**CHAPTER 1**

**INTRODUCTION**

* 1. **NETWORK SECURITY**

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. The primary goals of network security are confidentiality, Integrity, Availability. These three pillars of Network Security are often referred as CIA triangle. Ensuring network security may appear to be very simple. The goals to be achieved seems to be straightforward. But in reality, the mechanisms used to achieve these goals are highly complex, and understanding them involves sound reasoning. Some of these mechanisms are En-cipherment, Digital signature, Access control.

**1.2 SYSTEM OVERVIEW**

With the proliferation of websites, the security level of password-protected accounts are no longer purely determined by individual ones. User may register multiple accounts on the same sites or across multiple sites, and these passwords from the same users are likely to be same or similar. As a result, an adversary can compromise the account of a user on a web forum, then guess the accounts of the same user in sensitive accounts also called as shadow attack on passwords. In our proposed system we utilize image pixel-based authentication. So unauthorized users are preventing from accessing accounts.

* 1. **SCOPE OF THE PROJECT**

The main objective is to reduce shadow attack in text based passwords. Here clued click points is used which makes it more difficult to break graphical passwords. The goal of these methods is to improve the process of user authentication and provide more security. However, in the image pixel based approach the user can remember images easily than passwords. Most probably an attacker cannot easily guess the image pixels passwords and also the user is allowed only for certain number of wrong trials and the session will expire for certain time period then it sends an alert message to the original user’s mail. Thus the unauthorized users cannot easily hack our details.

**CHAPTER 2**

**LITERATURE SURVEY**

**[1] Weili Han, zhigong Li, Guofei Gu, Wenyuan Xu, “Shadow attacks based on password Reuses: A Quantitative Emperical Analysis”, IEEE Transactions on dependable and secure computing, 2018.**

Password-based authentication is one of the most widely used methods to authenticate a user before granting accesses to secured websites. The wide adoption of password-based authentication was the result of its low cost and simplicity. A user can enter his or her passwords anywhere by a keyboard or a touch screen without any other extra devices. The popularity of passwords and the proliferation of websites, however, lead to a concern on password reuses between accounts on different websites or even on the same websites.

**[2] Dheepanshu and Mayank sharma, “Enhancing password security using cyclic group matrix” International conference on telecommunication and Networks(TEL-NET), 2018.**

Password authentication is the first level of security which is used widely, being compromised whenever any intruder attacks an application. In case if password was strong enough threat to the security can be reduced. With more complex password, the possibility is less that attacker will guess the correct string. As an application of group theory, a new cyclic group matrix based password security technique was proposed. As a result of applying the security mechanism the risk of cracking the password was minimized and it enhanced the password security.

**[3]** [**Zubayr Khalid,**](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Zubayr%22&searchWithin=%22Last%20Name%22:%22Khalid%22&newsearch=true)[**Pritam Paul,**](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Pritam%22&searchWithin=%22Last%20Name%22:%22Paul%22&newsearch=true)**[Soummyo Priyo Chattopadhyay, “Secure authentication with dynamic password”, IEEE 7](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Soummyo%20Priyo%22&searchWithin=%22Last%20Name%22:%22Chattopadhyay%22&newsearch=true)[th](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Soummyo%20Priyo%22&searchWithin=%22Last%20Name%22:%22Chattopadhyay%22&newsearch=true) [Annual information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016.](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Soummyo%20Priyo%22&searchWithin=%22Last%20Name%22:%22Chattopadhyay%22&newsearch=true)**

Providing Authentication to any system provides more security to that system. There are many authentication techniques available, such as textual password, biometrics etc. Almost all securities are covered with textual password, still it had some drawbacks. It is not hard for hackers to hack computer system secured with textual password. When user types password, the hacker can trace the elements in the password. The only way for preventing the tracing of elements in the password is to include a lot of possible elements in a password, making the job of tracing the entire password hard. Here the concept of 3-D password has been included. 3-D password can fulfil the expectation of a user by securing an account with a password that may include a large number of possible combinations of elements. Still it can be hacked using Shoulder-surfing attack. Moreover, time and space complexity is large for the concept. The authors have introduced a new concept of securing an account. To prevent any type of hacking activity, they have included the concept of dynamic (changeable) password with system requirements including both software and hardware. New concept along with its simplicity has been verified, thus providing a less time and space complexity than 3-D password.

**[4] Lin zhang and zhenfeng zhang, “Security analysis of an ID based two server password authenticated key Exchange”, IEEE Communication letters, 2016.**

Two server password authenticated key exchange allows the client to split a low entropy password into two pieces and store them in two servers, respectively and the two servers collaboratively authenticate the client and establish session keys. Even though either server was corrupted, it guarantees that the password still remains secured. In 2014, Yi et al. proposed a compiler that transforms any two-party PAKE protocol to a two-server PAKE protocol by dint of the ID based public key encryption system under the standard model. Moreover, it was claimed that the scheme had probably secured in a relevant format model. An existing related key attack to scheme is pointed when one server was corrupted, the adversary can subtly derive the fresh key shared by the remaining two honest parties. In addition to that , they have suggested a simple patch to avoid the concern.

**[5] Ashutosh Gupta and Yogesh Kumar, “Banking security system using hand gesture recognition”, International conference on recent developments in**

**control, automation and power engineering, 2015.**

The hand gesture analysis for human-security system interaction. Hand gesture recognition consisted of five processes such as image acquisition, skin color information for recognizing hand gesture that was obtained from the arm region of the hand, background removal, canny edge detection and contour detection.

**[6] Zhigong Li and Weili Han, “A Large-Scale Empirical Analysis of Chinese Web Passwords”, Usenix security symposium, 2014.**

Users speaking different languages may prefer different patterns in creating their passwords, and thus knowledge on English passwords cannot help to guess passwords from other languages well. Research had already shown Chinese passwords are one of the most difficult ones to guess. But the conclusion is biased because, little empirical study has examined regional differences of passwords on a large scale, especially on Chinese passwords. The differences between passwords from Chinese and English speaking users, leveraging over 100 million leaked and publicly available passwords from Chinese and international websites in recent years. It was found that Chinese prefer digits when composing their passwords while English users prefer letters, especially lowercase letters. The strength against password guessing was similar. Secondly, it was observed that both users prefered to use the patterns that they were familiar with, Chinese Pinyins for Chinese and English words for English users. Thirdly, it was observed that both Chinese and English users prefer their conventional format when they use dates to construct passwords. Based on these observations, a PCFG (Probabilistic Context-Free Grammar) based password guessing method has been improved by inserting Pinyins (about 2.3% more entries) into the attack dictionary and inserting the observed composition rules into the guessing rule set. The experiments proved that the efficiency of password guessing increased by 34%.

**[7] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, “The Psychology of Security for the Home Computer User”, IEEE Symposium on security and privacy, 2012.**

The home computer user was often said to be the weakest link in computer security. They do not always follow security advice, and they take actions, as in phishing, that compromise themselves. In general, they do not understand why users do not always behave safely, which would seem to be in their best interest. Reviews in the literature of surveys and studies of factors that influence security decisions for home computer users. The review was organized in four sections: understanding of threats, perceptions of risky behavior, efforts to avoid security breaches and attitudes to security interventions. These studies revealed a lot of reasons why current security measures did not match the needs or abilities of home computer users and suggested future work was needed to inform how security is delivered to the user group.

**[8] Anupam Das, Joseph Bonneauy, Matthew Caesar, Nikita Borisov and XiaoFeng Wangz, “The Tangled Web of Password Reuse”, NDSS, 2009.**

Today’s Internet services rely heavily on text-based passwords for user authentication. The pervasiveness of these services coupled with the difficulty of remembering large numbers of secure passwords tempts users to reuse passwords at multiple sites. Investigation was done for the first time on how an attacker can leverage a known password from one site to more easily guess that user’s password at other sites. They analyzed several hundred thousand leaked passwords from eleven web sites and a user survey on password reuse was introduced. It was estimated that 43-51% of users reuse the same password across multiple sites. A few simple tricks users often employ to transform a basic password between sites which can be used by an attacker to make password guessing vastly easier. The first cross-site password-guessing algorithm, was able to guess 30% of transformed passwords within 100 attempts compared to just 14% for a standard password-guessing algorithm without cross-site password knowledge was developed.

**[9] Dino Schweitzer, Jeff Boleng, Colin Hughes, Louis Murphy, “Visualizing Keyboard Pattern Passwords”, International workshop on visualization for cyber security, 2009.**

Passwords are a fundamental security vulnerability in many systems. Several researchers have investigated the tradeoff between password memorability versus resiliency to cracking and had looked at alternative systems such as graphical passwords and biometrics. To create stronger passwords, many systems enforce rules regarding the required length and types of characters passwords must contain. The authors suggested the approach was to use passphrases to combat dictionary attacks. One common “trick” used to remember passwords that conform to complex rules was to select a pattern of keys on the keyboard. While appearing random, the pattern was easy to remember. Investigation was done on how often patterns were used, whether patterns could be classified into common categories, and whether those categories would be used to attack and defeat pattern-based passwords. Visualization techniques were used to collect data and assist in pattern categorization. The approach successfully identified two out of eleven passwords in a real-world password file that were not discovered with a traditional dictionary attack. The approach was used to collect and categorize patterns, and they described that the resulting attack method successfully identified passwords in a live system.

**[10]**[**Fawaz A. Alsulaiman**](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Fawaz%20A.%22&searchWithin=%22Last%20Name%22:%22Alsulaiman%22&newsearch=true)**,** [**Abdulmotaleb El Saddik**](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Abdulmotaleb%22&searchWithin=%22Last%20Name%22:%22El%20Saddik%22&newsearch=true)**, “Three-DimensionalPassword for More Secure Authentication”,** [**IEEE Transactions on Instrumentation and Measurement**](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=19)**, 2008.**

Current authentication systems suffer from many weaknesses. Textual passwords were commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords had a password space that was less than or equal to the textual password space. Smart cards or tokens was easily stolen. Many biometric authentications had been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The authors have presented the 3-D password scheme. The 3-D password is a multifactor authentication scheme. To be authenticated, a 3-D virtual environment where the user navigates and interacts with various objects was presented. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determined the 3-D password key space.

**CHAPTER 3**

**SYSTEM ANALYSIS**

* 1. **EXIXTING SYSTEM**

Password based authentication was one of the most commonly used methods to authenticate a user before granting access to secured websites. Large number of password reuses often result in shadow attacks where an adversary easily guesses the password and compromise our accounts. Avoid the hand gesture recognition system was proposed as part of the authentication process. The risk of cracking the password was minimized by using cyclic matrix-based password security. Three-dimensional password also used. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment.

**3.1.1 DISADVANTAGES OF THE EXISTING SYSTEM**

* User may register multiple accounts on the same site or across multiple sites and these passwords from the same users are likely to be the same or similar. As a result, the hacker may guess the similarity of these passwords, in that way they easily misuse our accounts.
* In hand gesture recognition system, similar gestures might have different orientation histograms and different gestures could have similar orientation histograms.
* Three dimensional password is more expensive and it is difficult for blind people.
  1. **PROPOSED SYSTEM**

In addition to providing password, two images are to be chosen by the user at a time of creating account. Along with images, certain pixels from the images are also selected by the user. The user can access his/her accounts only when he types the correct password and also chooses the correct pixels which were already selected. If a wrong pixel is chosen for the first image, then random images appear, instead of the correct second image. If the users repeat choosing wrong pixels, then an alert message is sent to the registered email.

**3.2.1 ADVANTAGES OF PROPOSED SYSTEM**

* Image-pixels based authentication technique provides an additional level of security.
* User is alerted if repeated failed attempts take place. Thus, detection of shadow attacks is made simple.
* Choosing images and pixels is simple and secure compared to gestures technique and 3-d password.

**3.3 REQUIREMENTS SPECIFICATION**

**3.3.1 Hardware Requirements**

Processor : Pentium Dual Core 2.3 GHz

Hard Disk : 250 GB or Higher

Ram : 2 GB

**3.3.2 Software Requirements**

Operating System : Windows 7 or Higher

Languages used : Java (JSP, Servlet), HTML

Tools : JDK 1.7, Net Beans 7.3.1, SQLyog

Backend : MySQL

* 1. **LANGUAGE SPECIFICATION**

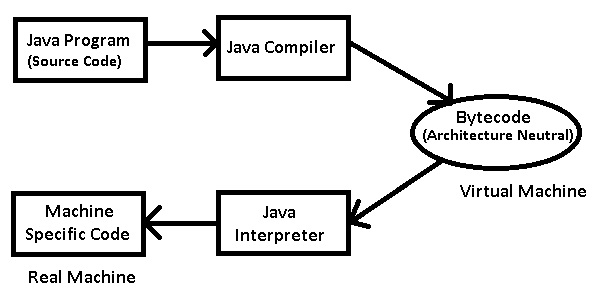
**3.4.1.JAVA**

**Overview**

Java is a general purpose, high-level programming language developed by Sun Microsystems. The Java programming language was developed by a small team of engineers, known as the Green Team , who initiated the language in 1991.Originally called Oak, the Java language was designed for handheld devices and set-top boxes. Oak was unsuccessful and in 1995 Sun changed the name to Java and modified the language to take advantage of the burgeoning World Wide Web.

**Working of Java**

For those who are new to object-oriented programming, the concept of a class will be new to you. Simplistially, a class is the definition for a segment of code that can contain both data called attributes anf function alled methods. When the interpreter executes a class, it looks for particular method by the name of main, whichWill sound familiar to C progammers.

****

**Fig 3.1 Java Virtual Machine**

**The Java Platform**

A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Microsoft Windows, Linux, Solaris OS, and Mac OS. Most platforms can be described as a combination of the operating system and underlying hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.The Java platform has two components:

* The Java Virtual Machine
* The Java Application Programming Interface (API)

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related components. The following figure depicts a Java program, such as an application or applet, that’s running on the java platform

****

**Figure 3.2 Java Platform**

**3.4.2 MYSQL**

MySQLis a database management system (DBMS). A database is a structured collection of data. To access, and process data stored in a database, you need a DBMS. Because computers are very effective at handling large amounts of data, database management plays a central role in computing. But more than being a DBMS, MySQL is relational database management (RDBMS). A relational database stores data in separate tables rather than putting all the data into one large repository. Doing adds tremendous speed and flexibility. MYSQL is easy to use, yet extremely powerful, secure and scalable. And because of its small size and speed, it is the ideal database solution for Web sites.

**3.4.3 NET BEANS**

Netbeans is an [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) for [Java](https://en.wikipedia.org/wiki/Java_(programming_language)). NetBeans allows applications to be developed from a set of modular [software components](https://en.wikipedia.org/wiki/Software_component) called modules.Netbeansrunson [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows),  [macOS](https://en.wikipedia.org/wiki/MacOS), [Linux](https://en.wikipedia.org/wiki/Linux) and [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)). In addition to Java development, it has extensions for other languages like [PHP](https://en.wikipedia.org/wiki/PHP), [C](https://en.wikipedia.org/wiki/C_(programming_language)), [C++](https://en.wikipedia.org/wiki/C%2B%2B), [HTML5](https://en.wikipedia.org/wiki/HTML5), and [JavaScript](https://en.wikipedia.org/wiki/JavaScript). Applications based on NetBeans, including the NetBeans IDE, can be extended by [third party developers](https://en.wikipedia.org/wiki/Third_party_developer).

**CHAPTER 4**

**4.1 SYSTEM ARCHITECTURE**

Username and password verification

Image selection

Pixel selection

Random image generation

1st image pixel verification

2nd image generation

**n** noyes

Repetition of wrong image pixel

selection

2nd image pixel verification

Random image generation

Display Home Page

noyes

**y**

Send alert message to user’s mail

**Figure 4.1 Architecture of proposed system**

In Fig. 4.1 the initial authentication is done using the username and password. If the username and password is validated, then further authentication is proceeded by selecting a particular pixel in the first image. If the first pixel is selected correctly then it jumps to the second image. If the pixel in the second image is also selected correctly, then the user is allowed to login and proceed with the process. If the pixels are not selected correctly, then random images are generated and an alert message is notified to the original user’s mail.

**4.2 USE CASE DIAGRAM**

**User Admin**

**Fig 4.2 Use case diagram**

**4.3 SEQUENCE DIAGRAM**

**System**

**User**

**Admin**

**User**

1.Registration

2.Login

3**.**Usernameandpasswordenter

4**.** Username and

passwordverification

5**.**Image pixelselection

6**.**Pixelverification

**7**.Displayhomepage

8**.**Wrongpixelselection

9.Randomimagegeneration

10. Logout

**Fig 4.3 Class diagram**

**CHAPTER 5**

**5.1 MODULES**

The modules are

1.Image pixel selection

2.Pixel verification

3.Random image generation

4.Alert message to user’s mail

**5.1.1 Image pixel selection**

User authentication is the process of giving individuals access to system objects based on their identity. Initial authentication of the user is done by entering username and password in text type. In registration two images are uploaded and pixel can be selected in two images. In this clued click point technique is used. Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each image rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point.

**5.1.2** **Pixel verification**

when we are login the website using password and then choose the pixel of the two images. If the correct point of the image pixels is chosen and the second image is display. Original user is the one who knows the correct pixel of the image, and others cannot point the image pixels. Using these techniques, the risk of many attacks can be minimized. This design provides protection against password related attacks.

* + 1. **Random image generation**

The correct pixel is not chosen in first image, then random pictures are been generated continuously in two times and the page return to home page, second image cannot display. If we chosen the correct image pixel in first image then second image is display. In that wrong pixel is chosen, the random images are generated continuously in two times. Finally unauthorized users cannot login our account.

* + 1. **Alert message to user’s mail**

Email alerts are emails generated by an automated process and sent to designated recipients. When the unauthorized user can misuse your account, alert message is sent to the original user. In that way original users are alerted.

**CHAPTER 6**

**CONCLUSION AND FUTURE ENHANCEMENT**

**6.1 CONCLUSION**

Currently shadow attacks are so common because it can attack globally

and capture the user’s confidential details. This system will provide more security and minimize the risk of many attacks.

**6.2 FUTURE ENHANCEMENT**

In this proposed system integrating text passwords with images is used to strengthen the security of systems. In future this system can be extended to study CSPR from both adverseries and defenders’ point of view, leveraging the logs or activities that are available in the public domain.

**APPENDIX 1**

**SAMPLE CODE**

**Login**

import java.io.IOException;

import java.io.PrintWriter;

import java.sql.\*;

import java.sql.DriverManager;

import java.sql.ResultSet;

import java.sql.SQLException;

import java.util.logging.Level;

import java.util.logging.Logger;

import javax.servlet.RequestDispatcher;

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 login extends HttpServlet {

\* @param request servlet request

\* @param response servlet response

\* @throws ServletException if a servlet-specific error occurs

\* @throws IOException if an I/O error occurs

\*/

protected void processRequest(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {

response.setContentType("text/html;charset=UTF-8");

try (PrintWriter out = response.getWriter()) {

/\* TODO output your page here. You may use following sample code. \*/

out.println("<!DOCTYPE html>");

out.println("<html>");

out.println("<head>");

out.println("<title>Servlet login</title>");

out.println("</head>");

out.println("<body>");

out.println("<h1>Servlet login at " + request.getContextPath() + "</h1>");

out.println("</body>");

out.println("</html>");

}

// <editor-fold defaultstate="collapsed" desc="HttpServlet methods. Click on the + sign on the left to edit the code.">

/\*\*

\* Handles the HTTP <code>GET</code> method.

\*

\* @param request servlet request

\* @param response servlet response

\* @throws ServletException if a servlet-specific error occurs

\* @throws IOException if an I/O error occurs

\*/

@Override

protected void doGet(HttpServletRequest request, HttpServletResponse response)

throws ServletException, IOException {

processRequest(request, response);

}

@Override

protected void doPost(HttpServletRequest request, HttpServletResponse response)

throws ServletException, IOException {

String accountno=request.getParameter("Customer Id");

String pass=request.getParameter("pass");

String user=request.getParameter("user");

String pass1=request.getParameter("pass");

PrintWriter out = response.getWriter();

boolean f = false;

//String get=request.getParameter("commit");

try {

Class.forName("com.mysql.jdbc.Driver");

Connection con=DriverManager.getConnection("jdbc:mysql://localhost/bank","root","admin");

Statement st=con.createStatement();

ResultSet rs1=st.executeQuery("select \* from registration where accountno='"+accountno+"' and password='"+pass+"'");

if(rs1.next())

{

HttpSession hs=request.getSession(true);

hs.setAttribute("accountno", accountno);

// RequestDispatcher rd=request.getRequestDispatcher("loginwait.jsp");

RequestDispatcher rd=request.getRequestDispatcher("login\_choosepoint.jsp");

rd.forward(request, response);

}else{

//

// else{

// ResultSet rs=st.executeQuery("select \* from user where accountno='"+accountno+"' and password='"+pass+"'");

// if(accountno.equalsIgnoreCase("1234561111")&& pass.equals("admin"))

// {

// RequestDispatcher rd=request.getRequestDispatcher("a\_home.jsp");

// rd.forward(request, response);

// }

// if(rs.next())

// {

//// String accountno=rs.getString(10);

// String balance=rs.getString("balance");

// HttpSession hs=request.getSession();

// hs.setAttribute("accountno", accountno);

// hs.setAttribute("balance", balance);

// RequestDispatcher rd=request.getRequestDispatcher("home.jsp");

// rd.forward(request, response);

// }

// else

// {

// RequestDispatcher rd=request.getRequestDispatcher("login.jsp");

// rd.include(request, response);

// }

//

//// }String account=rs.getString("accountno");

//// HttpSession hs=request.getSession();

//// hs.setAttribute("account", account);

// }

// }

String aname=request.getParameter("Customer Id");

String apass=request.getParameter("pass");

if(aname.equals("admin") && apass.equals("admin")){

RequestDispatcher rd=request.getRequestDispatcher("managerhome.jsp");

rd.forward(request, response);

}else{

f = true;

}

}

if(f){

RequestDispatcher rd=request.getRequestDispatcher("/login.jsp?err=fail");

rd.forward(request, response);

}

catch (SQLException | ClassNotFoundException ex) {

Logger.getLogger(login.class.getName()).log(Level.SEVERE, null, ex);

}

HttpSession hs=request.getSession();

// hs.setAttribute(user, "user");

hs.setAttribute(pass, "pass");

}

/\*\*

\* Returns a short description of the servlet.

\*

\* @return a String containing servlet description

\*/

@Override

public String getServletInfo() {

return "Short description";

}// </editor-fold>

}

**Choose point**

import java.io.IOException;

import java.io.OutputStream;

import java.io.PrintWriter;

import static java.lang.System.out;

import java.sql.Connection;

import java.sql.DriverManager;

import java.sql.ResultSet;

import java.sql.Statement;

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 login\_choosepoint extends HttpServlet {

@Override

protected void doGet(HttpServletRequest request, HttpServletResponse response)

throws ServletException, IOException

{

try{

Class.forName("com.mysql.jdbc.Driver");

String url="jdbc:mysql://localhost/bank";

String user="root";

String password="admin";

HttpSession hs=request.getSession();

String accountno=(String)hs.getAttribute("accountno");

hs.setAttribute("accountno",accountno);

System.out.println(accountno);

//String name=(String)request.getAttribute("Name");

// String employee\_id=(String)request.getAttribute("employee\_id");

String sql="select \* from registration where accountno='"+accountno+"'";

// String sql="select \* from user where accountno='"+accountno+"'";

Connection conn=DriverManager.getConnection(url, user, password);

Statement st=conn.createStatement();

ResultSet rs=st.executeQuery(sql);

int i=1;

String cnt=(String)hs.getAttribute("cnt");

if(cnt!=null){

i=Integer.parseInt(cnt);

}

OutputStream img;

while(rs.next())

{

// String accountno=rs.getString("accountno");

out.println("<h1>"+accountno+"</h1>");

System.out.println(accountno);

out.println("<h1>");

byte barray[]=rs.getBytes("image1");

response.setContentType("image/png");

img=response.getOutputStream();

img.write(barray);

byte barray1[]=rs.getBytes("image1");

response.setContentType("image/png");

img=response.getOutputStream();

img.write(barray);

out.println("</h1>");

}

rs.close();

st.close();

conn.close();

//employee\_details.invalidate();

}catch(Exception ex){

ex.printStackTrace();

}

}

/\*\*

\* Handles the HTTP <code>POST</code> method.

\*

\* @param request servlet request

\* @param response servlet response

\* @throws ServletException if a servlet-specific error occurs

\* @throws IOException if an I/O error occurs

\*/

/\*\*

\* Returns a short description of the servlet.

\*

\* @return a String containing servlet description

\*/

@Override

public String getServletInfo() {

return "Short description";

}// </editor-fold>

}

**Alert message**

package newpackage;

import java.util.\*;

import javax.mail.\*;

import javax.mail.internet.\*;

import javax.activation.\*;

import java.util.Properties;

import javax.mail.Message;

import javax.mail.MessagingException;

import javax.mail.PasswordAuthentication;

import javax.mail.Session;

import javax.mail.Transport;

import javax.mail.internet.InternetAddress;

import javax.mail.internet.MimeMessage;

import java.util.Properties;

import javax.mail.Message;

import javax.mail.MessagingException;

import javax.mail.PasswordAuthentication;

import javax.mail.Session;

import javax.mail.Transport;

import javax.mail.internet.InternetAddress;

import javax.mail.internet.MimeMessage;

public class Sendmail {

public static void mailsend(String to) {

Properties props = new Properties();

props.put("mail.smtp.host", "smtp.gmail.com");

props.put("mail.smtp.socketFactory.port", "465");

props.put("mail.smtp.socketFactory.class",

"javax.net.ssl.SSLSocketFactory");

props.put("mail.smtp.auth", "true");

props.put("mail.smtp.port", "465");

Session session = Session.getDefaultInstance(props,

new javax.mail.Authenticator() {

protected PasswordAuthentication getPasswordAuthentication() {

return new PasswordAuthentication("vishaaleeo197@gmail.com","buijuvok");

}

});

try {

Message message = new MimeMessage(session);

message.setFrom(new InternetAddress("vishaaleeo197@gmail.com"));

message.setRecipients(Message.RecipientType.TO,

InternetAddress.parse(to));

message.setSubject("Alert");

message.setText("Someone tried to login your account" );

Transport.send(message);

System.out.println("Done");

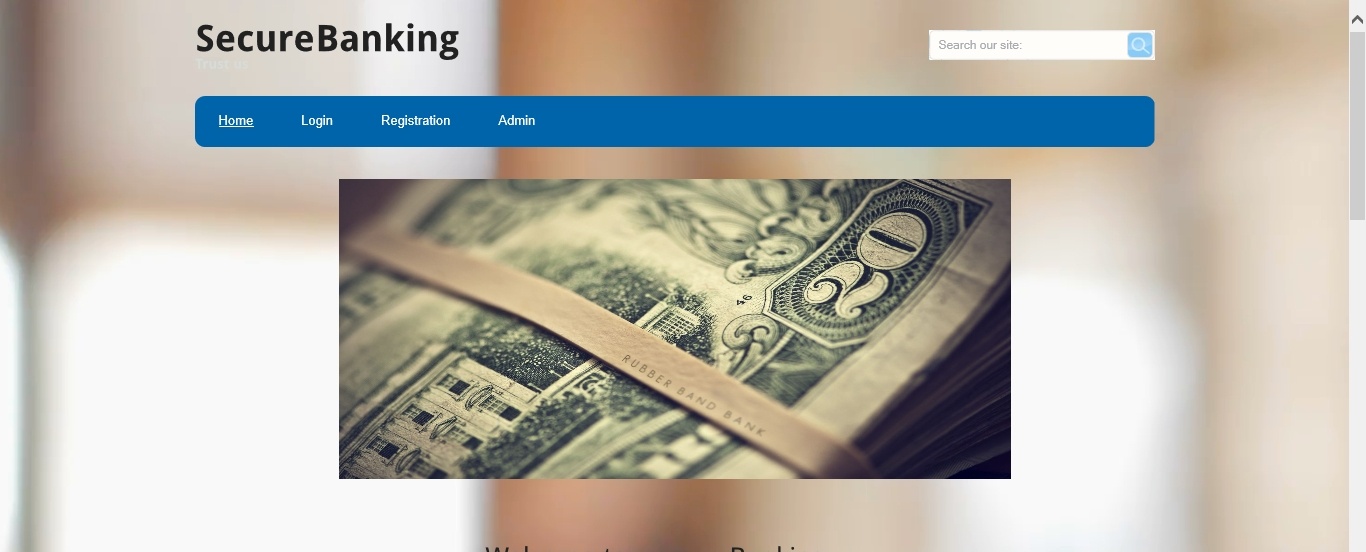
} catch (MessagingException e) {

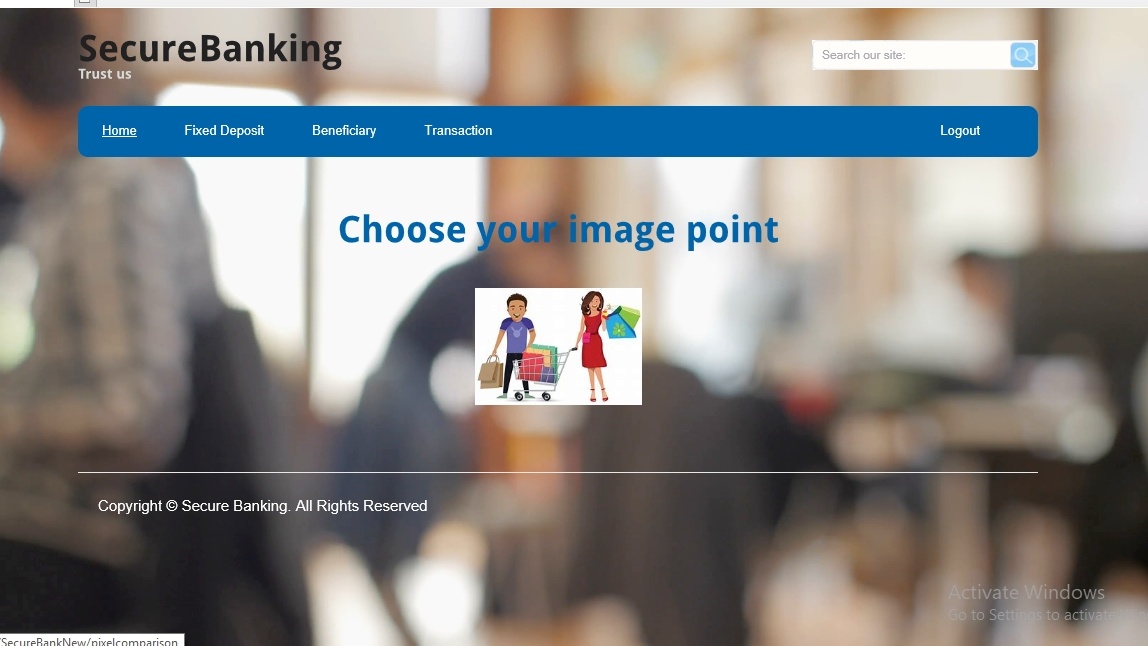
throw new RuntimeException(e);

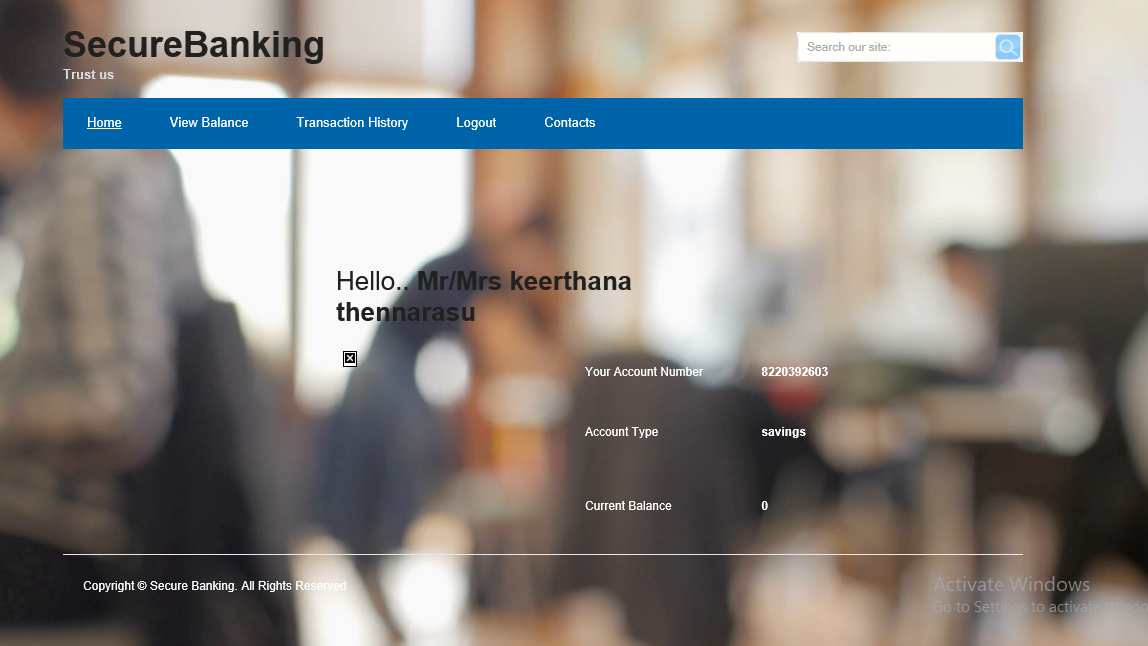
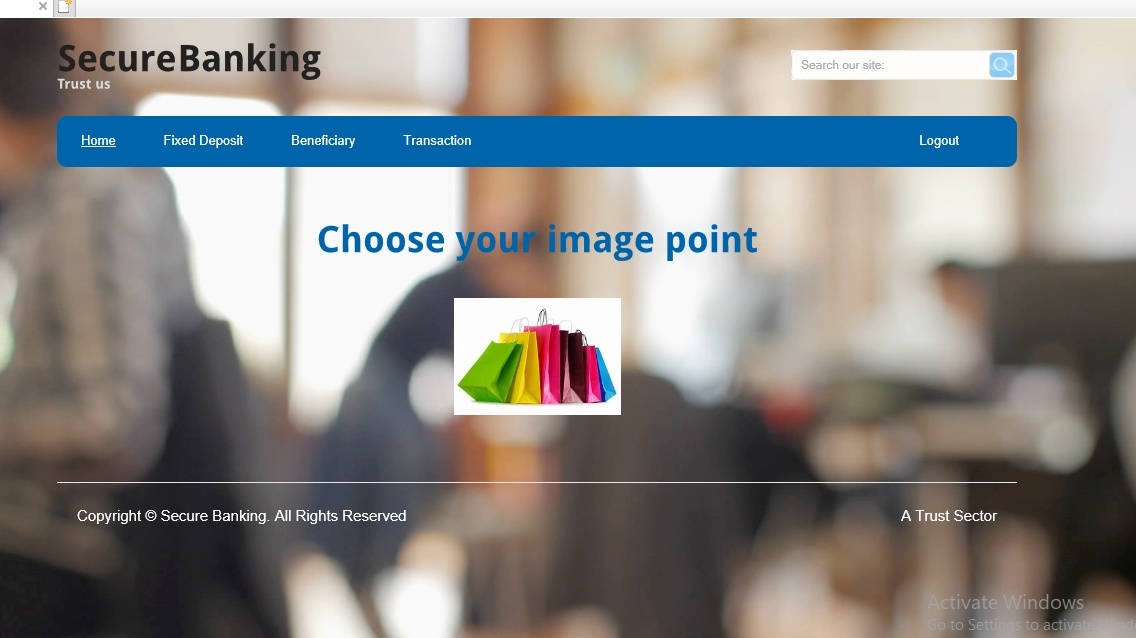
}

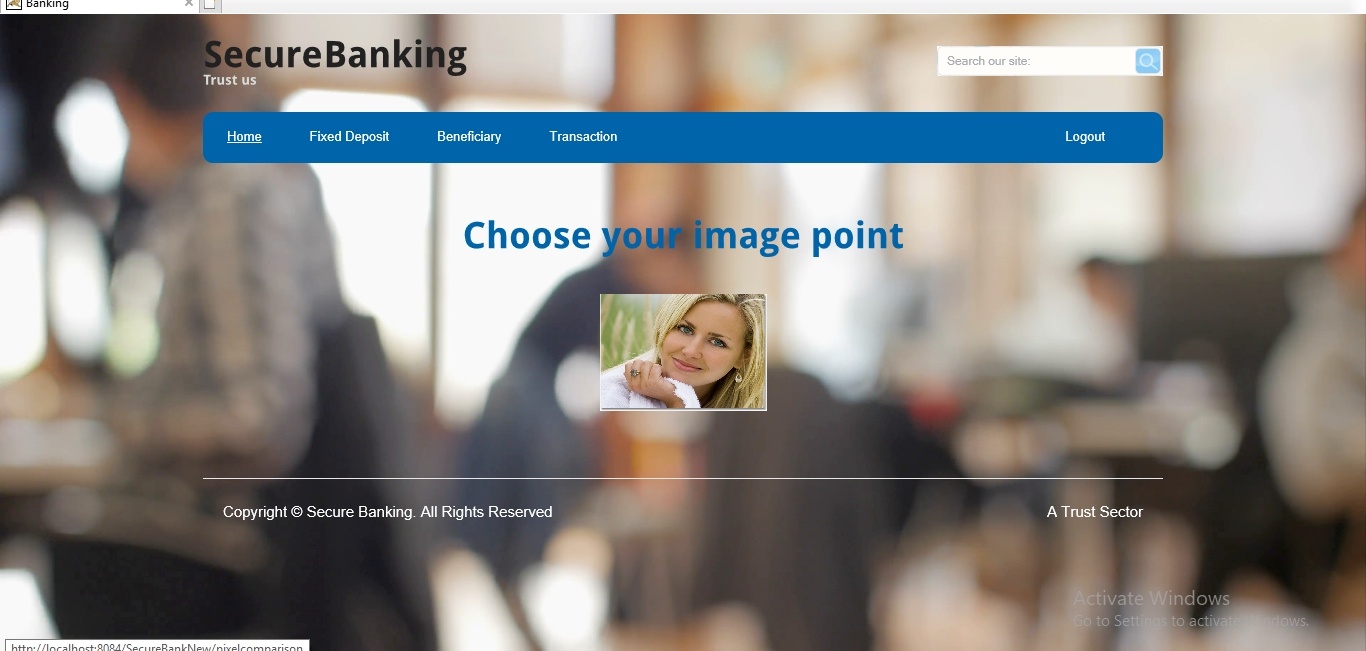
**APPENDIX 2**

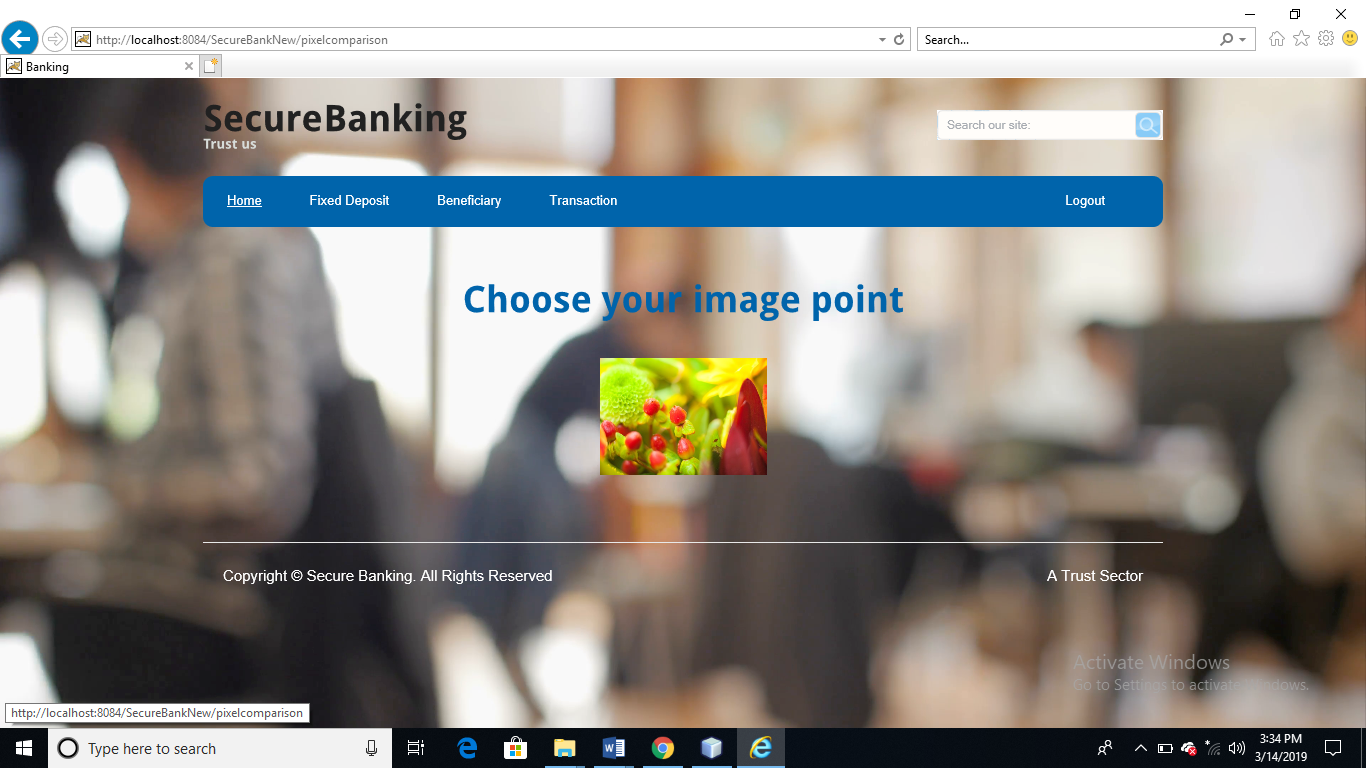
**SCREENSHOTS**

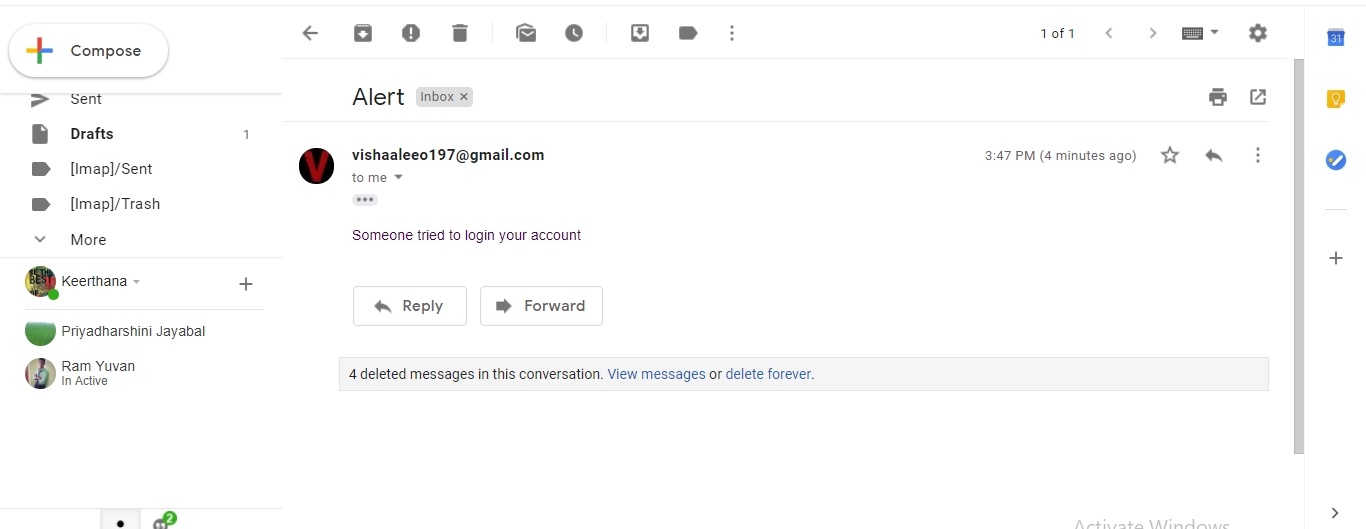
****

****

****

****

****

****

**REFERENCES**

[1] Weili Han, zhigong Li, Guofei Gu, Wenyuan Xu “shadow attacks based on password reuses: A quantitative empirical analysis”IEEE Transactions on dependable and secure computing, 2018.

[2] Dheepanshu and mayank sharma “Enhancing password security using cyclic groupmatrix”International conference on telecommunication and Networks(TEL-NET),2018.

[3] [Zubayr Khalid,](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Zubayr%22&searchWithin=%22Last%20Name%22:%22Khalid%22&newsearch=true)[Pritam Paul,](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Pritam%22&searchWithin=%22Last%20Name%22:%22Paul%22&newsearch=true)[Soummyo Priyo Chattopadhyay](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Soummyo%20Priyo%22&searchWithin=%22Last%20Name%22:%22Chattopadhyay%22&newsearch=true)“Secure authentication with dynamic password” [IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7740393),2016.

[4] Lin zhang and zhenfeng zhang“Security analysis of an ID based two server password authenticated key exchange”IEEE Communication letters,2016.

[5] Ashutosh Gupta and Yogesh Kumar“Banking security system using hand gesture recognition”International conference on recent developments in control, automation and power engineering,2015.

[6] Zhigong Li and Weili Han“A Large-Scale Empirical Analysis of Chinese Web passwords”Usenix security symposium,2014.

[7] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska“The Psychology of Security for the Home Computer User”IEEE Symposium on security and privacy,2012.

[8] Anupam Das, Joseph Bonneauy, Matthew Caesar, Nikita Borisov and XiaoFeng Wangz “The Tangled Web of Password Reuse”NDSS,2009.

[9] Dino Schweitzer, Jeff Boleng, Colin Hughes, Louis Murphy“Visualizing Keyboard Pattern Passwords”International workshop on visualization for cyber security,2009.

[10] [Fawaz A. Alsulaiman](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Fawaz%20A.%22&searchWithin=%22Last%20Name%22:%22Alsulaiman%22&newsearch=true), [Abdulmotaleb El Saddik](https://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22First%20Name%22:%22Abdulmotaleb%22&searchWithin=%22Last%20Name%22:%22El%20Saddik%22&newsearch=true)“Three-Dimensional Password for More Secure Authentication”[IEEE Transactions on Instrumentation and Measurement](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=19) ,2008.