**CHAPTER 1**

**INTRODUCTION**

* 1. **About**

Stock Market is the aggregation of buyers and sellers who buys and sell stock. A stock represent share in a company but that does not mean that you own the power to influence decision of the top management and leaders in a company. A Stock Exchange is a place where trading of stocks take place. Investors buy stocks for making profits and companies sell stocks to raise funds for finance of the company. Investors buy stock at a price and then sell it for a higher price and make profit.

Smart Investors look for trends, fundamental data, finance of company, history of the company, technical charts etc. and then decide whether to invest or not. Trading strategies are divided into two categories (i) fundamental analysis (ii) technical analysis.

Fundamental analysis is the study of financial statements and determining the true value of the stock and then taking decision.

Technical analysis is the study of charts and then determining the trend based on past stock data and then making a decision. It deals with looking for patterns. There are 3 principles in technical analysis:

* Technical analysis believes that it is important to understand what investors think of stock and what they know and what they perceive.
* Stock Prices follow trends.
* History repeats itself.

Various technical tools like SMA, EMA, RSI, MACD, Bollinger Bands etc. have been in use for a long time. They are used by technical analysts. This project has also made an attempt of making a smart decision based on indicators, oscillators. An attempt to predict stock price has also made. Statistical Regression is used for determining relationship between index and stock price.

**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**

The fundamental analysis involves the in-depth analysis of a company’s performance and the profitability to measures it’s intrinsic value by studying the company physically in terms of its product sales, man power quality, infrastructure, profitability on investment. It uses revenues, earnings, future growth, return on equity, profit margins, and other data to determine a company's underlying value and potential for future growth. To a fundamentalist, the market price of a stock tends to move towards its “real value” or “intrinsic value”. If this value of a stock is above the current market price, the investor can decide to purchase the stock because the stock price

will bound to rise and move towards its “intrinsic or real value”. If this value of a stock is below the market price, the investor may decide to sell the stock because the stock price is bound to fall and come closer to its intrinsic value. To start finding out the intrinsic value, the fundamentalist analyzer makes an examination of the current and future overall health of the economy as a whole.

Technical analysis is a method of evaluating stocks by analyzing statistics generated by market activity, past prices, and volume. It looks for peaks, bottoms, trends, patterns, and other factors affecting a stock's price movement.Future values of stock prices often depend on their past values and the past values of other correlated variables. Technical analysis looks for patterns and indicators on stock charts that will determine a stocks future performance .However, it is used by approximately 90% of the major stock traders. Despite its widespread use, technical analysis is

criticized because it is highly subjective. Different individuals can interpret charts in different manners.Recently, neural networks have been successfully applied in time-series problems to improve multivariate prediction ability. Neural networks have good generalization capabilities by mapping input values and output values of given patterns. Neural networks are usually robust against noisy or missing data, all of which are highly desirable properties in time series prediction problems. Various neural network models have already been developed for the stock marketanalysis.

**3.1.1 DISADVANTAGES OF THE EXISTING SYSTEM**

* It becomes harder to formalize all this knowledge for purposes of automation (with a neural network for example), and interpretation of this knowledge may be subjective.
* It is hard to time the market using fundamental analysis.
* Despite its widespread use, technical analysis is criticized because it is highly subjective.
* Different individuals can interpret charts in different manners.
  1. **PROPOSED SYSTEM**

**4.1 Data Collection:**

Quandl API is used to fetch the stock quote of any company under NSE. Stock Quote consist of Close Price, High, Low, Volume, Open etc. as a data-frame. A data-frame is a labelled two dimensionnal data structure that stores data of different types in different columns. A data-frame consists of columns and a single column represent a series.

Series of Close price is extracted and is used as data source for every indicator, oscillator and neural network. Date is the index of the series and is also used as data for indicators and oscillators. This series represents the past closing prices of a company under NSE.

**4.2 Implementation of Indicators and Oscillators:**

The following are implemented:

* SMA
* EMA
* MACD
* RSI
* Bollinger Band
* Statistical Regression(Not an indicator/Oscillator)

**4.2.1 SMA (Simple Moving Average):**

It is a type of moving average in which mean is calculated over the price of n-periods. Using it, we get a series of averages of different subsets of full dataset.

SMA = ( pm + pm-1 + pm-2 + ………….. + pm-(n-1) )/n 1.1

n = 20 but it can have any value.

Where numerator is the summation of previous n-periods prices and n is the length of period.

If the data used are not centered around the mean, a simple moving average lags behind the latest datum point by half the sample width. An SMA can also be disproportionately influenced by old datum points dropping out or new data coming in. One characteristic of the SMA is that if the data have a periodic fluctuation, then applying an SMA of that period will eliminate that variation. But a perfectly regular cycle is rarely encountered.

**4.2.2 EMA (Exponential Moving Average):**

EMA or EWMA is a type of moving averagethat is similar to a simple moving average, except that more weight is given to the latest data. It's also known as the exponentially weightedmoving average. This type of moving average reacts faster to recent price changesthan a simple moving average[.](http://www.investopedia.com/terms/s/sma.asp)

Calculating EMA is a 3 step process:

* Calculate the SMA
* Calculate the multiplier
* Calculate the current EMA

Multiplier = 2 / (n+1), 1.2

EMA = (Closing Price – EMA (previous day))\*multiplier + EMA (previous day)) 1.3

**4.2.3 MACD (Moving Average Convergence Divergence)**

Moving average convergence divergence (MACD) is a trend-following momentum indicator that shows the relationship between two moving averages of prices. The MACD is calculated by subtracting the 26-day EMA from the 12-day EMA. A nine-day EMA of the MACD, called the "signal line", is then plotted on top of the MACD, functioning as a trigger for buy and sell signals.

MACD = ((12-day EMA) – (26-day EMA)) 1.4

**4.2.4 RSI (Relative Strength Index)**

The relative strength index (RSI) is a momentum indicator developed by noted technical analyst Welles Wilder , that compares the magnitude of recent gains and losses over a specified time period to measure speed and change of price movements of a security. It is primarily used to attempt to identify overboughtor oversoldconditions in the trading of an asset.

RSI = 100 - 100 / (1 + RS) 1.5

Where RS = Average gain of up periods during the specified time frame / Average loss of down periods during the specified time frame

RSI values range from 0 to 100. The default time frame for comparing up periods to down periods is 14, as in 14 trading days. Traditional interpretation and usage of the RSI is that RSI values of 70 or above indicate that a security is becoming overbought or overvalued, and therefore may be primed for a trend reversal or corrective pullbackin price.

On the other side of RSI values, an RSI reading of 30 or below is commonly interpreted as indicating an oversold or undervalued condition that may signal a trend change or corrective price reversal to the upside.

**4.2.5 Bollinger Band**

A Bollinger Band, developed by famous technical trader John Bollinger[, is plotted two standard deviations away from a simple moving average.](http://www.investopedia.com/video/play/understanding-bollinger-bands/) Many traders believe the closer the prices move to the upper band, the more overboughtthe market, and the closer the prices move to the lower band, the more oversoldthe market. John Bollinger has a set of 22 rules to follow when using the bands as a trading system.

Upper-Band= SMA-20 + 2 \* standard deviation of 20 day closing 1.6

Lower-Band= SMA-20 + 2 \* standard deviation of 20 day closing 1.7

%B =((price – lower band) / (upper band – lower band))\*100 1.8

%B quantifies a security's price relative to the upper and lower Bollinger Band. There are six basic relationship levels:

* %B equals 1 when price is at the upper band
* %B equals 0 when price is at the lower band
* %B is above 1 when price is above the upper band
* %B is below 0 when price is below the lower band

**4.2.6 Statistical Regression**

It is a way of determining a relation between variables. There are 2 independent variables here.

1. Index
2. Stock Price

y = mx +c → trend line equation 1.9

where y = closing price , x = nth number, m =slope

m = (sum(x\*y)-sum(y)\*sum(x))/sum((x-mean(x))^2) 2.0

c = y – mx 2.1

**4.3 Determining Buy/Sell Signals:**

* If previous SMA is lower than the previous Close Price and current SMA is greater than current Close Price then Buy Signal is generated.
* If previous SMA is greater than the previous Close Price and current SMA is lower than current Close Price then Sell Signal is generated.
* If previous EMA-20 is lower than the previous EMA-50 and current EMA-20 is greater than current EMA-50 then Buy Signal is generated.
* If previous EMA-20 is greater than the previous EMA-50 and current EMA-20 is lower than current EMA-50 then Sell Signal is generated.
* If previous MACD value is less than previous EMA-9 and current MACD value is greater than current EMA9 then Buy Signal is generated.
* If previous MACD value is greater than previous EMA-9 and current MACD value is lower than current EMA-9 then Sell Signal is generated.
* If [Close Price - lower band]<[Upper Band - Close Price] and both the differences are greater than 0 then buy Signal is generated
* If [Upper band – Close Price]<[Close Price – Lower Band] and both the differences are greater than 0 then Sell signal is generated

**4.4 Predicting Stock Price:**

* RBF Neural Network is used for predicting stock price for the next day.
* Previous 30 day stock price is used as training data.
* For ex., for index n, output is X. where n can be anything between 1 – 30
* For index 31st , stock price is predicted which is the next day stock price
* Sklearn Library is used for implementing RBFNN

**3.2.1 ADVANTAGES OF PROPOSED SYSTEM**

* .

**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 : Linux

Languages used : Python

Tools : Eclipse

Backend : Terminal

* 1. **LANGUAGE SPECIFICATION**

**3.4.1.PYTHON**

**Overview**

Python pathi eluthanum\*\*\*\*\*\*

**Working of Java**

**\*\*\*\***

**3.4.2 TERMINAL**

Write something

**3.4.3 Eclipse**

**Write something about eclipse**

**CHAPTER 4**

**4.1 Flow Chart:**

Username and password verification

START

INPUT TICKER NAME

FETCH STOCK DATA using Quandl API

Calculate ‘SMA’ and Determine Buy/Sell Signals

Calculate ‘EMA’ and Determine Buy/Sell Signals

Calculate ‘MACD’ and Determine Buy/Sell Signals

STOP

Calculate ‘RSI’ and Determine oversold/overboughtSignals

Display the report

Calculate ‘Bollinger Bands’ and Determine Buy/Sell Signals

Predict Stock Price for next day

Plot the data

Determine trendline equation

**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**

* Technical Analysis of stock market is a method of evaluating securities by analyzing statistics generated by market activity. Chartist uses these data to determine whether they are going to invest in that stock. They look for the buy and sell signals. This project has also performed technical analysis over stock prices by using some of the mostly used indicators and oscillators. We have also tried to predict stock price for the next day.
* Stock price is influenced by many factors including –internal information, news, speeches of ministers etc. So this does not give accurate results all the time. But it is better than blindly investing
* Hence, it can be concluded that a smart investing decision can be made if one uses technical indicators and oscillators and other sorts of information like news etc. before making an investment

**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");

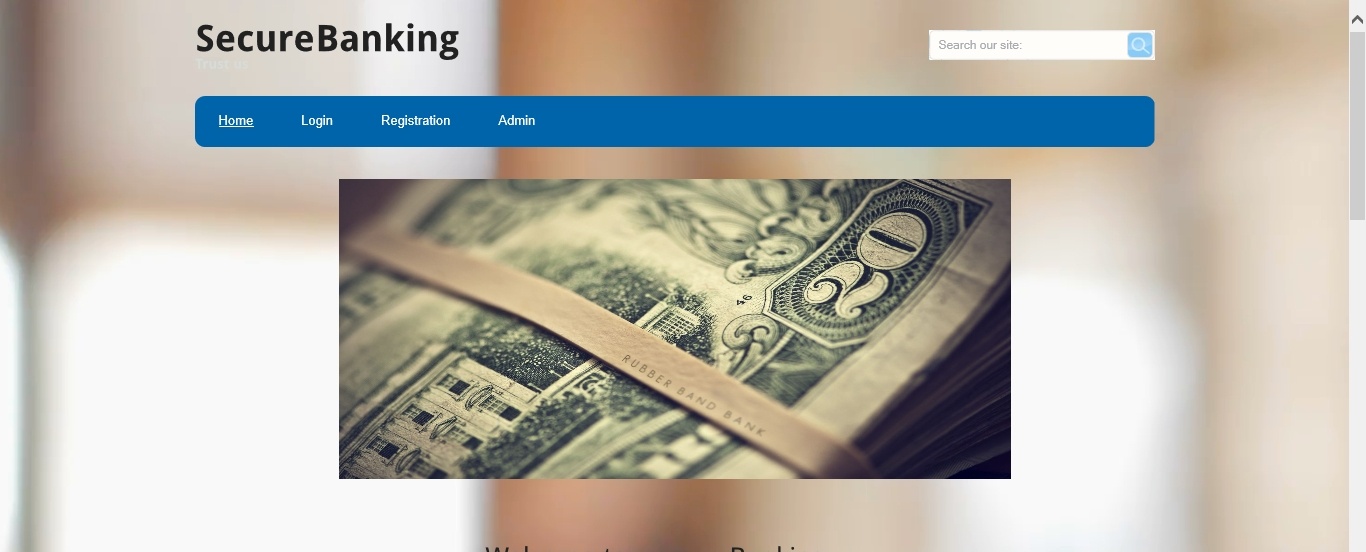
} catch (MessagingException e) {

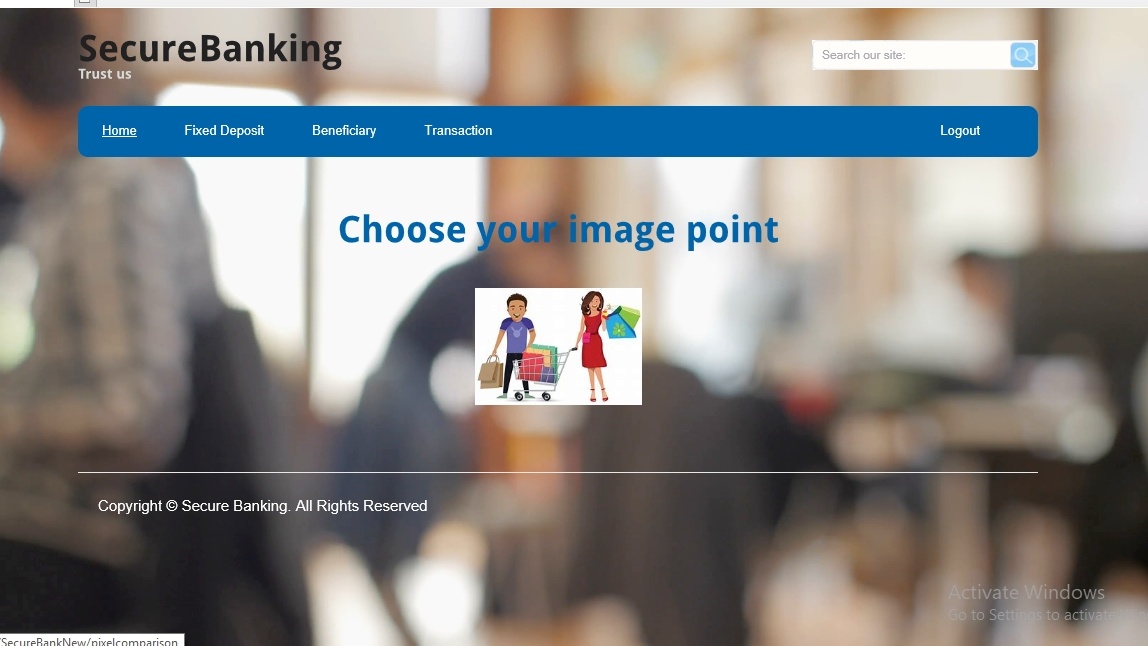
throw new RuntimeException(e);

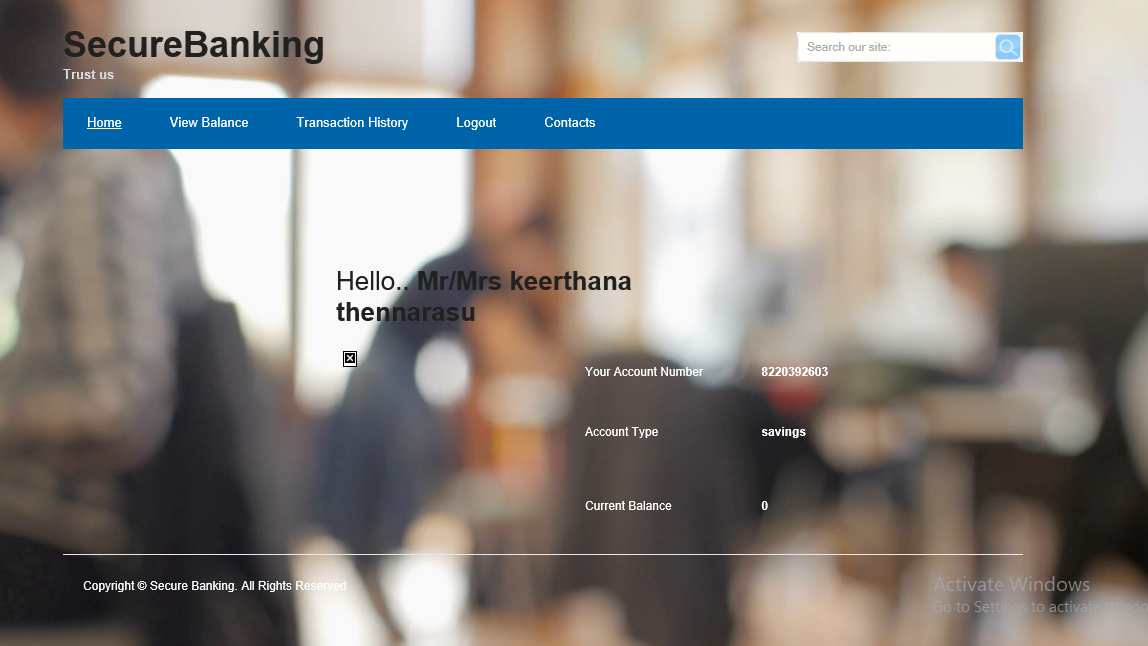
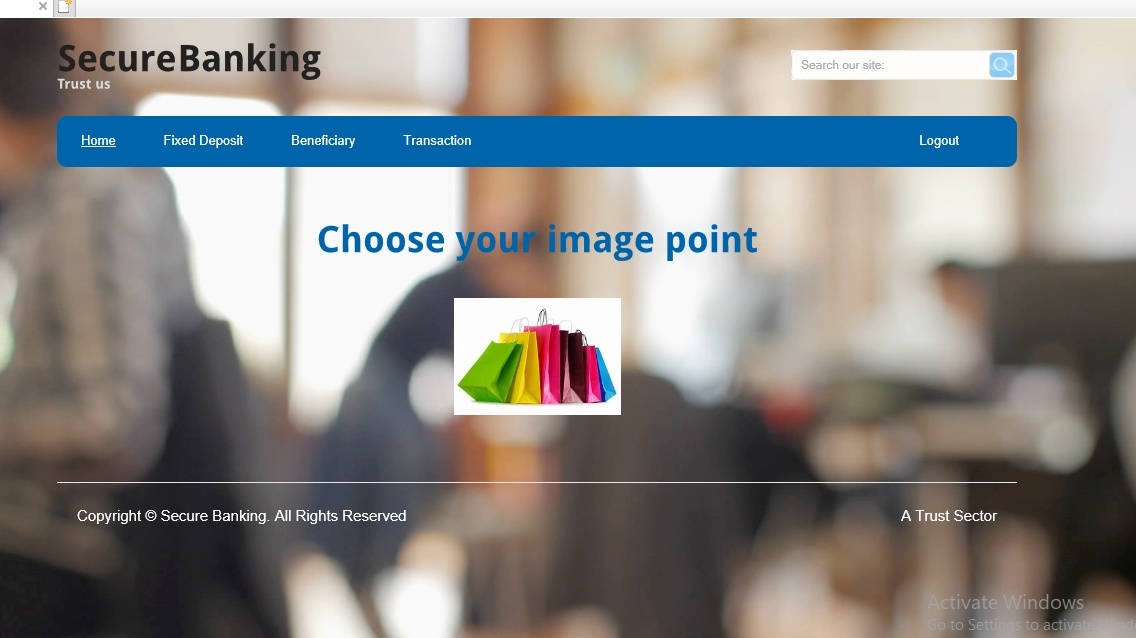
}

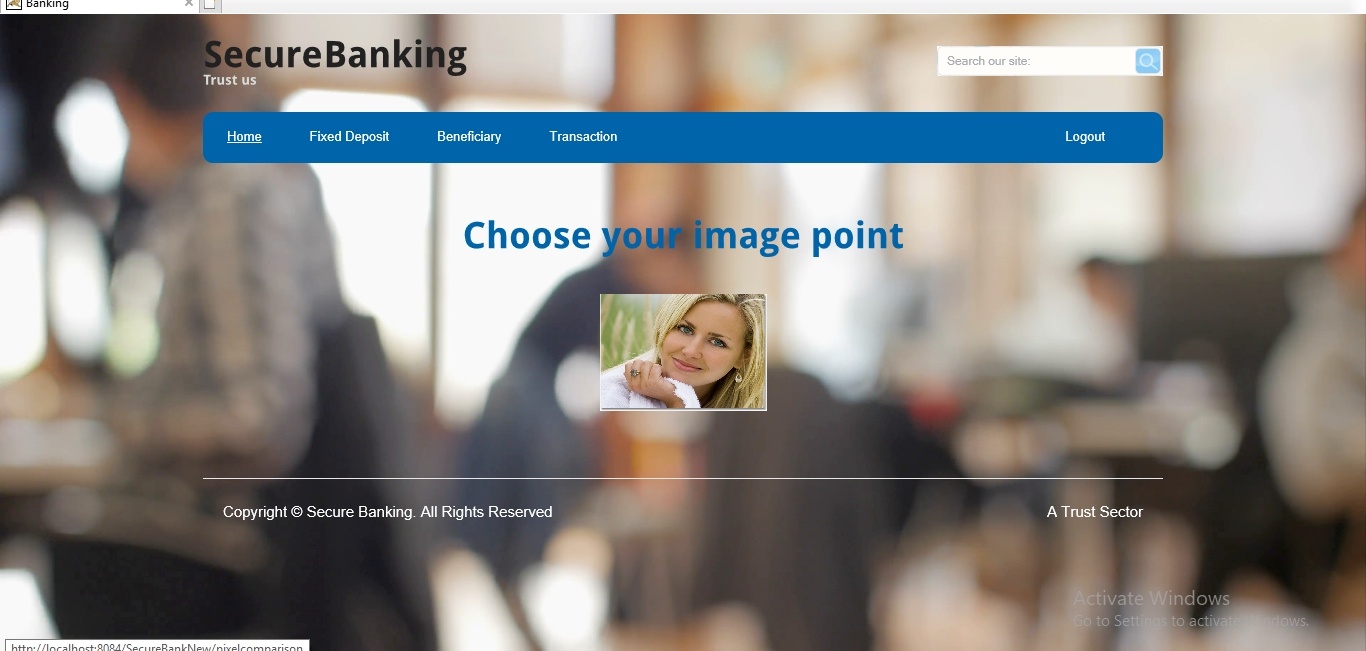
**APPENDIX 2**

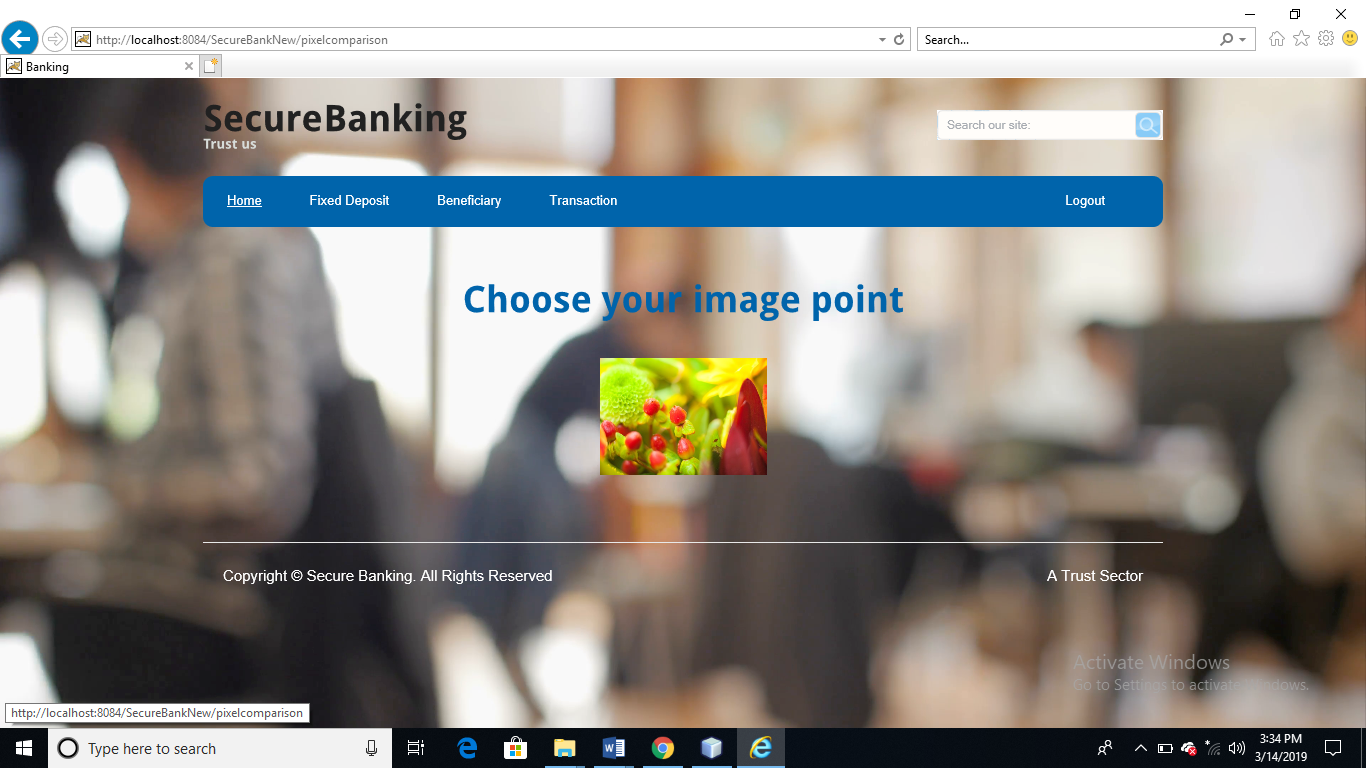
**SCREENSHOTS**

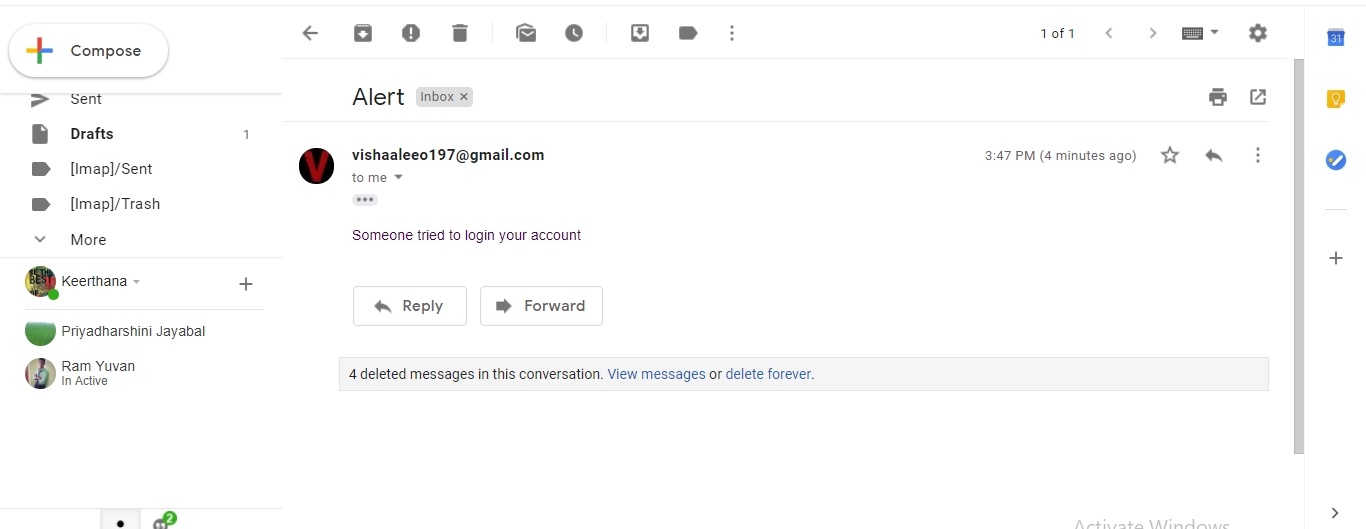
****

****

****

****

****

****

**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.