AUTHENTICATION SYSTEM BY IMAGE SEGMENTATION AND SHUFFLING

Rashika Koul, Tanya Kumar, Radhika Malpani, Ashwini Dhongade, Rupali Deshmukh
Department of Information Technology,
Fr. C. Rodrigues Institute of Technology, Vashi
{rashikak295, kumartanya1995, 23radhikamalpani, ashwinidhongade9, rupali7580}@gmail.com

Abstract:* *Prevention of data theft such as bank account numbers, credit card information, passwords, work related documents, etc. is essential in today's communication systems, since many of daily activities depend on the security of the data networks. Although Graphical Authentication Systems have been playing an important role in balking various kinds of bot attacks by acting as an additional mechanism over alphanumeric passwords, yet those have not been used for human authentication to its full potential. By exploiting its feature of easy memorability and the possibility of quadrillion permutation and combination of images that could form the graphical password, an independent human authentication system can be made. The present words focused on developing a authentication system by image segmentation and shuffling. The present system provides high security because shuffling the segments of the image can prevent shoulder surfing attack, as each time the shuffled output will be different, thus the user will pick the same segment from different position each time. The position and sequence should be correct to authenticate a user while logging into the system. The present system concludes that more the number of rows and columns, more will be the number of segments of the image and thus more will be the length and security of the password.

Keywords:* Data Theft, Communication Systems, Security, Bot Attacks, Alphanumeric Password, Graphical Password, Memorability, Graphical password using segmentation of image(GPSI).

I . INTRODUCTION

Graphical Authentication systems such as CAPTCHA , recognition and pure recall based techniques have proved to be useful in many real time systems, but only to prevent bot attacks. Other recall based techniques such as draw a secret and pass points have been introduced as human authentication systems, but have not been implemented widely.[1]
In recognition based techniques, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images . In pure recall based techniques users have to reproduce their passwords without being given any type of hints or reminder.[1]
CAPTCHA is used to test whether the user is human or a robot.Here user is supposed to type the alphanumeric characters of a distorted image that appears on the screen.[2]

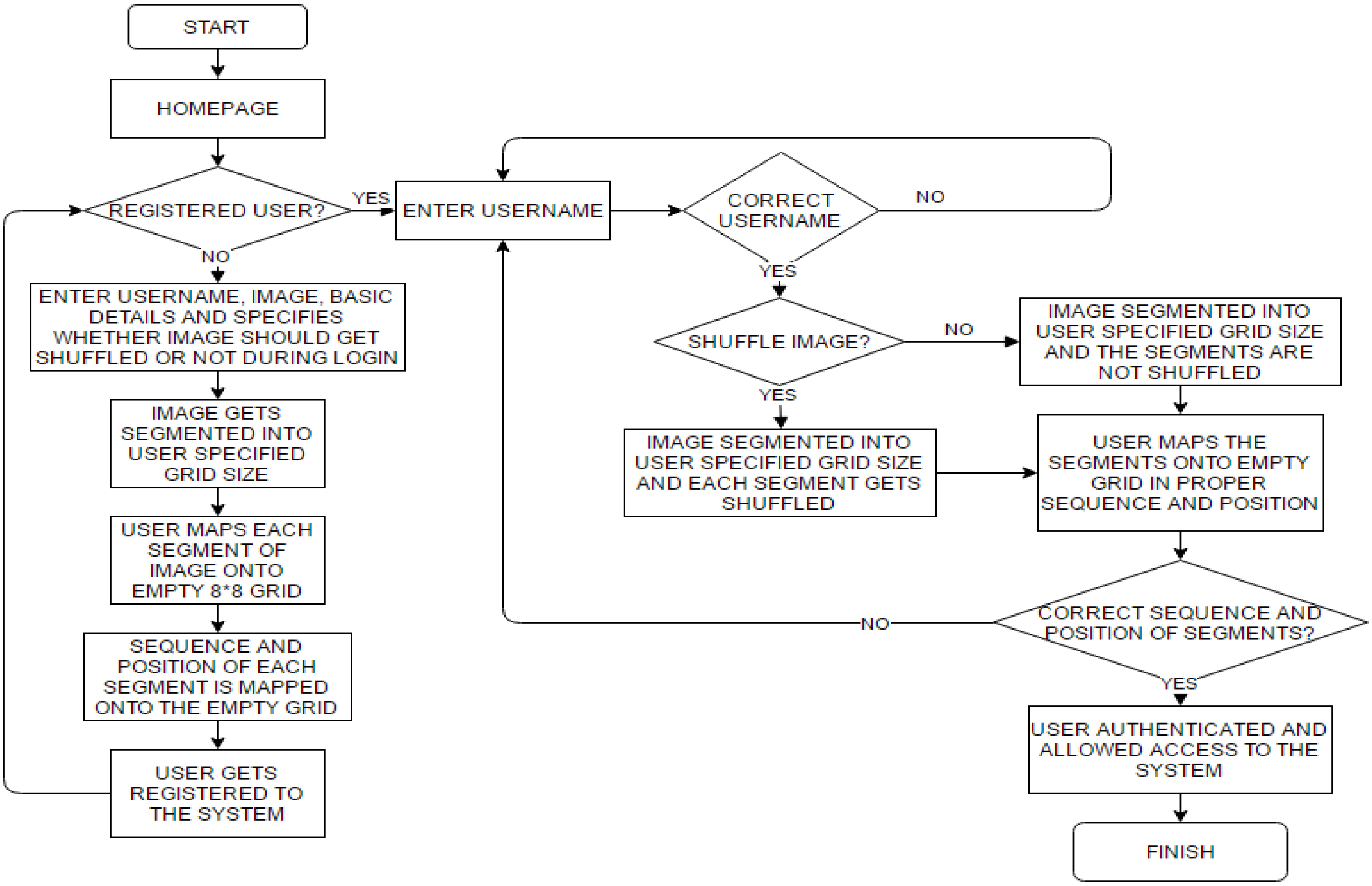
In draw a secret (DAS), user is asked to draw a simple picture on a 2D grid,the coordinates of the grid, occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated.[3]

In the PassPoints graphical password scheme a password consists of a sequence of click points (say 5 to 8) that the user chooses in an image.To login, the user has to click again closely to the chosen points, in the chosen sequence.[3]
Graphical passwords introduced so far have never been used as main authentication systems. The reasons are, that selecting the very same points on the image or using the mouse to draw on the image is a tedious job and to get the exact same design every time one draws with the mouse is nearly impossible.[4]

Graphical Password by Segmentation of Image (GPSI) is a human authentication system that aims to provide security to all kinds of systems like web applications, digital lockers and even real lockers for that matter. Because Graphical Password by Segmentation of Image (GPSI) can be used independently to authenticate users, it has a potential to replace existing authentication systems such as alphanumeric passwords. It also eliminates the need to select same intricate points on an image or draw the same design every time during login.[4]

II. IMPLEMENTATION

To understand the complete workflow of a system , flow chart of present system is shown and explained below.


START
HOMEPAGE
REGISTERED USER?
YES
NO
ENTER USERNAME, IMAGE, BASIC DETAILS AND SPECIFIES WHETHER IMAGE SHOULD GET SHUFFLED OR NOT DURING LOGIN
IMAGE GETS SEGMENTED INTO USER SPECIFIED GRID SIZE
USER MAPS EACH SEGMENT OF IMAGE ONTO EMPTY 8*8 GRID
SEQUENCE AND POSITION OF EACH SEGMENT IS MAPPED ONTO THE EMPTY GRID
USER GETS REGISTERED TO THE SYSTEM
ENTER USERNAME
CORRECT USERNAME
NO
YES
SHUFFLE IMAGE?
NO
YES
IMAGE SEGMENTED INTO USER SPECIFIED GRID SIZE AND THE SEGMENTS ARE NOT SHUFFLED
IMAGE SEGMENTED INTO USER SPECIFIED GRID SIZE AND EACH SEGMENT GETS SHUFFLED
USER MAPS THE SEGMENTS ONTO EMPTY GRID IN PROPER SEQUENCE AND POSITION
CORRECT SEQUENCE AND POSITION OF SEGMENTS?
NO
YES
USER AUTHENTICATED AND ALLOWED ACCESS TO THE SYSTEM
FINISH

.Fig. 1**.** Flowchart of Graphical Password by Segmentation of Image[4]

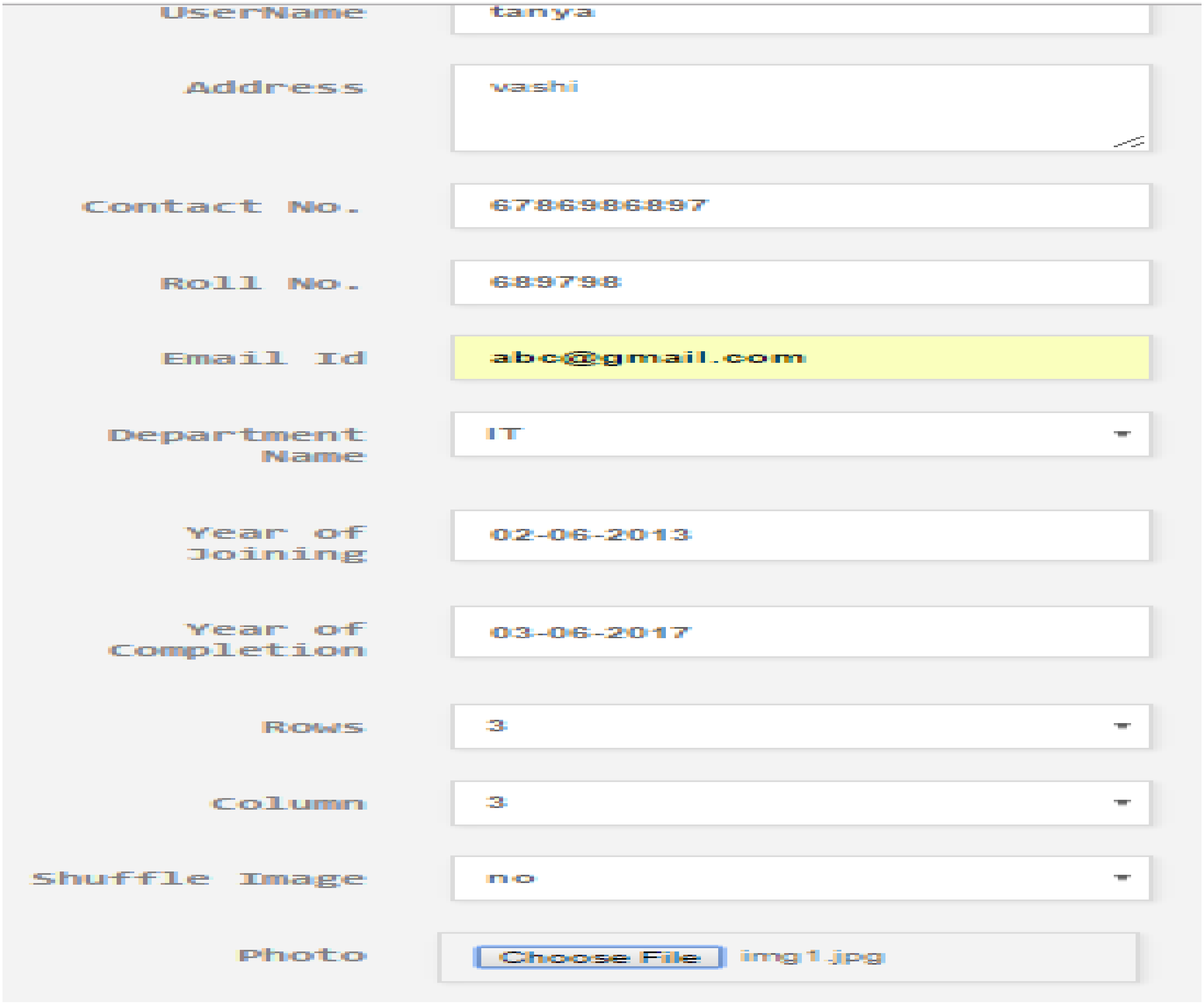
The flow of the system can be divided into two phases:

A. Registration Phase

B. Login Phase

A. Registration Phase

Apart from the general user credentials like username, email id, etc. the user is asked to provide an image and mention the number of rows (maximum of 8) and columns (maximum of 8) of the grid in which the user’s image will be segmented as shown in Fig. 2.



UserName	tanya
Address	vashi
Contact No.	6786986897
Roll No.	689798
Email Id	abc@gmail.com
Department Name	IT
Year of Joining	02-06-2013
Year of Completion	03-06-2017
Rows	3
Column	3
Shuffle Image	no
Photo	Choose File img1.jpg

Fig. 2. Registration form

Initially, Input image is scaled as follows :

Step 1. Obtain length X and width Y of image.

Step 2. If X and Y is less than fixed length(3cm) and width then X and Y is incremented.

Then , the image is segmented using Block-Based Normalised-Cut Algorithm:-

Step 1: Obtain length X and width Y of image.

Step 2: Get the number of rows and columns in which image is to be segmented.

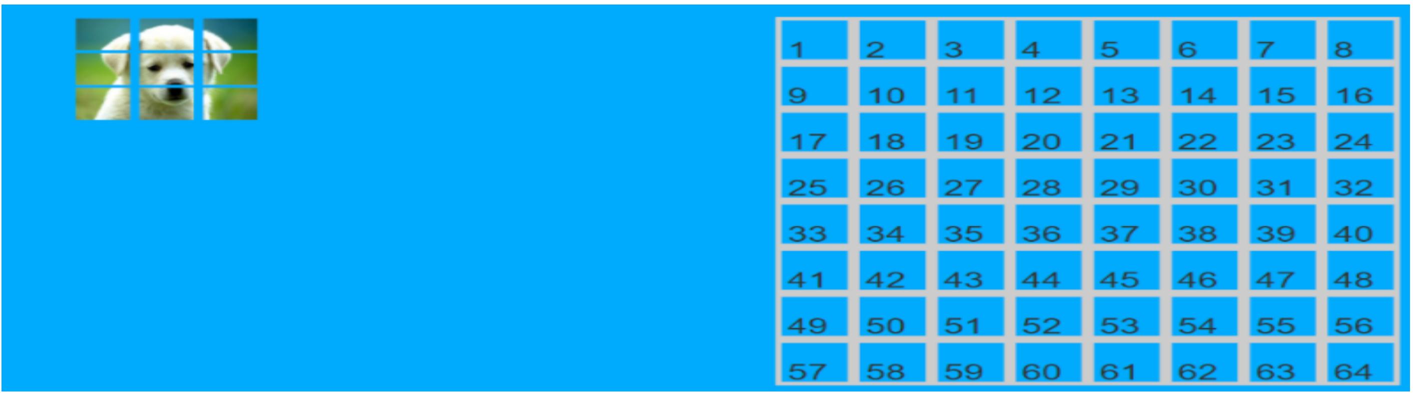
Step 3: Obtain the length of each segment by dividing the length of the image by the number of columns.

Step 4: Obtain the width of each segment by dividing the width of the image by the number of rows.

Step 5: Display each segment.

Hence , User's image is then segmented into the grid of user specified rows and columns for the user to drag each segment onto the empty grid of size 8x8 as shown in fig.3 and fig. 4 respectively.

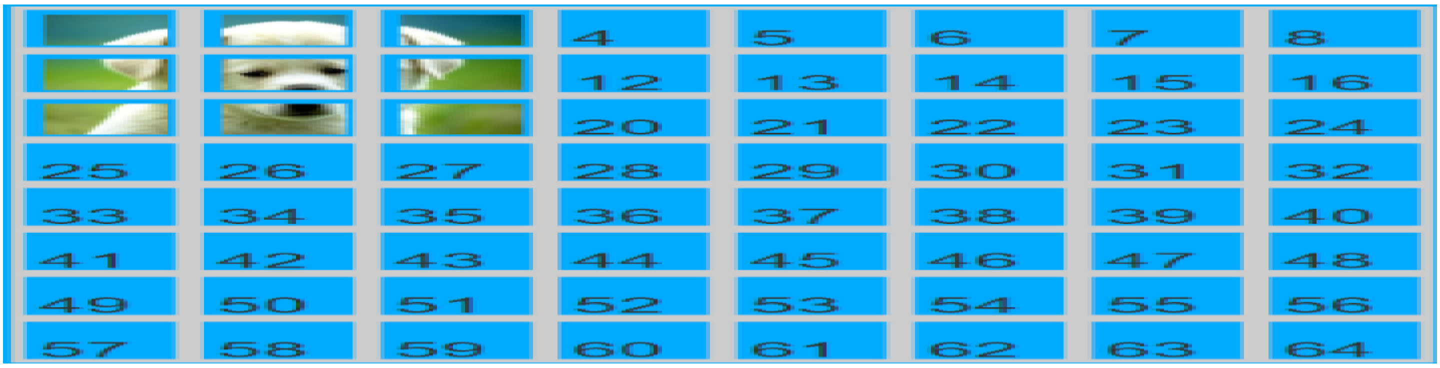
,



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig. 3. Segmented image

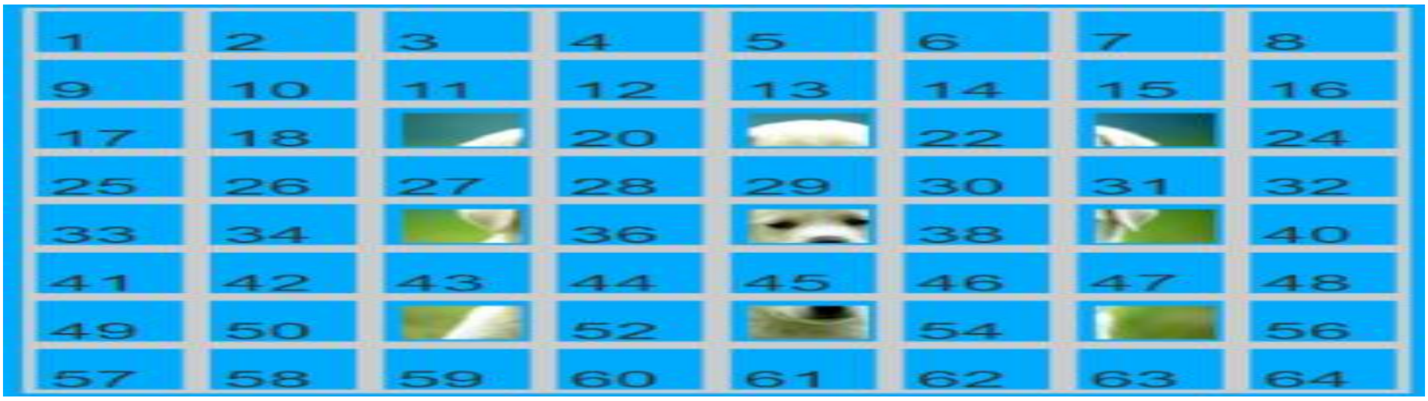
Image chosen by the user during registration phase is presented to user in segmented form as shown in fig 3.



			4	5	6	7	8
			12	13	14	15	16
			20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

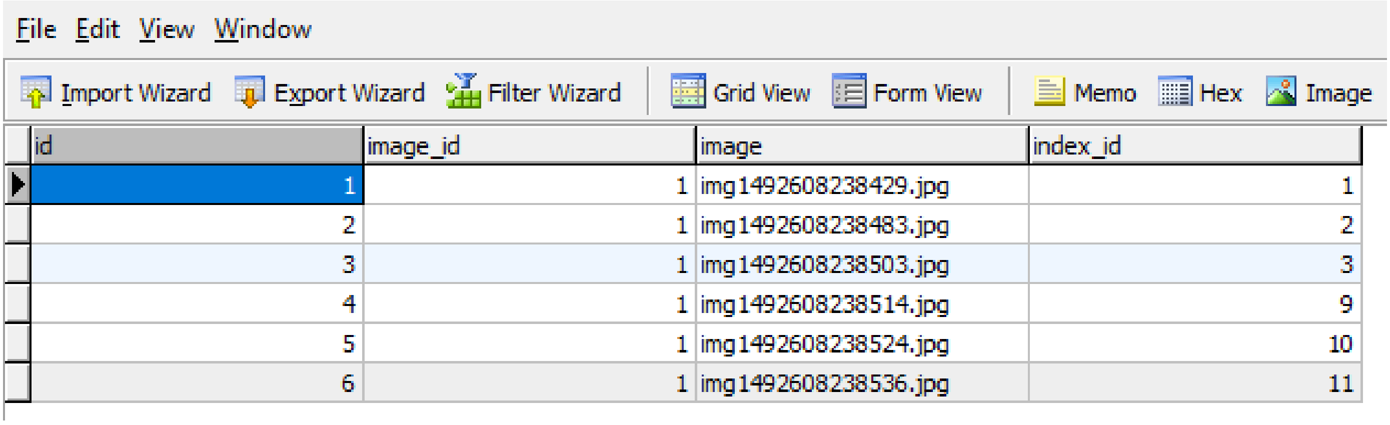
Fig. 4. Setting of user’s password for 3x3 segmentation

User is asked to drag and drop each segment of image anywhere on a 8x8 empty grid as shown in fig 4and fig 5.User is supposed to remember the sequence and position of where the segment is mapped in a 8x8 empty grid.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18		20		22		24
25	26	27	28	29	30	31	32
33	34		36		38		40
41	42	43	44	45	46	47	48
49	50		52		54		56
57	58	59	60	61	62	63	64

Fig. 5. A different complex example of user’s password for 3x3 segmentation



id	image_id	image	index_id
1	1	img1492608238429.jpg	1
2	1	img1492608238483.jpg	2
3	1	img1492608238503.jpg	3
4	1	img1492608238514.jpg	9
5	1	img1492608238524.jpg	10
6	1	img1492608238536.jpg	11

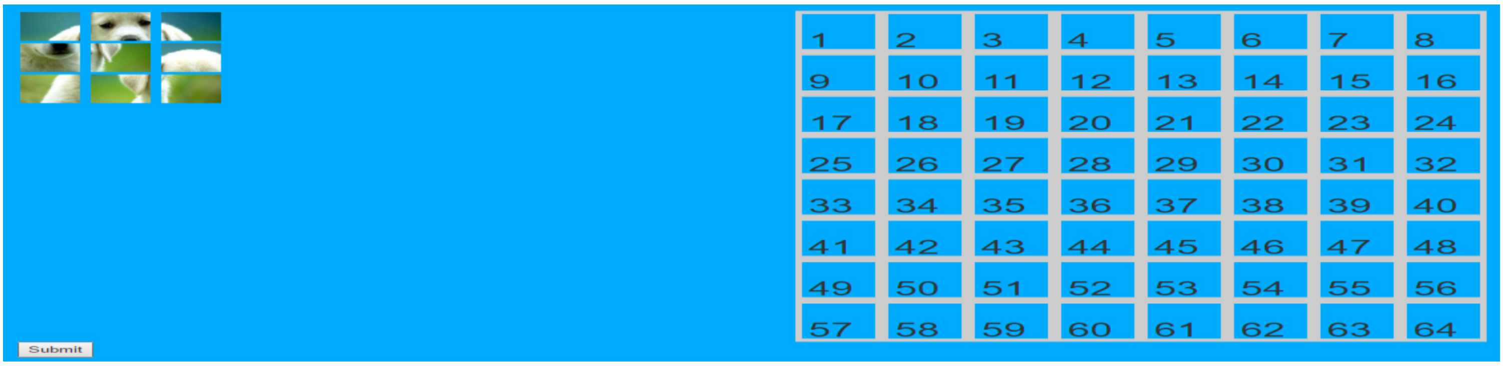
Fig.6 Database of a 3x2 segmentation

Each image segment is represented by a number in column ‘id’.Each user is represented by a number as shown in column ‘image id’.Each image segment is stored with particular image name in column ‘image’.The last column show how each segment is saved in the same sequence in which the user had picked them up along with their position number represented by ‘index_id’.

B. Login Phase

During login, when the user wishes to access the system the image segments will be presented in a shuffled manner as shown in fig. 7, if the user has enabled shuffling during registration. Otherwise, segments are displayed without shuffling as shown in fig. 8. The shuffling is done using Collections.shuffle function in java.util package, which basically uses the Fisher-Yates Shuffle[5] algorithm explained as follows:

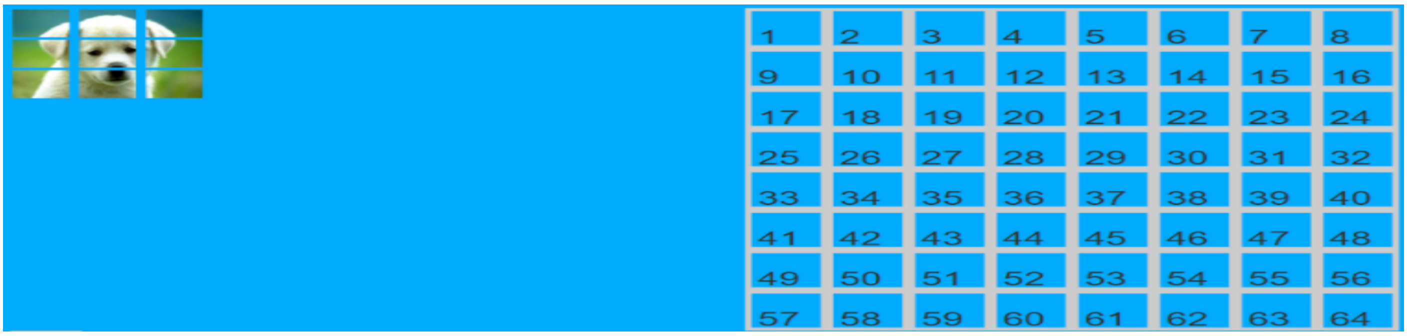
1. Store the segments from 1 through N as numbers from 1 to N where N=mxn and m and n are number of rows and columns respectively.
2. Pick any random number k between one and the number of unstruck numbers remaining (inclusive).
3. Counting from the low end, strike out the kth number not yet struck out, and write it down at the end of a separate list.
4. Repeat from step 2 until all the numbers have been struck out.
5. The sequence of numbers written down in step 3 is now a random permutation of the original numbers.
6. Since each of these numbers represent each image segment, the segments are also jumbled accordingly.[5]



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig.7 Shuffled Image

Image chosen by the user during registration phase is segmented,shuffled and presented to user during login phase as the user choses to shuffle image during registration phase.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

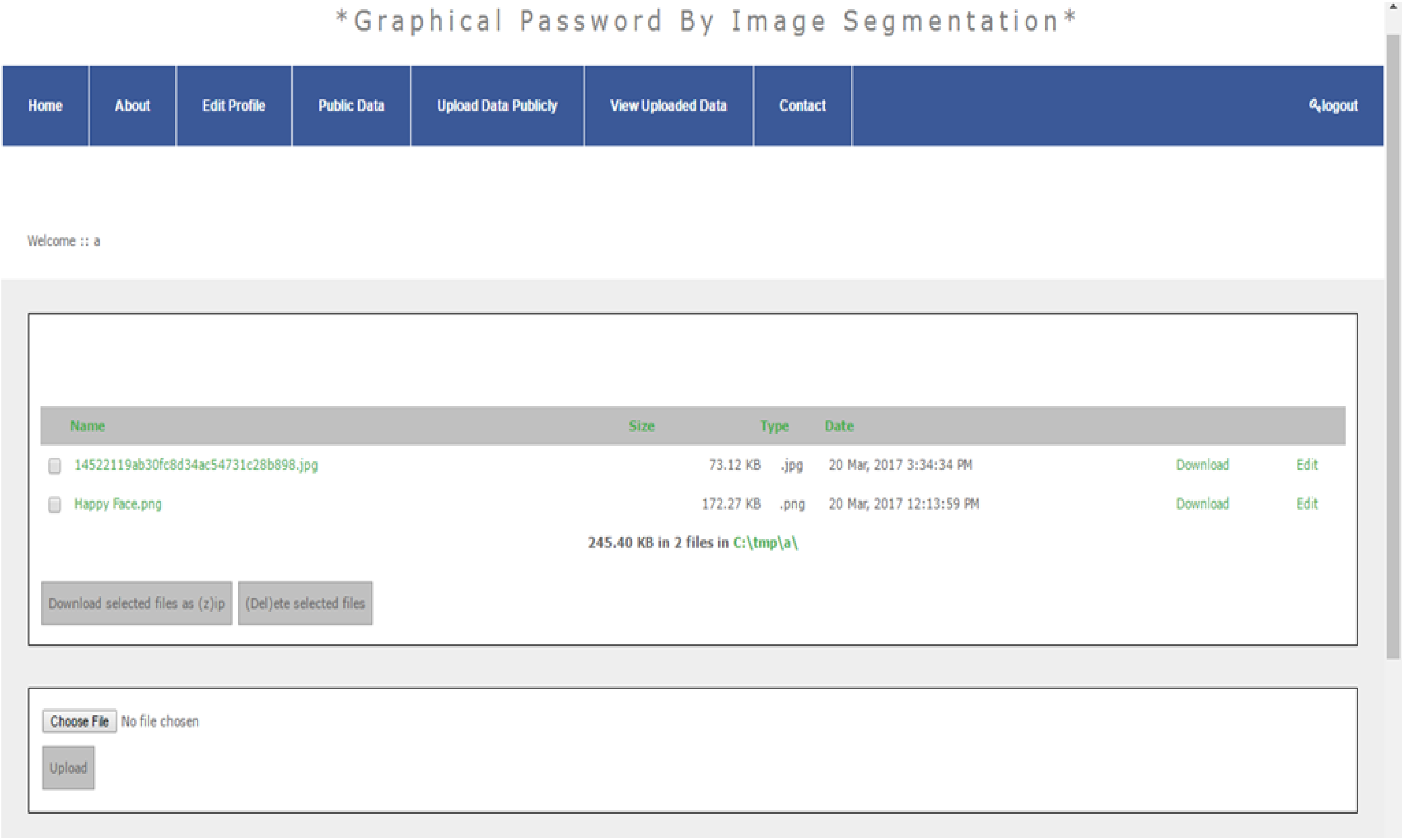
Fig. 8. Unshuffled Image

Image chosen by the user during registration phase is segmented,unshuffled and presented to user during login phase as the user choses to unshuffle image during registration phase.

To be considered as authentic, the user has to drag the segments onto the empty grid of size 8x8 in the correct sequence and at the correct position.[4]

C. Learning Management System

After the user is authenticated , user will be directed to the Learning Management System. This is an application developed for the department of a college, wherein data can be shared between the students and the faculty, faculty and the hod and hod and students. It allows the user to grant access to the other users to view and download the data/file.



Graphical Password By Image Segmentation

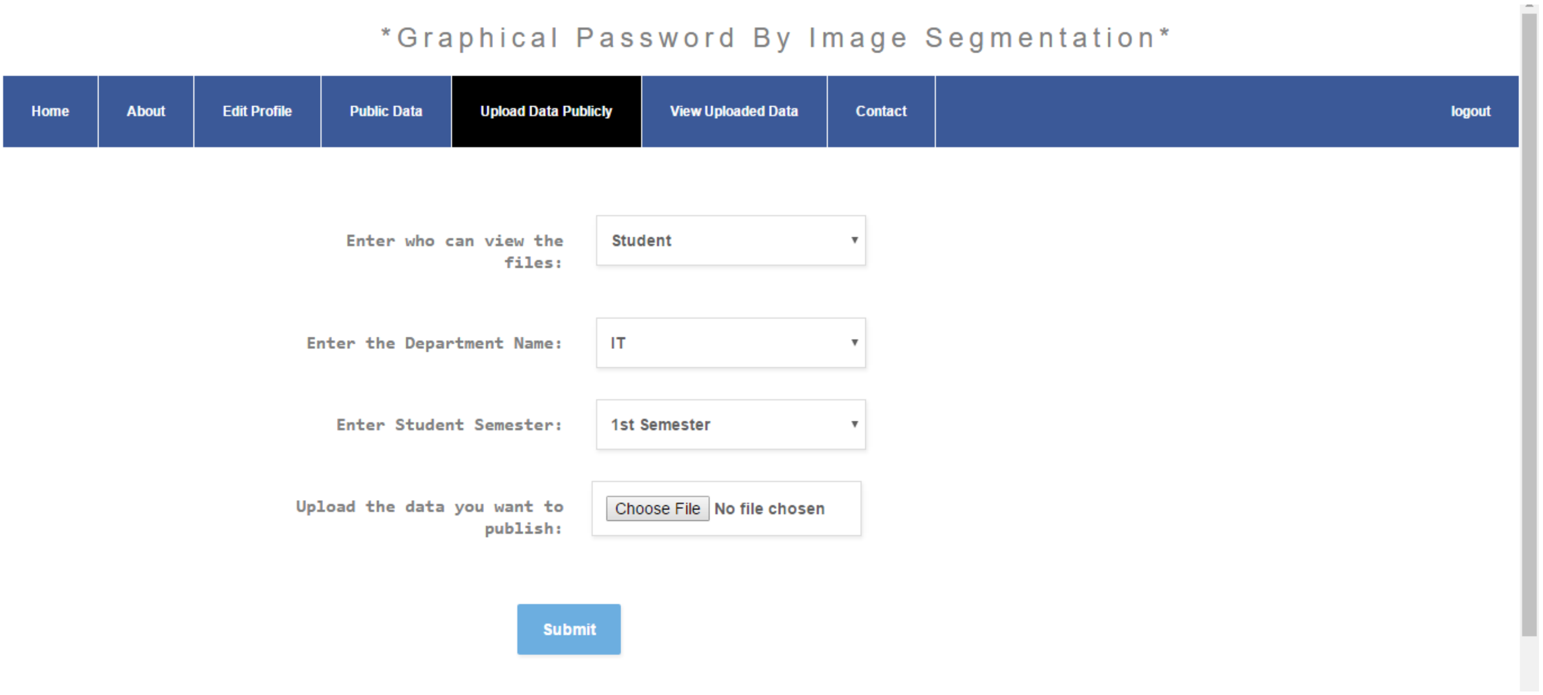
Welcome :: a

Name	Size	Type	Date		
□ 14522119ab30fc8d34ac54731c28b898.jpg	73.12 KB	.jpg	20 Mar, 2017 3:34:34 PM	Download	Edit
□ Happy Face.png	172.27 KB	.png	20 Mar, 2017 12:13:59 PM	Download	Edit

245.40 KB in 2 files in C:\tmp\a\

Fig. 9. Learning Management System User Homepage

Fig 9 shows the home page of the application where user is directed after successful login to the system. Here , user can upload/download his personal files and these files can be viewed only by him.



Enter who can view the files: Student

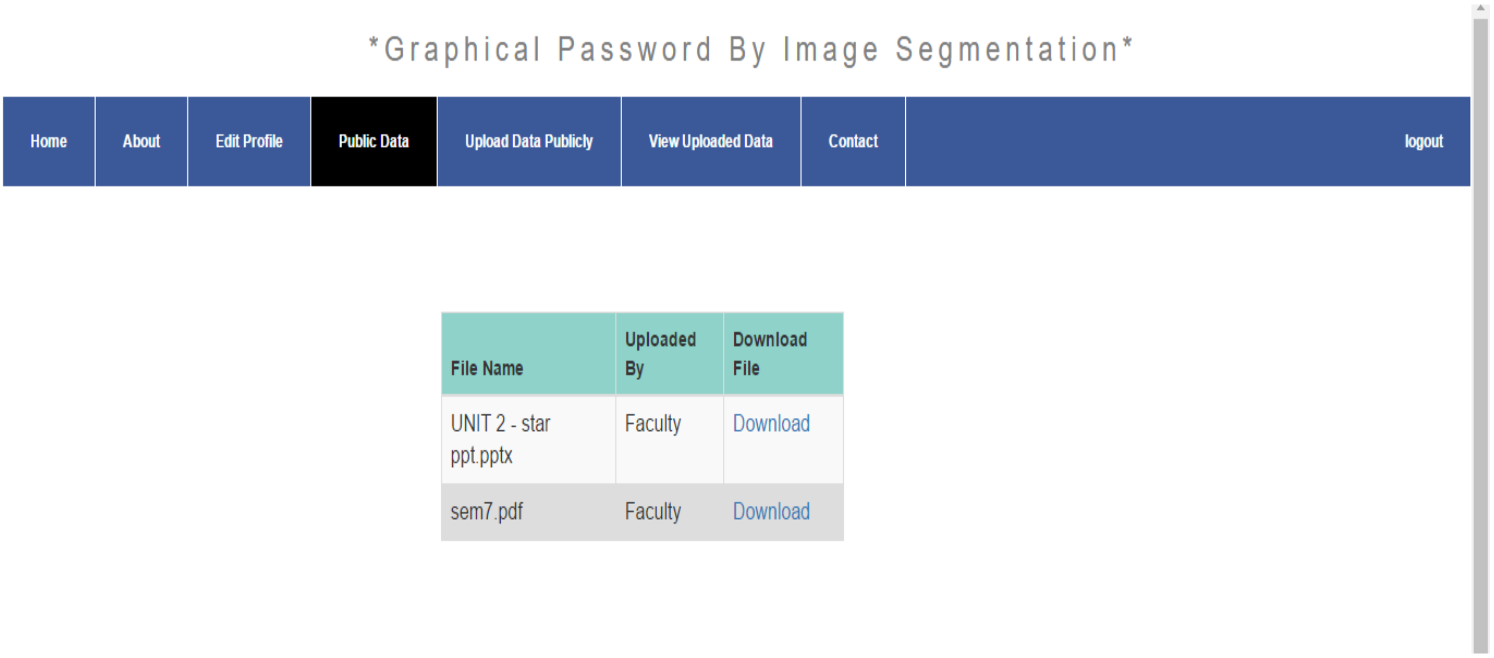
Enter the Department Name: IT

Enter Student Semester: 1st Semester

Upload the data you want to publish: Choose File No file chosen

Fig. 10. User giving access to other users to view and download data.

User can choose between student/faculty/hod of particular department i.e, IT/COMPS/EXTC/MECH/ELEC and also the semester to which he wants to grant access to download and view data as shown in fig 10.

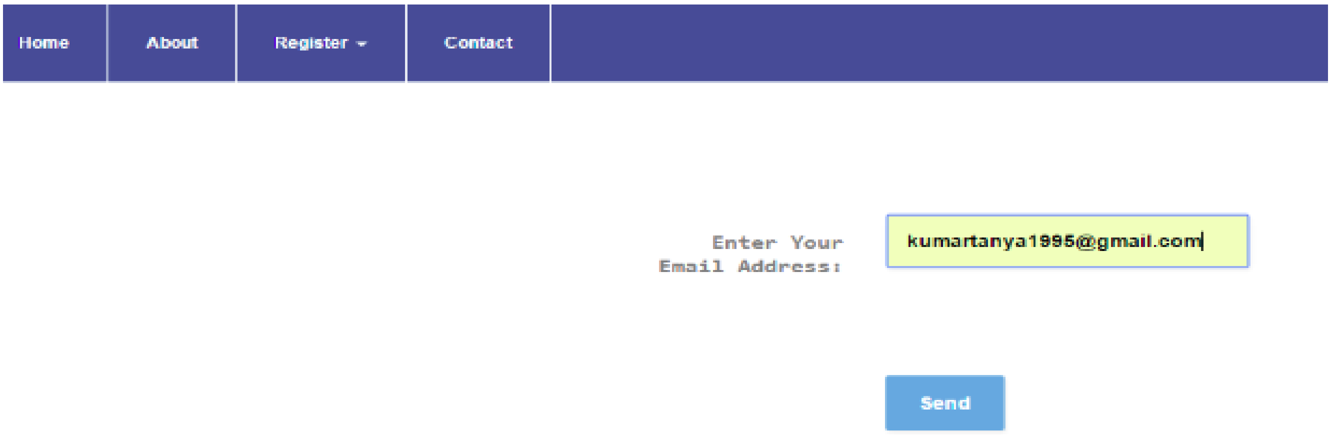


File Name	Uploaded By	Download File
UNIT 2 - star ppt.pptx	Faculty	Download
sem7.pdf	Faculty	Download

Fig. 11. Public data that this user is given access to.

Other users can provide access to this user to view and download data and the files which the user is given access and can be viewed and downloaded under ‘public data’ as shown in fig 11.

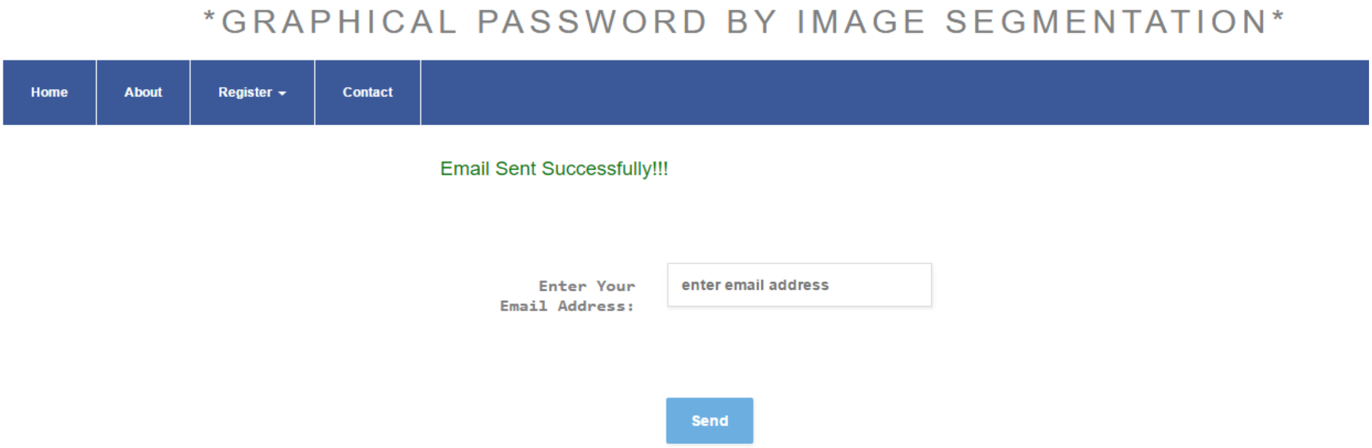
D. Forgot Password



Enter Your Email Address: kumartanya1995@gmail.com

Fig. 12**.** User enters registered email address

If user forgets his password then user clicks on forget password. Here, user is asked to provide correct email id as shown in fig 12. If email id matches with that of mentioned by the user during registration phase then an link is sent to the users email address.



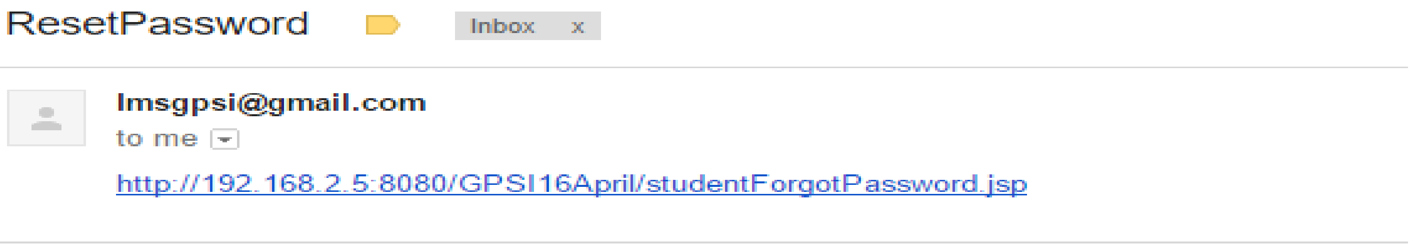
GRAPHICAL PASSWORD BY IMAGE SEGMENTATION

Email Sent Successfully!!!

Enter Your Email Address: enter email address

Fig 13. Email sent to mail address.

After link has been sent to user’s mail address ,message is displayed which confirms email has successfully sent to provided mail address of user as shown in fig 13.



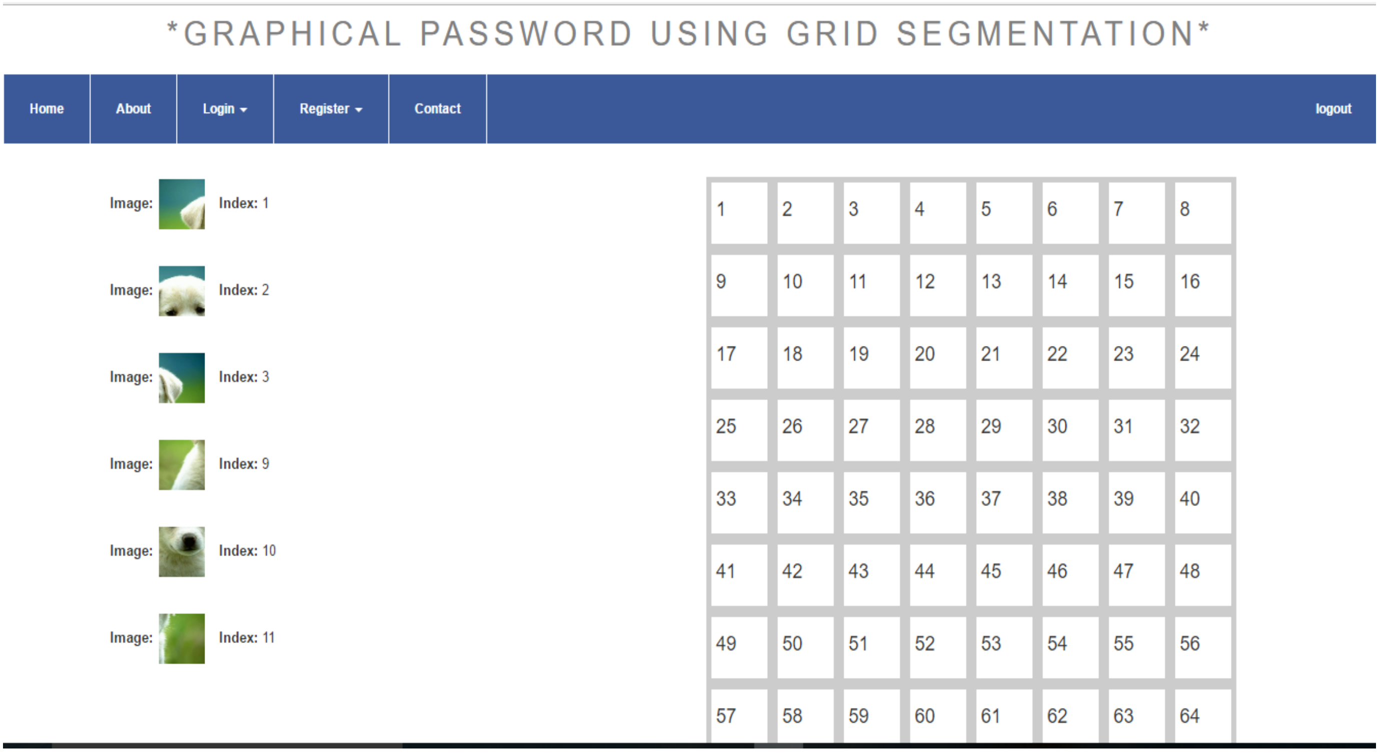
ResetPassword

Imsgpsi@gmail.com

to me

http://192.168.2.5:8080/GPSI16April/studentForgotPassword.jsp

Fig 14. Link recieved on mail address



GRAPHICAL PASSWORD USING GRID SEGMENTATION

Image: Index: 1

Image: Index: 2

Image: Index: 3

Image: Index: 9

Image: Index: 10

Image: Index: 11

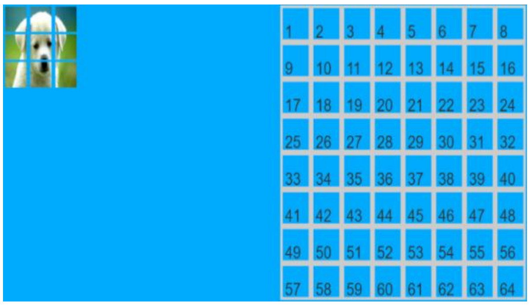
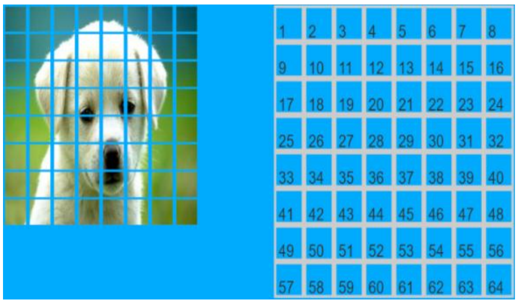
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

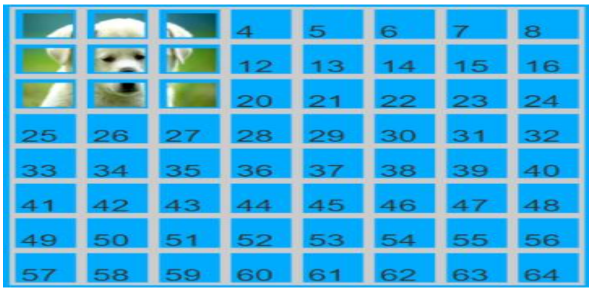
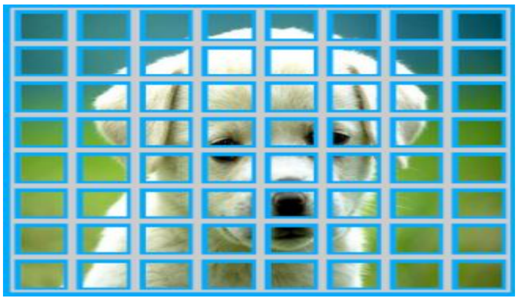
Fig. 15. Password with proper index and sequence retrieved.

After the user clicks on the link,user is directed to a page which will provide user password with correct sequence and index as set by the user during registration phase is provided to user as shown in fig 15.

III.COMPARISON OF 3X3 AND 8X8 SEGMENTATION

Table 1. Comparison of 3x3 and 8x8 segmentation

	3x3 segmentation	8x8 segmentation
Snapshots		
Number of Segments	3 rows X 3 columns = 9 segments	8 rows X 8 columns = 64 segments
Length of Password	Length of the password will be 9 segments.	Length of the password will be 64 segments.
Password Strength	Since the user has to know the sequence in which the 9 segments were dragged and the 9 positions on which they were placed on the empty grid, the security is less in comparison to higher number of segments.	The security increases as it will be nearly impossible for the attacker to guess the sequence in which 64 segments were dragged and the 64 positions on which they were placed on the empty grid by the legitimate user.

User’s Password	 4 5 6 7 8 12 13 14 15 16 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64	

Apart from the number of segments, shuffling of segments is one more criteria that will decide the strength of the password. If the user chooses to shuffle the image then during login, the image segments will be displayed in shuffled manner. Every time the user logs in, the manner in which the segments are shuffled will be different. Thus the user will pick up the same segment from different positions each time.

IV.CONCLUSION

Graphical passwords offers better security than text-based passwords. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But in a series of selectable images, possible combinations that could form the graphical password are so many that it would take millions of years to break into the system.

This study concludes that more the number of rows and columns, more will be the number of segments of the image and thus more will be the length and security of the password. It is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. Shuffling the segments of the image can prevent shoulder surfing attack, as each time the shuffled output will be different, thus the user will pick the same segment from different positions each time while logging into the system.

V.REFERENCES

[1].Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget, “Modeling user choice in the PassPoints graphical password scheme” <https://cups.cs.cmu.edu/soups/2007/proceedings/p20_dirik.pdf>

[2]. Ragavendra .A, Jeysree .J, “GRAPHICAL PASSWORD AUTHENTICATION USING CaRP”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015

[3]. Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle, “Comparison of Graphical Password Authentication Techniques”, International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015

[4]. Rashika Koul, Tanya Kumar, Radhika Malpani, Ashwini Dhongade, Rupali Deshmukh, “GPSI: Graphical Password by Segmentation of Image” International Journal of Research and Scientific Innovation (IJRSI) | Volume III, Issue XI, November 2016 | ISSN 2321-2705

[5]. Ronald Fisher, Frank Yates [1938]. Statistical tables for biological, agricultural and medical research (3rd ed.). <https://en.wikipedia.org/wiki/Fisher–Yates_shuffle>

[6]. Margaret Rouse, “graphical password or graphical user authentication (GUA)”. <http://searchsecurity.techtarget.com/definition/graphical-password>

[7]. Xiaoyuan Suo, Ying Zhu, G. Scott Owen, “Graphical Passwords: A Survey.”, DOI: 10.1109/CSAC.2005.27 · Source: DBLP Conference: 21st Annual Computer Security Applications Conference (ACSAC 2005), 5-9 December 2005, Tucson, AZ, USA

[8] . Haiyu Song, Xiongfei Li, Pengjie Wang, Jingrun Chen, “Block-Based Normalized-Cut Algorithm for Image Segmentation”, Online ISBN 978-3-642-05173-9

[9]. J. C. Birget, D. Hong N. Memon, S. Man and S. Wiedenbeck., “The Graphical Passwords Project” Funded by the NSF Cyber Trust Program. http://clam.rutgers.edu/~birget/grPssw/

[10]. Arash Habibi Lashkari, Samaneh Farmand, Dr. Rosli Saleh, Dr. Omar Bin Zakaria, “A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns ”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009

[11]. Saranya Ramanan, Bindhu J S, “A Survey on Different Graphical Password Authentication Techniques”, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 12, December 2014

[12]. Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle, “Comparison of Graphical Password Authentication Techniques”, International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015

[13]. Ibrahim Furkan Ince, Ilker Yengin, Yucel Batu Salman, Hwan-Gue Cho, Tae-Cheon Yang, “DESIGNING CAPTCHA ALGORITHM: SPLITTING AND ROTATING THE IMAGES AGAINST OCRs”, Third 2008 International Conference on Convergence and Hybrid Information Technology