Graphical Authentication System

A Sivasankar Reddy[1], M Kusuma[2]
[1] *Student, Dept. of MCA, EAIMS*
[2] *Professor, Dept. of MCA, EAIMS, Tirupati, A.P.*

***Abstract*- This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.**

***Index Terms*- purpose of the system, existing system, proposed system, architecture, modules.**

I. INTRODUCTION

The objective is to develop a system, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly. Online business review/rating.

Purpose of the system

This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. The accuracy perspective focuses on the successful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase.

1.2 Existing System

In order to be more secure than the existing Android pattern password with entropy 18:57 bits against brute force attacks, users have to set two pass-images and use the graphical method to obtain the one-time login indicators. Like most of other graphical password authentication systems, PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing. TEXTUAL passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

1.3 Proposed System

The proposed system maintains a centralizes database to store information related to blood donors and

blood providing organizations. The system maintains means it coordinates the details of donors and organizations at one place. The system allows one to access the information about the particular donors or organizations. Nonusers can interact with our system and they can get the details of the donors and organizations. Through our system the nonuser can also become as a donor.

Advantages:

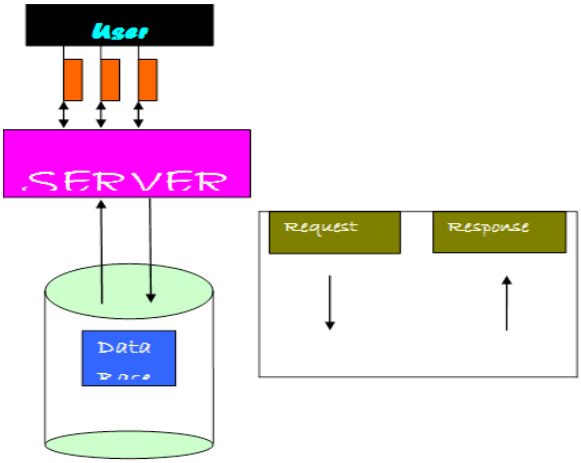
1) Any communication between the client device and the server is protected by SSL so that packets or information will not be eavesdropped or intercepted by attackers during transmission.

2) The server and the client devices in our authentication system are trustworthy.

3) The keyboard and the entire screen of mobile devices are difficult to protect, but a small area (around 1:5 cm2) is easy to be protected from malicious people who might shoulder surf passwords.

4) Users are able to register an account in a place that is safe from observers with bad intention or surveillance cameras that are not under proper management.

II. ARCHITECTURE DIAGRAM



III. MODULES

The project has been divided into 7 different modules:

1. Multi Layer Image Authentication
2. Random Guess Attack
3. Login / Register
4. Upload Image
5. View Status
6. View Requests
7. Approve / Cancel

3.1 Multi Layer Image Authentication

To overcome (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues to devices, we introduced a graphical authentication system called Pass Matrix. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. Figure 5 demonstrates the proposed scheme, in which the first pass-square is located at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image. In Pass Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points [7] scheme. Based on the user study of Cued Click Points . CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image the login will be failed

Fig. 5. A password contains three images (n=3) with a pass square in each. The pass squares are shown as the orange-filled area in each image.

3.2 Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each pass image until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of Pass Matrix against random guess attacks, we define the entropy of a password space as in equation 3. Table 7 defines the notations used in the equation. If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

3.3 Login / Register

Me X will provide a secure user-id/password based secured login mechanism to access its services.

3.4 Upload Image

This is the main module in this application. The Main Process in the Mex application will be worked here. The bill picture is already stored in the mobile gallery. The user will select the picture from the gallery and upload in to the server. And also upload the details like employee name, employee id and Bill details. All the details uploaded here is stored in to the wamp server.

3.5 View Status

After uploading the details the user can check the status of the request using the same application. The status will be shown as pending until the higher authority accept or cancel the Request.

3.6 View Request

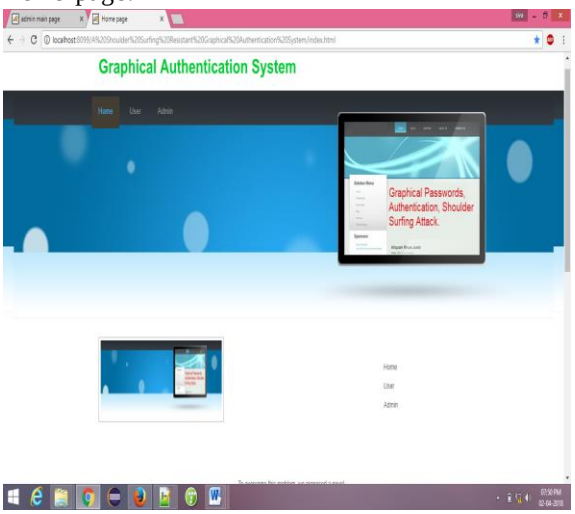
The User Requested data can be view by the Higher authority. Admin is the authority to accept or reject the request. This module is done by using PHP. The Admin will use System to view the request

3.7 Approve / Cancel

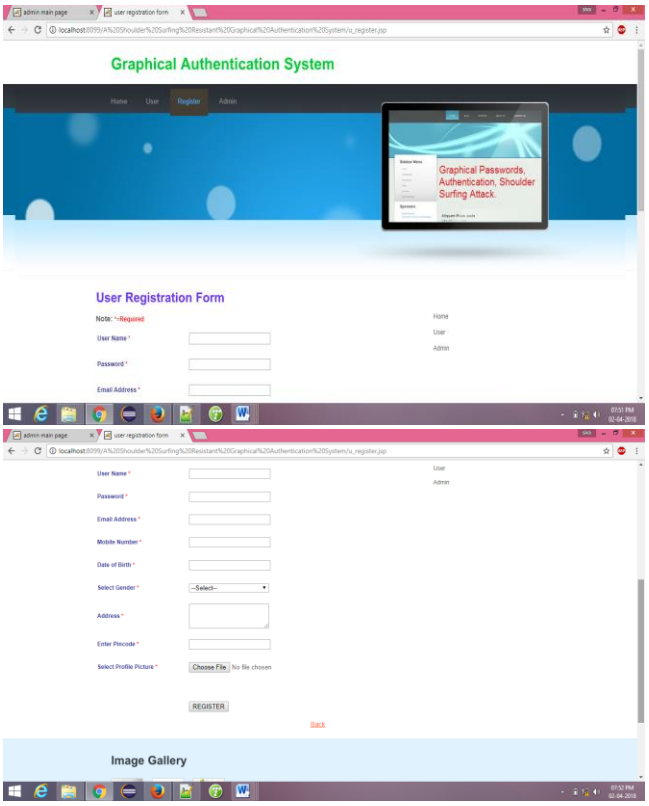
After viewing the Request the admin can have the permission to accept or reject the request. The user can check the status.

IV. SCREENSHOTS

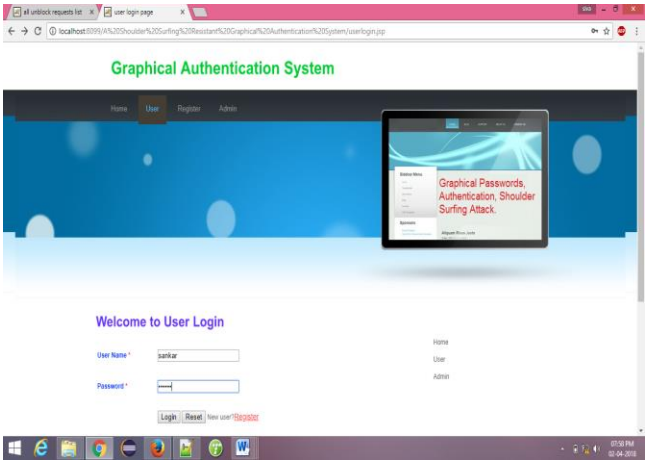
Home page:



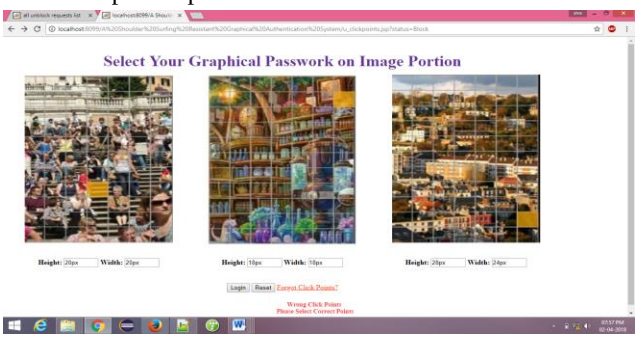
User Registration Fome:



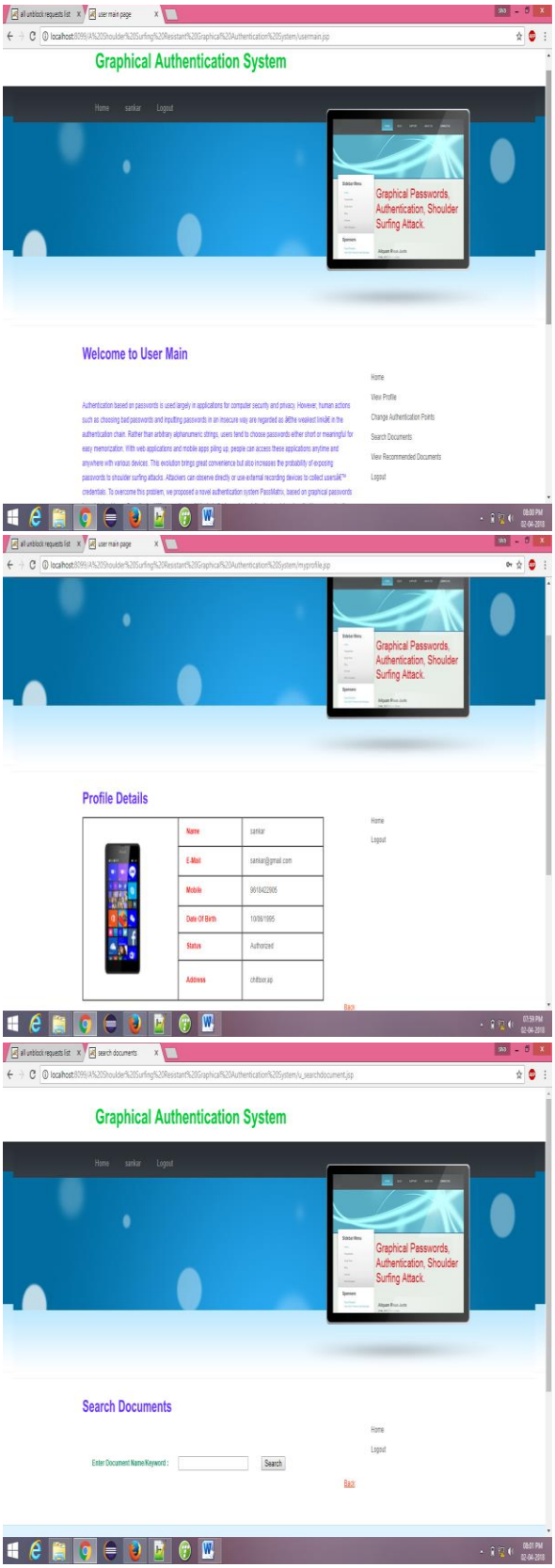
User login:



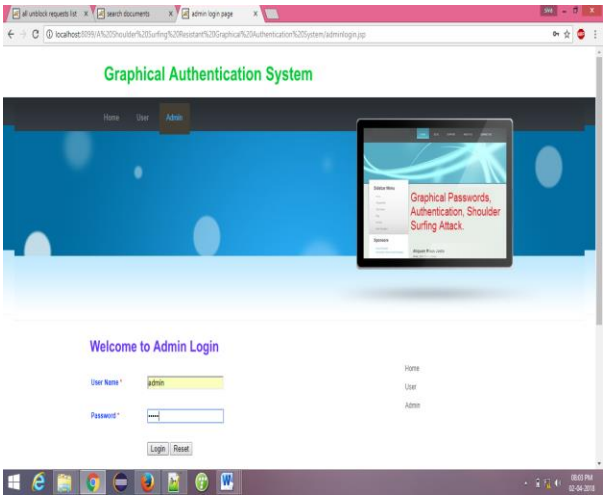
Select Graphical points:



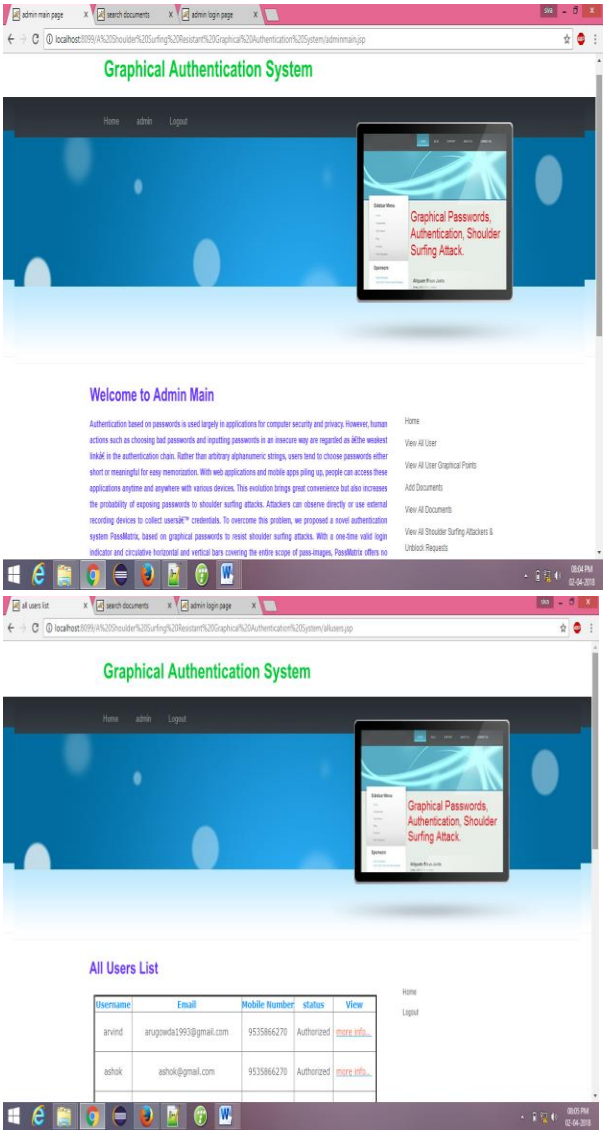
User menu:

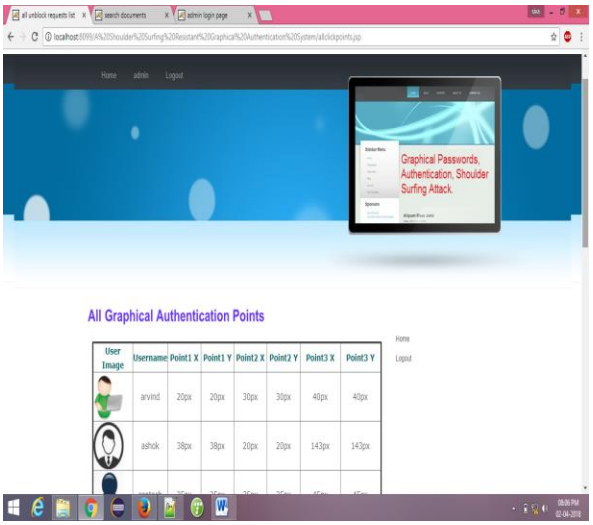


Admin Login Form:

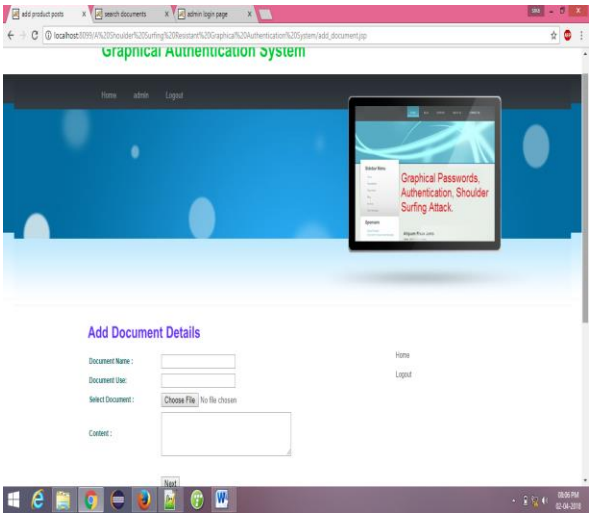


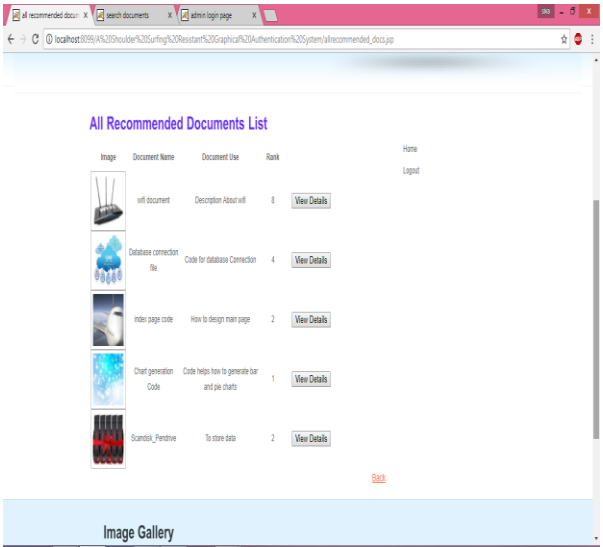
Admin Menu:




Graphical Passwords, Authentication, Shoulder Surfing Attack.
All Graphical Authentication Points
User Image
Username
Point1 X
Point1 Y
Point2 X
Point2 Y
Point3 X
Point3 Y
arvind
ashok


Shoulder Surfing Attacks Users Unblock Request List
Image
Username
Requested Date
Action
arvind
04/11/2016 18:15:03
Unblocked
arvind
04/11/2016 18:44:16
Unblocked
arvind
04/11/2016 18:45:45
Unblocked
ashok
05/11/2016 18:31:41
Unblocked
Rajesh
10/11/2016 16:21:59
Unblocked
Rajesh
10/11/2016 17:20:03
Unblocked


Graphical Authentication System
Graphical Passwords, Authentication, Shoulder Surfing Attack.
Add Document Details
Document Name :
Document Use:
Select Document :
Choose File
No file chosen
Content :
Next


All Recommended Documents List
Image
Document Name
Document Use
Rank
wifi document
Description About wifi
8
View Details
Database connection file
Code for database Connection
4
View Details
index page code
How to design main page
2
View Details
Chart generation Code
Code helps how to generate bar and pie charts
1
View Details
Scandisk_Pendrive
To store data
2
View Details
Back


All Documents List
Document Name
Document Image
Document Use
Uploaded Date
Details
wifi document
Description About wifi
02/11/2016 12:51:04
View More..
Database connection file
Code for database Connection
05/11/2016 18:21:12
View More..
index page code
How to design main page
05/11/2016 18:22:21
View More..
Chart generation Code
Code helps how to generate bar and pie charts
07/11/2016 10:48:57
View More..
Scandisk_Pendrive
To store data
10/11/2016 18:09:18
View More..
ws
abc
11/02/2018 15:48:03
View More..

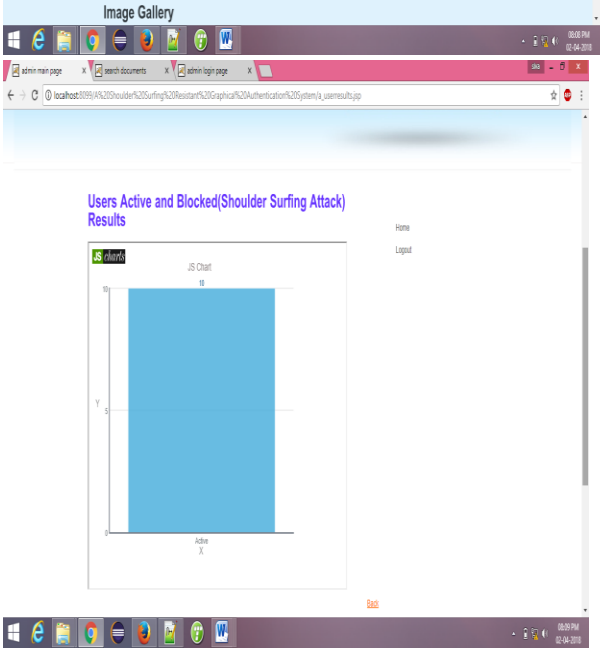
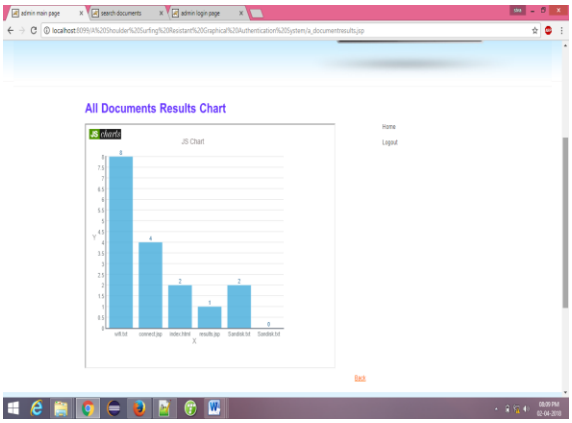


Image Gallery
Users Active and Blocked(Shoulder Surfing Attack) Results
JS Chart
Active
Back



V. CONCLUSION

Instead use the With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to
type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

REFERENCES

References for the project development were taken from the following books and web sites.

[1] JAVA Technologies
[2] JAVA Complete Reference
[3] Java Script Programming by Yehuda Shiran
[4] Mastering JAVA Security
[5] JAVA2 Networking by Pistoria
[6] JAVA Security by Scotl oaks
[7] Head First EJB Sierra Bates
[8] J2EE Professional by Shadab siddiqui
[9] JAVA server pages by Larne Pekowsley
[10] JAVA Server pages by Nick Todd
[11] HTML
[12] HTML Black Book by Holzner
[13] Java Database Programming with JDBC by Patel moss.