ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Implementation of Passmatrix Based Shoulder Surfing Resistant Graphical Authentication System

A. A. Ghasad[1], A. B. Deshmukh[2], A. A. Bardekar[3]

PG Scholar, Department of Information Technology, Sipna COET, Amravati, Maharashtra, India[1]

Assistant Professor, Department of Information Technology, Sipna COET, Amravati, Maharashtra, India[2]

Assistant Professor, Department of Information Technology, Sipna COET, Amravati, Maharashtra, India[3]

ABSTRACT: Day by day password security and protection are assumed fundamental part in PC application with increasing in PC innovation, for the diverse sorts of PC wrongdoing, misrepresentation and attacks. So, in this aspect we are proposing a novel confirmation framework which is opposed the different types of attack which happens in client account. With a one-time substantial sign up indicator for an image, the user has selected pass-images of the PassMatrix which is a graphical password of a user and register in the system. After registering successfully user login into system with two factor verification. In this two factor verification, we use an Android application. It offers no insight for attackers to make sense of or restricted down the secret word even they direct various cameras-based assaults. It maintained privacy and authority. The proposed framework will accomplish better imperviousness to attacks while looking after ease of use.

KEYWORDS: PassMatrix, Graphical Password, QR code scan, Two factor Authentication, Android application.

I. INTRODUCTION

Today, technology increased very fast and with newly developed innovation, competition, performances, maintains, security, privacy also increased. Security and privacy are playing vital role in any online application. To access or share any Information other user required password. So to maintained password security and privacy, user used different types of authentication technique one of them is textual password.

Textual password has been the most generally utilized confirmation technique for a considerable length of time comprised of numbers and upper and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. Be that as it may, a strong textual password is difficult to retain and remember. Subsequently, users have a tendency to pick passwords that are either short or from the dictionary, as opposed to arbitrary alphanumeric strings. Surprisingly, more dreadful, it is not an uncommon case that users may utilize just a single username and password for different records. As per an article in Computer world, a security group in a vast organization ran a system password cracker and shockingly split around 80% of the worker's passwords in 30 seconds. Printed passwords are regularly unreliable because of the trouble of keeping up strong ones. [1] [12]

To keep up password secure the other validation technique mostly used in the banking sector and also for online transaction two factor authentication using OTP and ATM pin/cards has been implemented. Two Factor Authentication, user provides dual means of Identifications username and security code as well as something that's exclusive, and just, that user has on them, i.e. a bit of data just they ought to know or have quickly to hand, for example, a physical token such as a card. Utilizing a username and security code, i.e. password together with a bit of data that exclude the user knows it makes harder for potential intruders to gain access and steal that individual's personal information or an identity.[2]

Utilizing a Two Factor Authentication process can bring down the quantity of instances of wholesale fraud on the Internet, and also phishing by means of email, on the grounds that the criminal would require more than simply the username and password subtle elements. The drawback to this security procedure is that the cost of purchasing, issuing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

and managing the tokens or cards, requesting new hardware tokens (as key dandies or card per users) should be requested, then issued and this can bring about log jams and issues in an organization's clients needing and holding up to access their own particular private information by means of this validation strategy. The tokens are likewise generally little and effectively lost so bringing about more issues for everybody when client bring in asking for new ones. [4]

Overcomes this problem we have utilized a safe graphical verification system named as PassMatrix Based Shoulder Surfing Resistant Graphical Authentication System that are protecting users from getting to be casualties of shoulder surfing attacks while contributing passwords in public through the use of one-time login pointers. In this user have set their graphical password at registration time and when a user login user must require two factor authentications. User can scan the QR code and download image in their mobile then user have selected the pass-image same as when selected at the time of registration.[9] If selected pass-image is correct then user login into the system. A login marker will randomly create for every passer-image and will be pointless after the session ends. The login marker will gives better security against shoulder surfing attacks, since users utilize a dynamic pointer to call attention to the position of their passwords instead of tapping on the password object directly. Due to this user access their data more secure. The main purposed of our system to maintain the privacy and authority of the user.

II. RELATED WORK

The Deja Vu system, proposed by Dhamija and Perrig in the year 2000, takes advantage of the human ability to remember images even if seen for a short duration of time. It uses random art images, which are hard to describe to reduce the likelihood of users writing down their password images or telling it to another person. Users are presented with a grid during the authentication session where they have to choose their password images among distracting images during individual login attempts. Similar to the Pass-faces system, the Deja Vu system is vulnerable to shoulder-surfing attack as the users select their password images for each of the authentication sessions. Guessing attack is also possible if the adversary knows the user well. [3] In 2005, Susan Wiedenbeck et al. Introduced a graphical authentication scheme Pass-points and at that time, handheld devices could already show high resolution colour pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo with a correct sequence and within their tolerant squares during the login stage. [8]

In the Minimizing Shoulder Surfing Attack Using Text and Colour Based Graphical Password Scheme proposed the graphical password which uses colour and is based on text and it provides resistance to Shoulder Surfing. The working of the proposed system is very simple and the proposed system is user friendly. The system is easy and simple for the users which are already familiar with the existing Textual password scheme. Using this system the system or any user can login the system easily and efficiently without using any physical keyboard or on-screen keyboard. But it is not more secure, it is a simple technique. [6]

In the Shoulder Surfing Resistance Using Graphical Password Authentication In ATM System, the focus is on a knowledge based approach using pictures as passwords. Graphical passwords have been proposed as a suitable alternative to text based schemes, as it is possible for humans to remember pictures better than text. The password space would be large compared to that of text based schemes which offers better resistance to attacks. Using graphical password user clicks on image to authenticate themselves rather than alphanumeric string. The graphical-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. The graphical password authentication method will briefly describes the difficulties users have with traditional passwords. [7]

In 2016, proposed A Secure Graphical Password Authentication System, S3APS. In S3PAS, the user has to mix his textual the login screen on password to get the session password. However, the login process of Zhao et al.'s plan is tedious and hard. And then, several secure graphical password authentication systems have been proposed, In this system, an improved secure graphical password authentication systems by using colours. The operation of the proposed scheme is easy and simple to learn for users familiar with textual passwords. The user can easily and efficiently login to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

the system without using any on-screen keyboard or physical keyboard. But this system is not against the shoulder surfing attack, key logging attack. [5]

Different graphical password authentication plan, were produced to address the issues and shortcomings connected with textual passwords. In light of a few reviews, for example, those in, people have a superior capacity to remember image with long term memory (LTM) than verbal representations. Image based passwords were turned out to be less demanding to recall in a few user considers. Subsequently, users can set up a complex authentication password and are capable for recalling it after quite a while regardless of the possibility that the memory is not actuated occasionally. In any case, the greater part of these image based passwords are powerless against shoulder surfing attacks (SSAs). This kind of attack either utilizes coordinate perception, for example, viewing behind someone or applies video catching procedures to get passwords, PINs, or other delicate individual information. [10]

Our inspiration comes from two representative graphical password schemes: DAS and Story. DAS allows users to draw a free-form picture on $N \times N$ grid to produce a password and Story requires users to select a sequence of images to make a story. Our new scheme Pass-Matrix grid (Come from DAS and Story) adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users select their password images (pass-images) orderly click directly on them.[11]

III. PROPOSED TECHNIQUE

PassMatrix

To maintain a strategic distance from the distinctive sorts of attacks which is happens in user account. To overcomes security weakness, the easiness of obtaining password by observers in public. We will utilize graphical validation system called PassMatrix. In PassMatrix, a password comprises of just selecting pass-squares per pass-image send for authentication form a sequence of n images. The image will be send by server. In the event that the If the user select incorrect pass-squares within the pass-image then user does not login into system. Be that as it may, primary motivation to oppose shoulder surfing attacks and maintain user privacy as well as authentication.

PassMatrix is made out of the accompanying parts

A) Login Indicator Generator Module

This module creates a login pointer comprising of a few recognizable characters, (for example, letters in order and numbers) or visual materials, (for example, hues and symbols) for users during the confirmation stage. In our implementation, we used characters A to D and 1 to 4 for a 4x4 grid. Both letters and the generated login indicator can be given to users visually to set password. For the former case, the indicator can shown on the display directly in notification on Android application when image download into application.

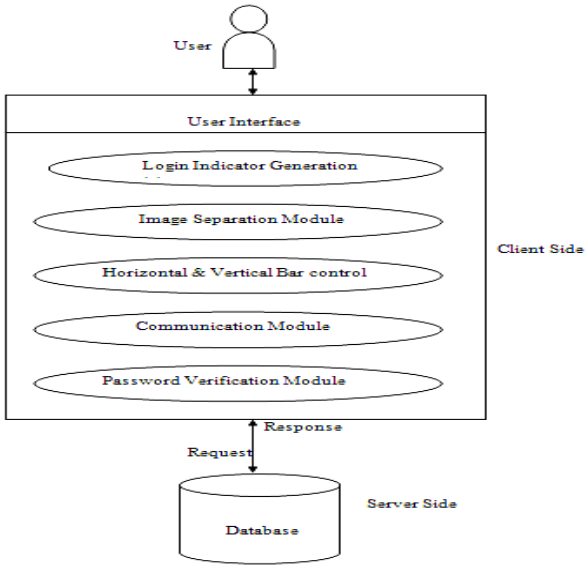


Fig. 1: Outline of the PassMatrix framework.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

B) Image Separation Module

This module divides each image into squares, from which users are choose the pass-square. An image is divided into a 4x4 grid. The smaller the image is separate to set the password. However, In our implementation, the existing width and height of random image is proportionally adjust into small images pixels width and height and save into temporary storage and display user into grid format.

C) Horizontal & Vertical Bar Control Module

There are two parchment bars: a level bar with a grouping of letters and a vertical bar with an arrangement of numbers. This control module gives drag and excursion capacities to users to control both bars. User can throw either bar utilizing their finger to move one alphanumeric at once. They can likewise move a few checks at once by dragging the bar for a separation. Both bars are user moves the horizontal bar in Figure 2(c) to left by three checkS, it will end up being the bar appeared in Figure 2(d). The bars are utilized to verifiably bring up (or at the end of the day, adjust the login indicator to) the area of the user's pass-square.

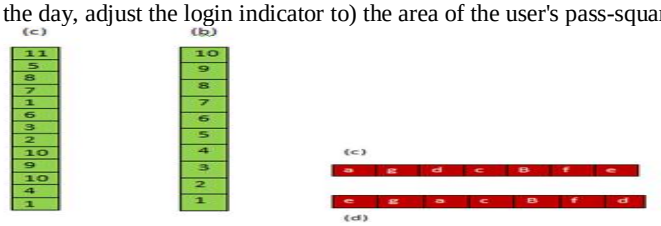


Fig.2: Horizontal bar (green) and Vertical bar (red)

D) Communication Module

This module is accountable for all the data transmitted between the customer gadgets and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

E) Password Verification Module

This module checks the user password during the validation stage. If the sequential selected pass-squares of pass-image are correct then user login into website.

F) Database

The database server contains a few tables cap store user accounts, passwords (ID number of pass-images and the places of pass-squares), and the time duration each user spent on both registration phase and login phase PassMatrix has all the required benefits toper form operations like insert, modify, delete and search.

IV. PROPOSED METHODOLOGY

The PassMatrix based shoulder surfing resistance graphical authentication system used two factor authentication processes to signup user and login user as follow-

A) Two Factor Signup Process

In Two Factor Signup process user fill the personal detail in normal the signup form and submit details. If details are valid then user is sign up into two factor form. In two factor signup form random pass-image which uploaded by admin save on server side local storage as shown in fig.5 or user select their own image and upload new image as shown in fig.3. Pass-image splits into the grid and display user. Users are select pass-squares sequential of pass-image and submit. In this way user register and user data send to the server and stored into a database for authentication.

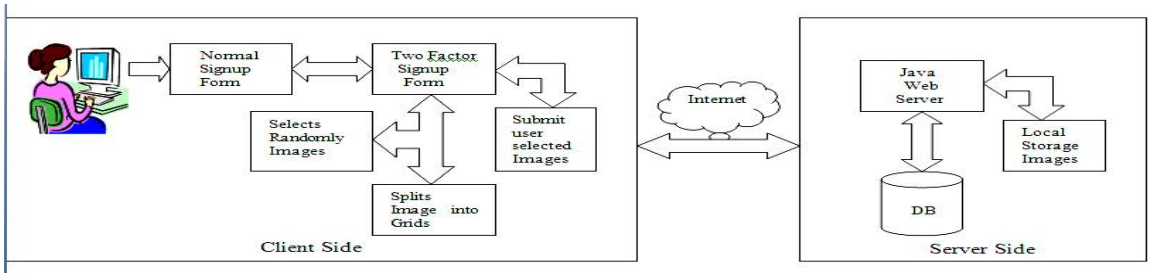


Fig.3: Block Diagram of two factor signup process

B) Two Factor Login Process

In two factor login process, the user fills normal detail such as username and password which is used as Signup process. If login is valid then for two factor authentication QR code display to the user as shown in fig.4. In QR code encoded image URL user scan the image from Android application and download image. The image split into the grid and user has select pass-image sequence

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

same as used in signup process. For remember we give short notify for a second display on user screen, the server verify authorized user or not as shown in fig.4. If selected pass-image is correct then user login into website and Android logout timer start after session end user logout and return into login page as shown in fig.6.

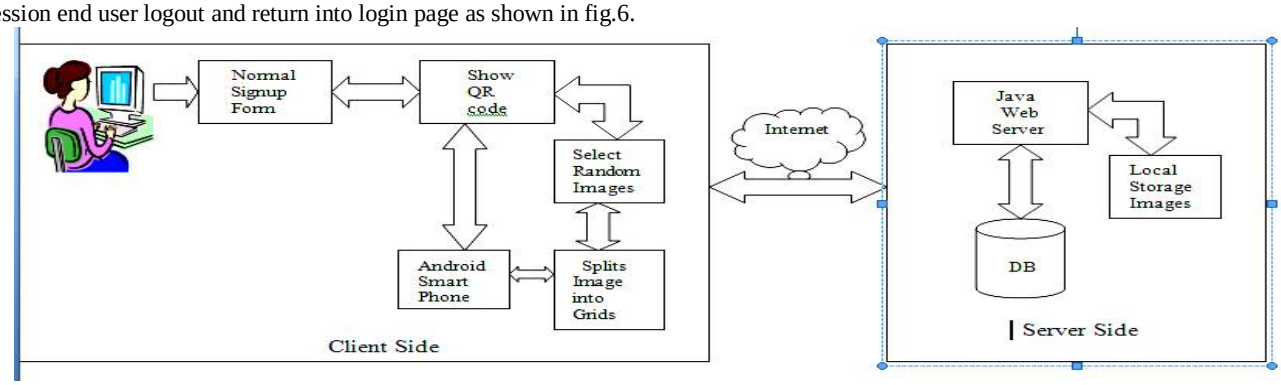


Fig. 4: Block Diagram of two factor login process

The following figure shows the data flow diagram of two factor signup process and login process.

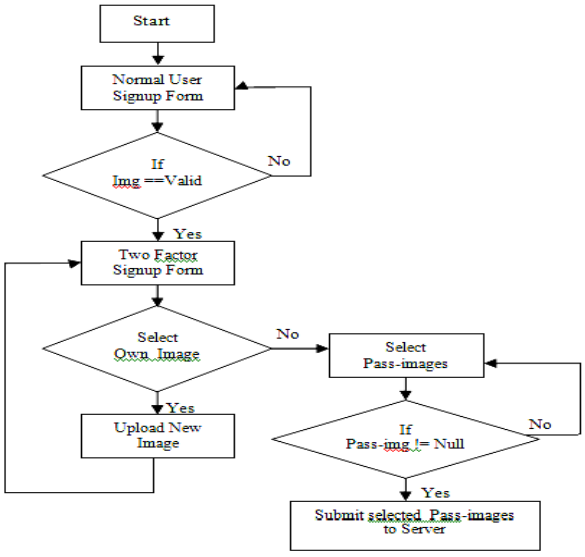


Fig. 5: The flowchart of Two Factor Signup process

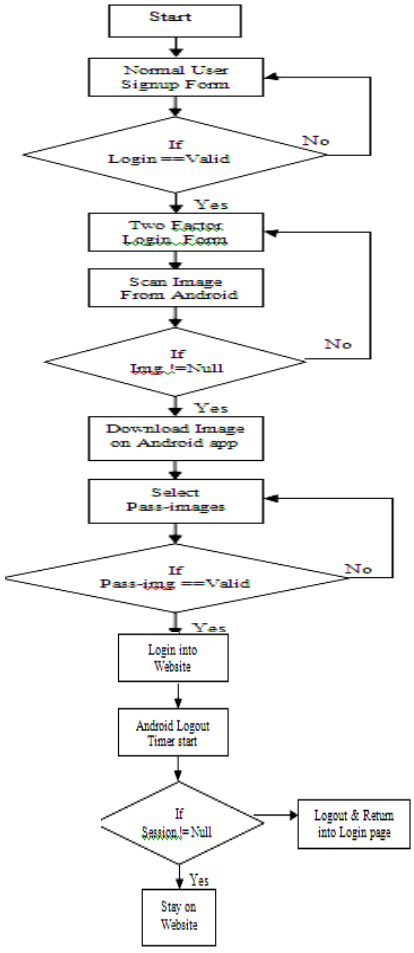


Fig. 6: The flowchart of Two Factor Login process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

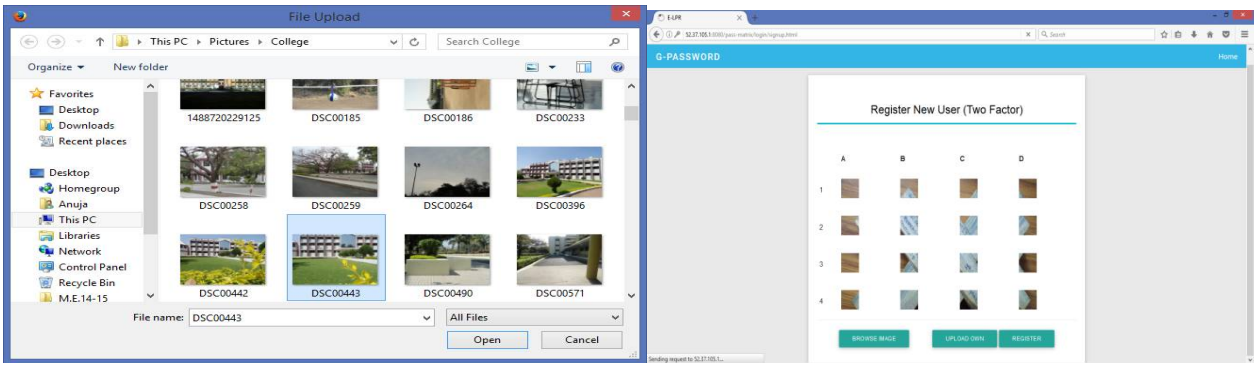
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

V. IMPLEMENTATION

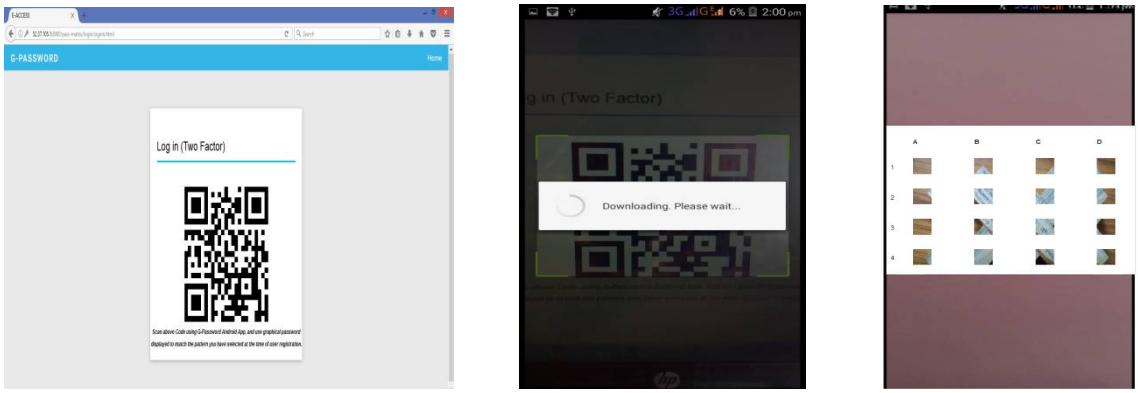
Although the PassMatrix prototype was implemented on an Android system it can be applied to a wide range of authentication scenarios. For instance user signup and login in Windows 8, email accounts login on web browser, and application login/ unlock on Android OS. It can also be applied to any client device such as personal computers, laptops, tablets, mobile phones, or bank ATM due to the fact that the method of authentication is simple and secure the entire authentication process can be completed by only touching or clicking on the screen. In our implementation, we assumed that users download an application from Google Play and register an account for later login to use the service. Since Android is an open source operating system based on Linux kernel and is widely used in mobile devices such as tablet PCs and smart phones, we implemented a PassMatrix prototype on Android and carried out user experiments to evaluate its usability.



(a) (b)

Fig.7: a) Upload own image at time of signup. b) Image display in 4x4 matrix format

The PassMatrix prototype is built with Android SDK 2.2.3 since it was the mainstream version of the distribution in 2012. After connecting to the Internet, users can Sign-Up an account, log in a few times in practice mode, and then log in for the experiment with a client's device in the client side of our prototype, we used XML to build the user interface and used JAVA and Android API to implement functions, including username checking, pass-images listing, image is in grid, pass-squares selection, login indicator delivery, and the horizontal and vertical bars circulation. In the server side of our implementation, we used JAVA web server and MySQL to store and fetch registered accounts to/from the database to handle the password verification. Although in our proposed system we mentioned that users can import their own images, or display image which stored in local storage of sever side. Each image size is not greater than 20 Mb and is grid into 4x4 matrix format. Thus, users have 4x4 squares of pass-image. After a user selects any number of pass-square of image sequence, the password will be stored as a list of coordinates in a database table (i.e., the locations of those selected pass-squares in the 4x4 grid as show in fig.7.



(a) (b) (c)

Fig.8: a) QR code display for authentication. b) User scan QR code in Android application. c) Image download and display in grid and user select pass-square of image and login.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

The password depends on the number of images selected by users. The first step in the login phase is fill the onetime valid login indicator same which is use in signup process and submit then if server check user id and password, image which is temporary stored. If valid then send URL of that image which is encoded into QR code and QR code display on user page as show in fig.8 below. [13] In our implementation, to provide more security and privacy we used two factor authentications that is android application. User can scan QR code on their Android application then Android smart phone download image and image divided into same matrix format 4x4 as show in fig.8.User select the pass-square of image same as used in signup process and selected pass-image send to list. If selected pass-square correct then sever set flag in javascript which is login user successfully into website and timer start. After session completed user logout.

VI. EXPERIMENTAL RESULT

A) Experimental Design

We conducted a user study for the proposed system to evaluate two performance metrics:

- Password recollection: How well do users remember their password and can they log into the system successfully after a period of time since registration?
- Usability: We measured the users' experience on PassMatrix, which includes the total time consumed for both registration and authentication, with security and accuracy in authentication phase.

In order to analyze the memorable, we display small notification for 10 sec in Android application to select pass-images sequence and login. To analyze the usability, we survey the issues of maintaining password. In our implementation password privacy and authority maintained so it is very secure.

B) Environment

We installed JAVA in our OS and JAVA web server, MySQL 5:5:51 are used in server and host in cloud and for two factors verification used Android application 4.4.2.

C) Graphical Analysis

In our implementation, we used two parameters for graphical analysis. First is the execution time of our application and second is user saturation level. In performance we used the execution time period is 5 minutes of whole authentication process user saturation level which is depends upon number of users used this application at a time. The sever cannot get result quickly and it required maximum time. In following graphical analysis blue colour shows for user saturation and green colour execution time for users which is load time for users. The following graph shows the result of analysis.

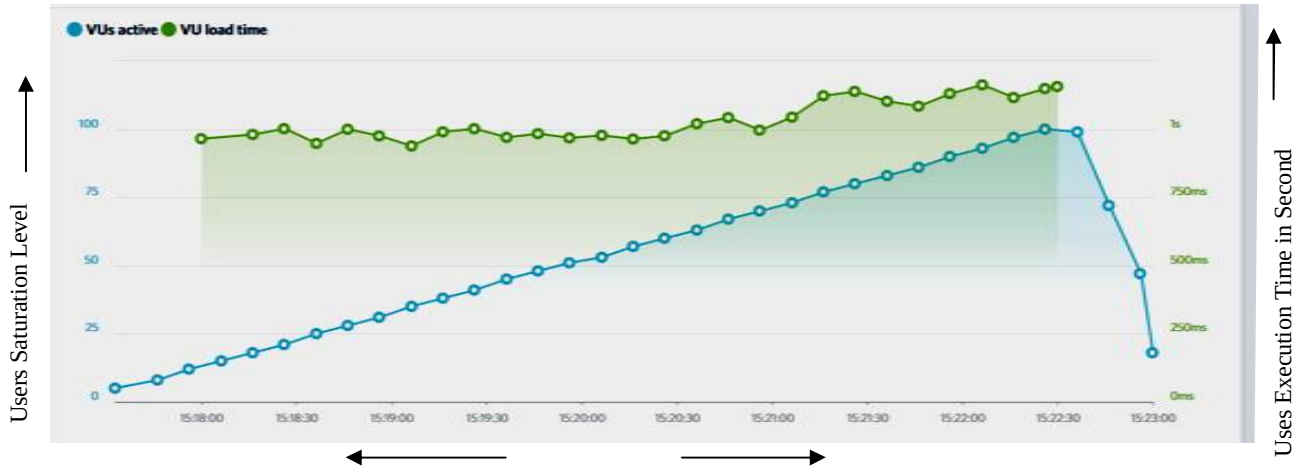


Fig. 9: The graph of analysis of server response time

VII. CONCLUSION

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

In many authentication methods and techniques are available, but each with its own advantages and shortcomings. But in our implementation, we have proposed authentication system which is based on PassMatrix based shoulder surfing resistance graphical authentication schemes. Although our system to reduce the problems with existing graphical based, password schemes and it is two factor authentication system so whenever user login into a system it must require Android application. Our authentication systems to be more secure, reliable and it is main motive to maintain user privacy and authentication.

VIII. ACKNOWLEDGMENT

This implementation work is finished effectively simply because support from every single one including educators, companions. Extraordinarily, I am extremely appreciative to the individuals who give me direction and make this work done.

REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Chen, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transaction on Dependable and secure computing,2016.
[2] S. Vaithyasubramanian, A. Christy and D. Saravanan, "Two Factor Authentications for Secured Login In Support Of Effective Information Preservation And Network Security", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 5, March 2015
[3] Peng Foong Ho, Yvonne Hwei-Syn Kam, Mee Chin Wee, Yu Nam Chong, and Lip Yee Por, "Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects Information", Hindawi Publishing Corporation,The Scientific World Journal, 27 May 2014.
[4] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones".
[5] Rajguru Dipali, J Walunj Jyoti, Jadhav Jayashree, HandeReshma, "Secure Graphical Password Authentication System", IJARIIE,2016.
[6] Prof. S. K . Sonk ar, Prof. R. L. Paikrao, Prof. Awadesh Kumar, Mr. S. B. Deshmukh, " Minimizing Shoulder Surfing Attack using Text and Color Based Graphical Password Scheme". IJARIIE, Vol-2 Issue-2 2016.
[7] Pooja K S, Prajna Venkatramana Dhooli, Prathvi, Prof. Ashwini N, "Shoulder Surfing Resistance Using Graphical Password Authentication In ATM Systems", IJITMIS, Volume 6, Issue 1, pp. 01-10, January - June (2015).
[8]Susan Wiedenbeck, "PassPoints: Design and longitudinal evaluation of a graphical password system", Int. J. Human-Computer Studies 63, 2005.
[9] Brian Chess, "The Case for Mobile Two-Factor Authentication", Building Security In, IEEE Computer Society-2011.
[10] Susan Wiedenbeck, "Authentication Using Graphical Passwords: Basic Results".
[11] Haichang Gao, "A New Graphical Password Scheme Resistant to Shoulder-Surfing".
[12] Xiaoyuan Suo, "Graphical Passwords: A Survey".
[13] Iuliia Tkachenko, "Two level QR code for private message sharing and document authentication",IEEE-2015

BIOGRAPHY

Miss. Anuja A. Ghasad received Bachelor of Engineering degree in Information Technology in the year 2015 and pursuing Master of Engineering degree in Information Technology from Sipna College of Engineering and Technology, Amravati, Maharashtra, India

Prof. A. B. Deshmukh received his Master of Engineering degree in Digital and Electronics, Ph.D (Pursuing)He is currently working as Assistant Professor in IT Department at Sipna College of Engineering and Technology, Amravati, Maharashtra, India

Prof. A. A. Bardekar received his Master of Engineering degree in Computer Science and Engineering, Ph.D (Pursuing) He is currently working as Associate Professor in IT Department at Sipna College of Engineering and Technology, Amravati, Maharashtra, India.