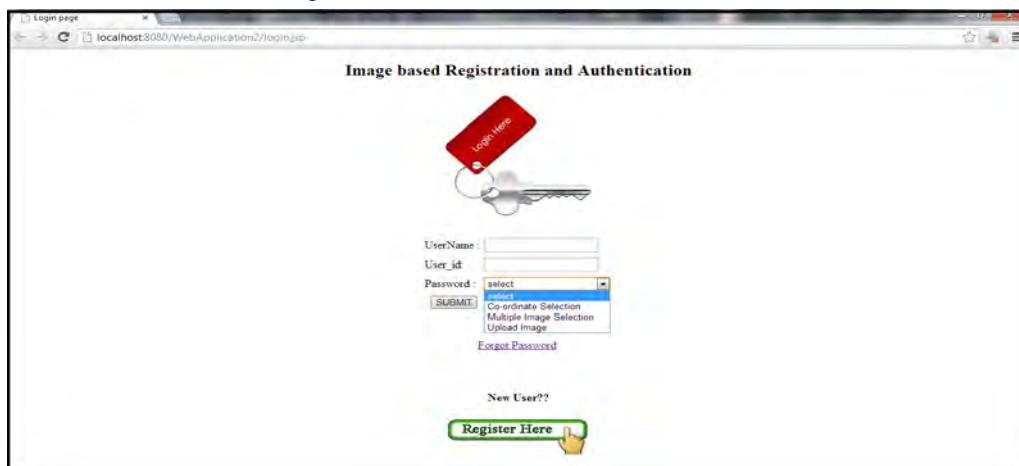


Fig 3.2.1 Login Page

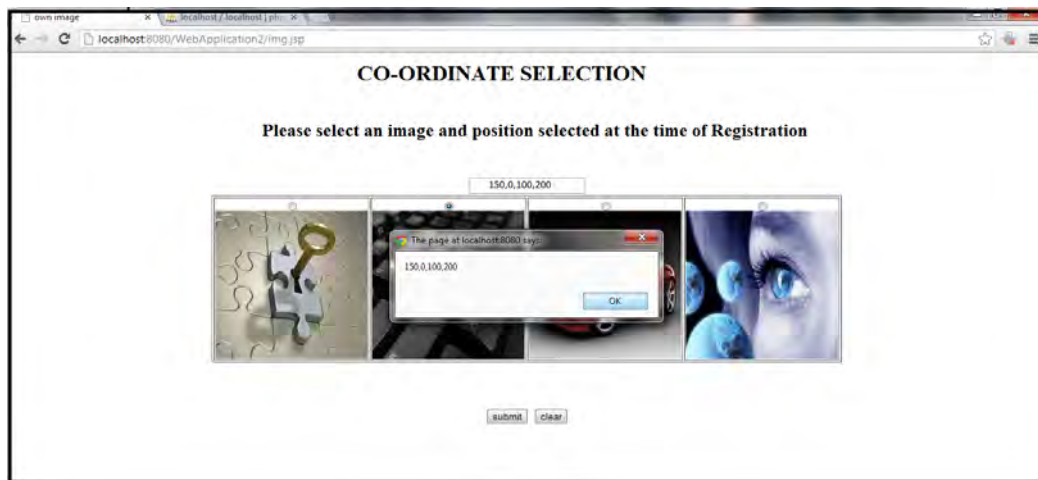


Fig 3.2.2 Co-ordinate Selection Login

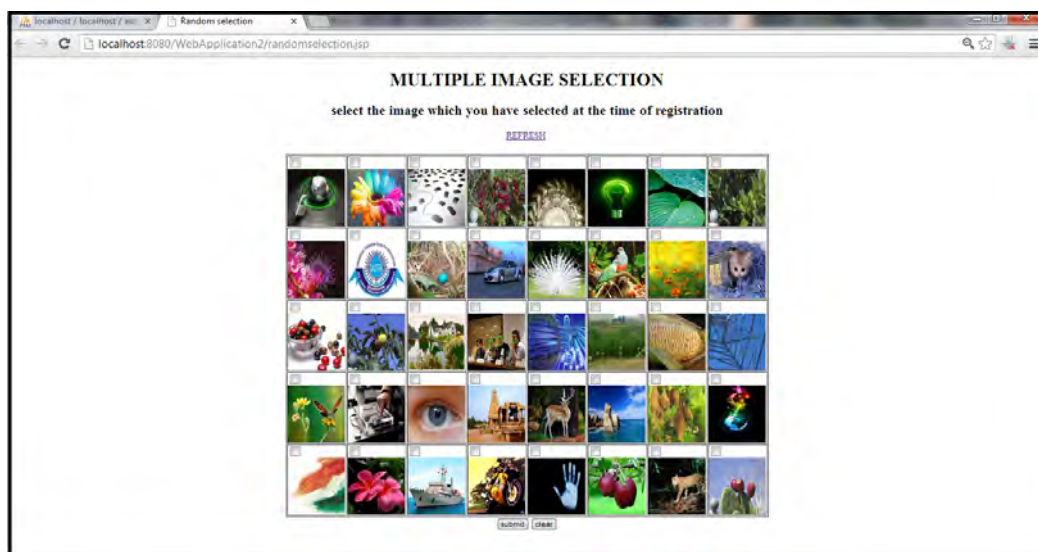


Fig 3.2.3 Multiple Image Selection Login

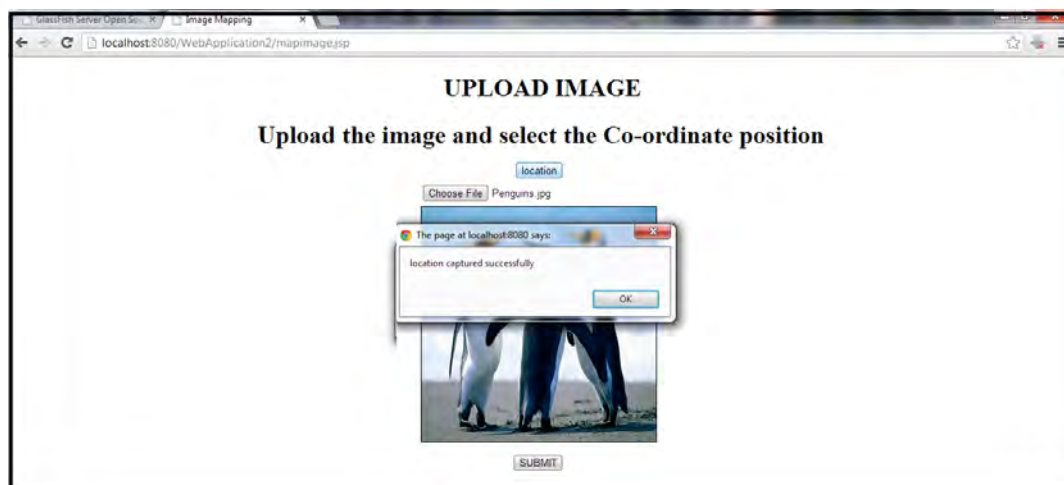


Fig 3.2.4 Upload Image Login

Benefits of T-IBA-S:

- ◆ The Two Level Authentication:
The users are directed to PassImage selection only if they choose correct type. Hence it cannot be guessed and strengthens the security.
- ◆ Session Expiry:

The user is allowed for only a certain number of wrong trials and the session will expire for certain hours to avoid Brute Force attack.

◆ Flexibility in PassImage selection:

The user can select any type of PassImage according to his convenience. So the users can easily remember their PassImage.

◆ BLOB and Hash value generation of images:

Since the image stored is BLOB, the storage area is reduced and hash value is generated to avoid duplication [6].

◆ No constrain on password length:

The pin based system has only 256 ASCII characters, text based passwords supports only 36 characters, particularly the ATM machines supports only 10 digits and constraint to 4 digits[1], which are brute force able. Whereas here the user is allowed to set the length of PassImage to their convenience. The images that can be stored are indeterminate and hence are non brute force able.

◆ Random position of images:

The grid of images, change position on every turn and refresh. This avoids the shoulder attack, mouse movement attack and key stroke attack.

4. CONCLUSION:

The system uses Image based passwords and integrates image registration and authentication. This method is thought to solve the traditional problems related to the authentication process in the internet environment by exploiting the human brain's ability in image recognition. The advantage of this method is that it is user-friendly, secure and cost effective. It can also be used both in heterogeneous network and with different devices. Thus, the paper effectively demonstrates that T-IBA-S can be used to improve the process of user authentication.

REFERENCES

- [1] Haitham Al-Sinani, Chi Nguyen, Branislav Vuksanovic, 2009.“ ‘H-IBAS-H’- Authentication System for University Student Portal using Images”. International Conference on Communication, Computer and Power.
- [2] Srinath Akula, Veerabhadram Devisetty. Image Based Registration And Authentication System, Department of Computer Science.
- [3] Lee Jackson, 2006. Analysis of Image-Based Authentication and its Role in Security Systems of the Future.
- [4] <http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies>
- [5] <http://finance.yahoo.com/blogs/the-exchange/password-isn-t-safe-90-vulnerable-hacking-213820350.html>
- [6] Richard E. Newman, Piyush Harsh and Prashant Jayaraman.“Security Analysis Of and Proposal for Image-Based Authentication”. CISE Dept, university Of Florida.