RESEARCH ARTICLE OPEN ACCESS

Improving Login Authorization by Providing Graphical Password (Security)

R.V.Sudhakar[1], A. Mruthyunjayam[2], D. Suguna Kuamari[3], M. Ravi Kumar[4], B.V.S. Ramesh Babu[5]
Associate Professor, CSE, St. Martin's Engineering College, Hyderabad, India[1]
Asst Professor, CSE, St. Martin's Engineering College, Hyderabad, India[2]
Asst Professor, CSE, St. Martin's Engineering College, Hyderabad, India[3]
Asst Professor, CSE, Abhinav Hi-Tech Engineering College, Hyderabad, India[4]

Abstract
Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods where in graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this project work merges persuasive selective click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.
Keywords: graphical password, shoulder-surfing, Intersection attack , User Authentication, Graphical User Authentication, , Security, task performance, memorability.

I. INTRODUCTION

Because of increasing threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Users interact with security technologies either passively or actively. For passive use understandability may be sufficient for users. For active use people need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction. Today there is an increasing recognition that security issues are also fundamentally human computer interaction. Authentication is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords are used widely for authentication, but other methods are also available today, including biometrics and smart cards. However, there are problems of these alternative technologies. Biometrics raise privacy concerns and smart cards usually need a PIN because cards can be lost. As a result, passwords are still dominant and are expected to continue to remain so for some time. Yet traditional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can exploit. The "password problem", arises because passwords are expected to comply with two conflicting requirements, namely:

1. Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2. Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text. Meeting these conflicting requirements is almost impossible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure way. Many problems that users have with alphanumeric passwords are related to memo ability of secure passwords. In an attempt to create more memorable passwords, graphical password systems have been devised. In these systems authentication is based on clicking on images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented. In recent work we have created a new kind of graphical password

system, called PassPoints, and have done studies of its human factors characteristics compared to alphanumeric password, in this paper we report on further research on usability and memorability of our system under different conditions. In specific we investigate the effect of the tolerance, or the margin of error, allowed when entering one's password points and the effect of the choice of images used in the password system. The following section briefly describes the difficulties users have with traditional passwords and the alternative of graphical passwords. This is followed by a description of PassPoints and a summary of our recent results comparing PassPoints to alphanumeric passwords.

II. SYSTEM OVERVIEW

Our goal was exploratory – to investigate a small number of images in order to get a sense of how sensitive performance in Pass Points is to the images used. We found that there were no striking differences in performance, either in the learning phase or the retention phase. As expected, there was a significantly higher number of incorrect password submissions in R2, and input times for incorrect and correct password submissions in R2 were longer.

However, there were few significant differences among the images. There were some differences in perceptions of the image groups, with the MURAL group usually more positive. Our sense of the results is that users can successfully use a variety of images. Nevertheless, we did observe that, although not significant, there was a trend for some images to perform more poorly than others. The POOL image tested most poorly in many of the analysis, whether it would be learning, retention, or participant perceptions. A possible explanation is that the POOL image had many more definable objects than, for example, the MURAL image, i.e., more choice and many objects that are very close together, which may have subtly affected memory. The POOL picture also had some large objects and several participants chose the large objects, such as umbrellas, but later were unable to home in on the correct part of the object. The trend for some images to perform better than other, suggest that there are likely to be better and worse images to use as password images. Unfortunately, specific criteria for a "good" image are not known and may only be discovered through research or practical experience. Clearly, one could find many bad images that should be avoided, for example, images with few memorable click points, such as an image with large expanses of blue sky or jumbled, incomprehensible scenes. Other images that one would want to avoid might be images with little color or low contrast.

Abstract images are also likely to be poor password images. Abstract swirls of color were used, apparently successfully, in but that system was based on image recognition. A swirl of color or other abstraction would probably be a poor image for a system based on clicking specific memorable area in an image. Images that are pleasant and have positive affect may support memorability. Finally, images associated with the individual graphical password user may be memorable, but pose the danger that someone who knows the user would be able to guess the password. While research from psychology helps, unfortunately limited knowledge about the relationship of image content and memory makes choosing password images an art rather than a science. It appears that many images are probably usable and the main goal should be to avoid bad images that will confound memory. While an image with poor memory characteristics may be acceptable if frequently used, it will probably be quite susceptible to forgetting in infrequent use.

Existing system with limitations

In existing system, passwords are mostly of text oriented. So the password can be broken by intruders by masquerading, brute force attack, dictionary attack etc., There are some application existing with graphical passwords, their major drawback is larger memory space. Some have prone to shoulder surfing attack. In Cued Click Point, the user has to select click point in five different images in sequence based on the previous image. The drawback of the concept is, it is difficult to remember the click points in different images.

Proposed system with features:

In proposed system, we use a click-based graphical password system. During password creation, User has to upload a image of his choice which is further used for authentication. After this process the same image is displayed to user to select a part of this image .This selected image area details (co-ordinates of selected area) are stored in system. In user login process, user uploaded image displayed to user, user has to select same part or area of that image that he selected in password creation process. If not user is unable to login into the system. Therefore this works encouraging users to select more difficult passwords to guess.

III. THE WORKING PRINCIPLE

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Module1:User

This module provides the access to the registered user to access system. The registration

process user has to provide the details like name, email-id, gender, date of birth and select a security question, provide answer for this question. This password, security questions and its answer details required when updating process.

Module2:Password Creation

Allows the registered user has to select the graphical password. User can upload their desired image which is further used for authentication. After this process the same image is displayed to user to select a part of this image .This selected image area details (co-ordinates of selected area) are stored in system.

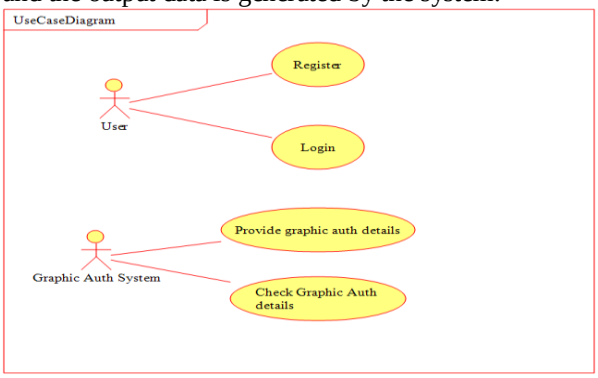
Module3:Authentication System

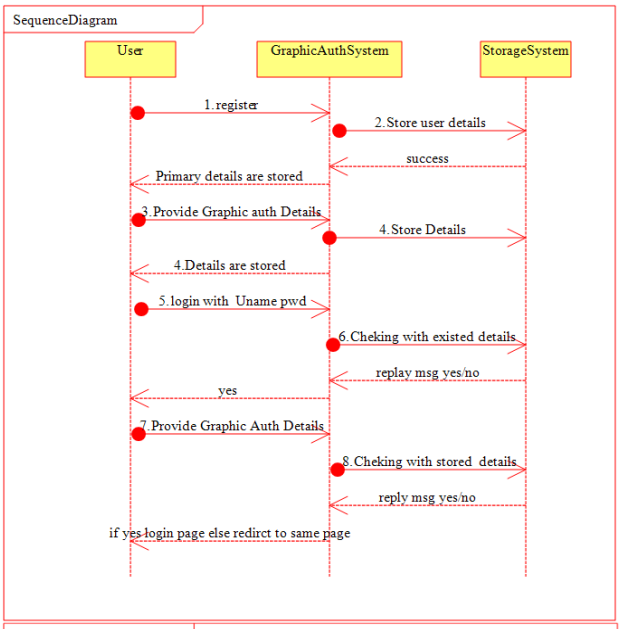
After user registration and password creation process, now user is able to access the system. In user login process, authentication system displays the image to user which he uploaded in system, now user has to select same part or area of that image that he selected in password creation process. If not user is unable to login into the system. User can update his graphic password details by providing correct details like password, answer for security question.

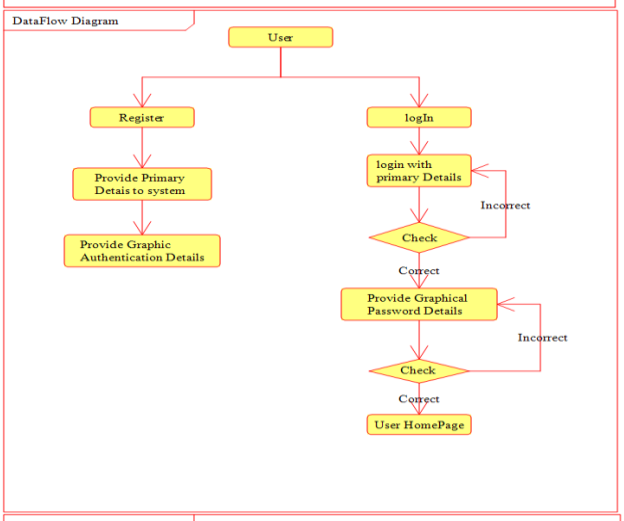
IV. SYSTEM DESIGN

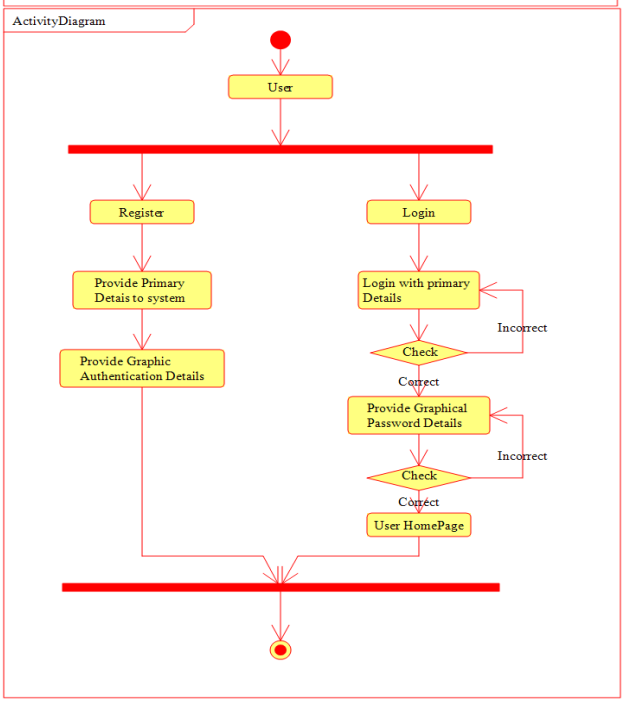
Data Flow Diagram / Use Case Diagram / Flow Diagram

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.







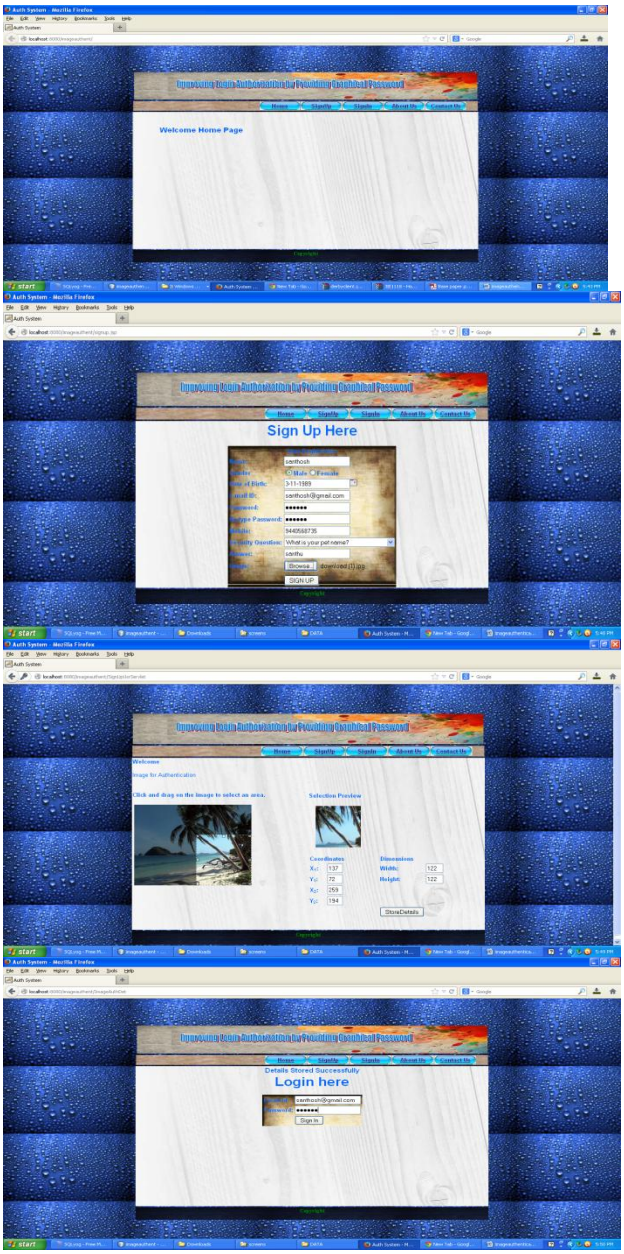


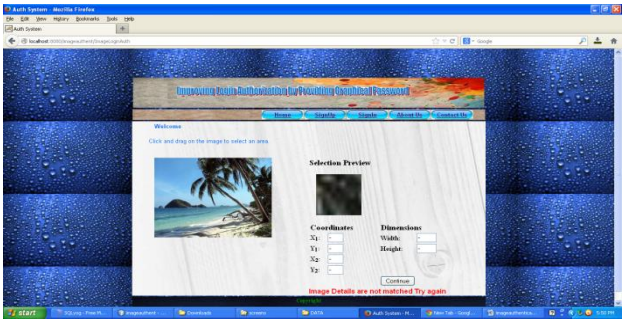
V. CODE IMPLEMENTATION

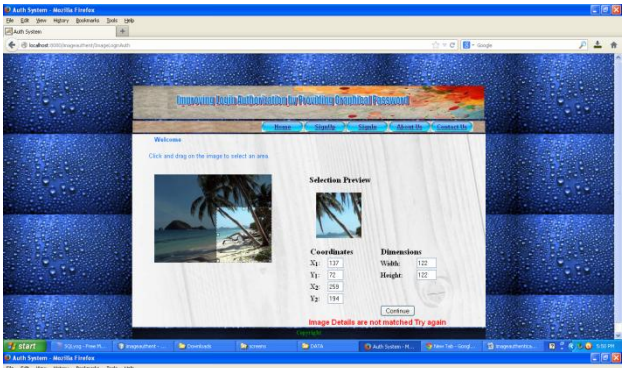
ImageLoginAuth.java

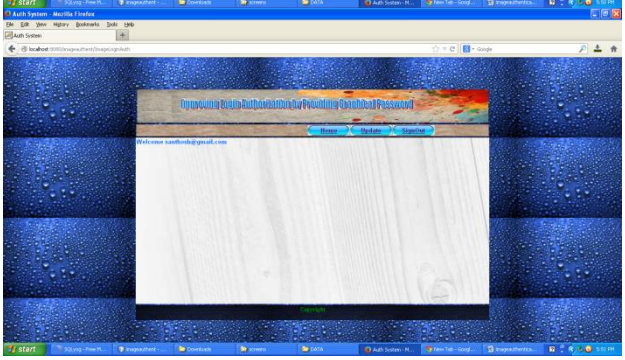
```
/*To change this template, choose Tools Templates
and open the template in the editor. */
package action;
import dao.ImageDAO;
import dto.ImageDTO;
import dto.UserDTO;
import java.io.IOException;
import java.io.PrintWriter;
import java.sql.SQLException;
import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;
public class ImageLoginAuth extends HttpServlet
{
protected void processRequest(HttpServletRequest
request, HttpServletResponse response)
throws ServletException, IOException,
ClassNotFoundException, SQLException {
response.setContentType("text/html;charset=UTF-8");
PrintWriter out = response.getWriter();
HttpSession session = request.getSession();
String email = (String)session.getAttribute("email");
ImageDTO  objImageDTO = new ImageDTO();
objImageDTO.setHeght(request.getParameter("height
"));
objImageDTO.setWidth(request.getParameter("width"
));
objImageDTO.setX1(request.getParameter("x1"));
objImageDTO.setX2(request.getParameter("x2"));
objImageDTO.setY1(request.getParameter("y1"));
objImageDTO.setY2(request.getParameter("y2"));
int  b= ImageDAO.checkImgAuth(objImageDTO,
mail);       if (b>0) {
RequestDispatcher rd =
request.getRequestDispatcher("home.jsp");
rd.forward(request, response);
} else {
RequestDispatcher rd =
request.getRequestDispatcher("loginNextStep.jsp?msg
=Image Details are not matched Try again");
rd.forward(request, response);
}  }
protected void doGet(HttpServletRequest request,
HttpServletResponse response)  throws
ServletException, IOException {
try {
processRequest(request, response);
}
catch (ClassNotFoundException ex) {
ex.printStackTrace();
}
catch (SQLException ex)
{   ex.printStackTrace();
}
}
protected void doPost(HttpServletRequest request,
HttpServletResponse response)  throws
ServletException,  IOException {
try {
processRequest(request, response);
}
catch (ClassNotFoundException ex) {
ex.printStackTrace();
ex.printStackTrace();
} catch (SQLException ex) {
ex.printStackTrace();
}
}
public String getServletInfo() {
return "Short description";
}
}
```

VI. EXPERIMENTAL RESULTS









VII.CONCLUSION

With respect to the tolerance experiment, we can conclude that the smaller tolerance of 10 x 10 pixels seriously impaired user's memory, and correspondingly increased their password input time, after one week in which the password was not used. Our interpretation of this phenomenon is that users who forgot their passwords failed in the learning phase to encode their password points in memory precisely. Generally, they were able to identify the area of their point but had not stored sufficiently precise knowledge about the points. With the small tolerance they were much less likely to click within the tolerance than users in the larger 14 x 14 pixel tolerance. This effect would be likely to decrease with long-term, regular use of the password, i.e., as their performance became more automated. However, if that precise memory decayed over a long lapse in usage, the user would again be susceptible to failure because of the small margin of error. In the images experiment we found that there were few significant differences among several images of everyday scenes. Using guidance from psychology as well as intuition one may be able to choose images that are sufficiently good password images and avoid at least the worst images that interfere with memorability. However, further work on password images is needed to determine to what extent images have "hot spots" that attract many users to choose password points in the same small areas. If hot spots occur frequently, then they reduce entropy of the system. This phenomenon has been shown in face recognition graphical passwords, but the danger may be less in our system with good choice of images to avoid hot spots. We plan to begin studying hot spots by collecting a large number of password points on multiple images.

REFERENCES

[1] Birget, J.C., Hong, d., Memon, N.Robust discretization, with application to graphical passwords. Cryptology ePrint Archive, http://eprint.iacr.org/2003/168, accessed Jan. 17, 2005.

[2] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K.Generating and remembering passwords. Applied Cognitive Psychology 18 (2004), 641-651.

[3] Boroditsky, M.Passlogix Password Schemes. http://www.passlogix.com. Accessed Dec. 2, 2002.

[4] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000).

[5] Adams, A. and Sasse, M.A. Users are not the enemy. CACM 42, 12 (1999), 41-46.

[6] Blonder, G.E. Graphical passwords. United States Patent 5559961, (1996).

[7] Bradley, M.M., Grenwald, M.K., Petry, M.C. and Lang, P.J. Remembering pictures: Pleasure and arousal in memory. Journal of Experimental Psychology 81, 2 (1992), 379-390.

[8] Bahrick, H.P. semantic memory content in permastore: Fifty years of memory for Spanish learned in school. Journal of Verbal Learning and Verbal Behavior 14 (1984), 1-24.

[9] Borges, M.A., Stepnowsky, M.A., and Holt, L.H. Recall and recognition of words and pictures by adults and children. Bulletin of the Psychonomic Society 9, 2 (1977), 113-114.

[10] Biederman, I., Glass, A.L. and Stacy, E.W. Searching for objects in real world scenes. Journal of Experimental Psychology 97 (1973), 22-27.

BIOGRAPHY

Mr Rayapati Venkata Sudhakar register Ph.D in JNTUH in 2012 on cloud computing, Post Graduated in Computer Science & Engineering (M.Tech) , JNTUH , 2008, and graduated in Information Technology (B.Tech) From

JNTU Hyderabad, 2005. He is working presently as Associate Professor in Department of Computer Science & Engineering in **St. Martin's Engineering College**, RR Dist, A. P, INDIA. He has 5+ years Experience. His Research Interests Include Software Engineering & Cloud Computing.

Mr A.Mruthyunjayam, Post Graduated in Computer Science Engineering (M.Tech) From JNTUH,2012, and graduated in Electronics & Computers (B.Tech)from JNTU Hyderabad, 2006. He is working presently as Assitant Professor in Department of Computer Science & Engineering in **St.Martin's Engineering College**, RR Dist, A.P, INDIA. He is has 5+ years Experience. His Research Interests Include Software Engineering, Network Security & Cloud Computing.

Mrs D.Suguna Kuamari, Post Graduated in Computer Science (M.Tech), ANU, 2010, and Graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2006. She is working presently as AssitantProfessor in Department of Computer Science & Engineering in **St. Martin's Engineering College**, RR Dist, A.P, INDIA. She has 5+ years Experience. Her Research Interests Include Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mr Mutyala Ravi kumar, Post Graduated in Computer Science & Engineering (M. Tech) , S R M Deemed University, Chennai , 2006, and graduated in Computer Science & Engineering (B.E) From Velagapudi Ramakrishna Siddhartha Engineering college ,Vijayawada (Nagarjuna University, Guntur, AP),2001. He is working presently as Senior. Assistant Professor in Department of Computer Science & Engineering in **Abhinav Hi-tech college of Engineering**, RR Dist, A.P, INDIA. He has 7+ years Experience.

Mr B V S Ramesh Babu, Post Graduated in Software Engineering (M.Tech) , JNTUH , 2012, and graduated in Computer Science & Engineering (B.Tech) From JNTU Hyderabad, 2007. He has 5+ years Experience. His Research Interests Include Network Security, Software Engineering & Cloud Computing.