INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

Graphical Password Authentication by using Image Segmentation

Pratiksha Pawar, Nikita Gadge, Shraddha Khamakr, Prof. S. S. Adsure

Department of Computer Engineering, JSPM's Bhivarabai Swant Institute of Technology, Pune, India

ABSTRACT: In this paper, Graphical passwords have been designed to try to make password more memorable and easier for people to use, and it is less vulnerable to brute force attacks than a text-based password. The aim of Graphical password by segmentation of image (GPSI) is to implement a strong security for a learning management system The coordinates of the segmented image allow the system to fragment the image and store it as different parts.

KEYWORDS: Graphical password , image,Login,Security.

I. INTRODUCTION

A) Passwords Should Be Easy To Remember, And The User Authentication Protocol Should Be Executable Quickly And Easily By Humans.B) Passwords Should Be Secure, I.E., They Should Look Random And Should Be Hard To Guess; They Should Be Changed Frequently, And Should Be Different On Different Accounts Of The Same User. They Should Not Be Written Down Or Stored In Plain Text. Hence, Graphical Passwords Act As Alternative To Alphanumeric Passwords Because They Serve As A Solution To The 'Password Problem'.

II. RELATED WORK

The different types of passwords used nowadays are recognition-based and recall based are some of the examples. In recall based,a person is required to regenerate the password, he stored atthe time of registration process. The disadvantage in this process is that it depends on recall of password and if the user does a mistake the authentication isdenied.In the recall based process, there is a chance of someone replicating the same password.Jeermyn,et al
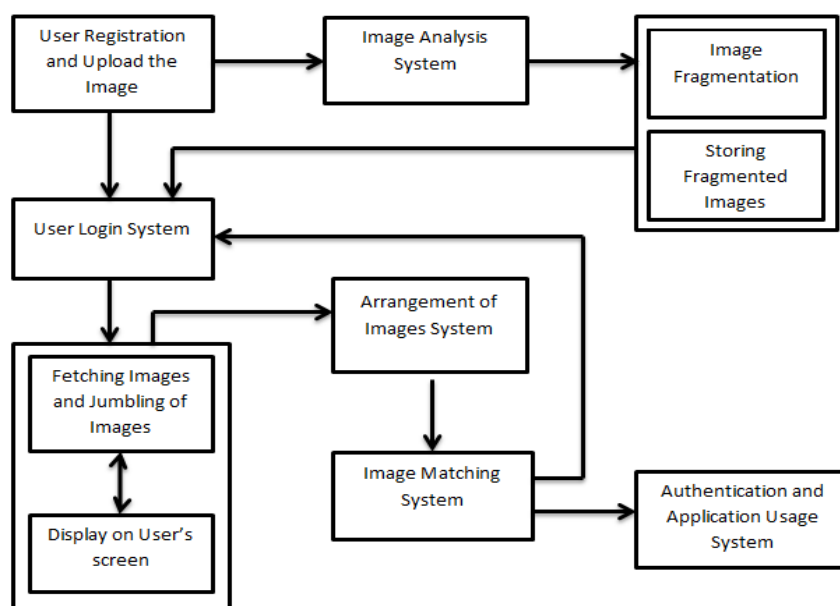
III. METHODOLOGY

Fig.1 System Architecture

In this architecture first is a user registration and upload the image .The user will be filled their information and select password image .Then system is analysis image and stored image as a password then user will be login to the system &fetcvh that image and this image will be jumbling then image will be display on our screen.ater fetching image system are arranged pattern of image then image will be the matching the system and check authentication & application use of system
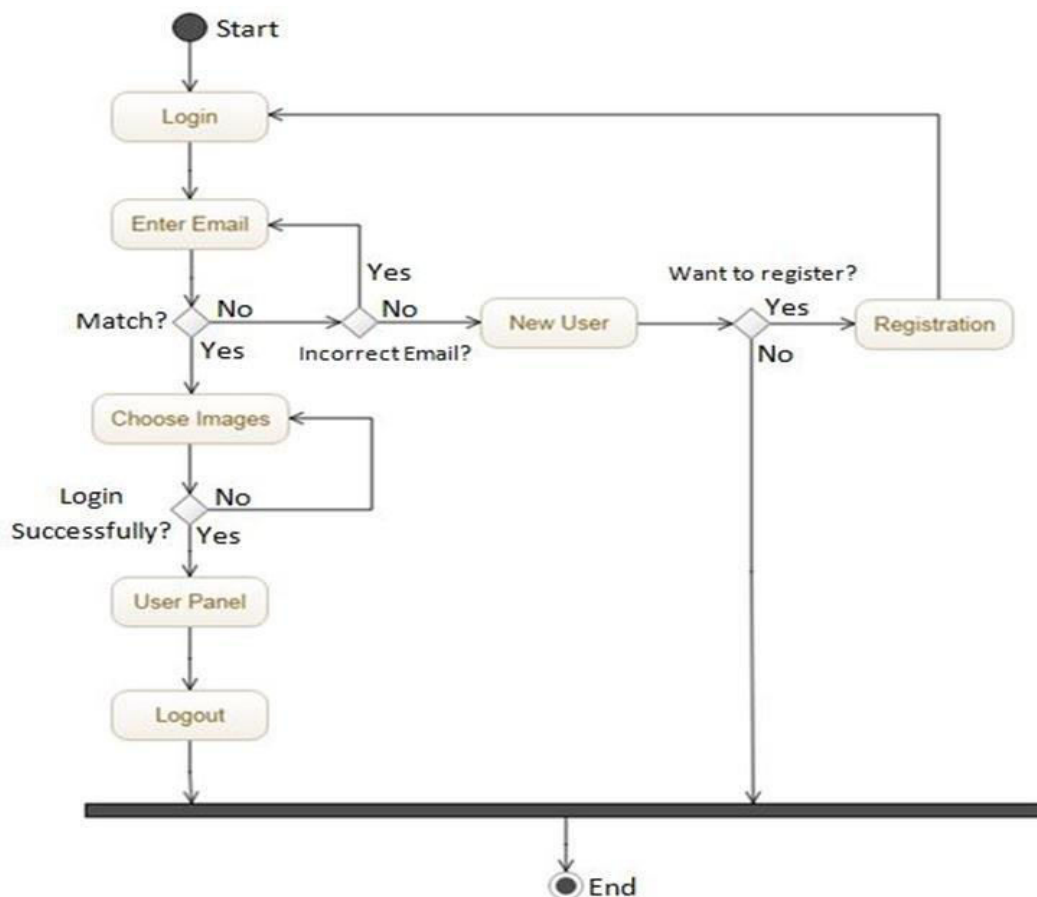

Fig.3 Activity Dig.

IV. CONCLUSION

The Main Argument For Graphical Passwords Is That People Are Better At Memorizing Graphical Passwords Than Text-Based Passwords. Our Preliminary Analysis Suggests That It Is More Difficult To Break Graphical Passwords Using The Traditional Attack Methods Such As Brute Force Search, Dictionary

REFERENCES

[1].J.C.Birget, D.Hong N.Memon, S.ManandS.Wiedenbeck., "The Graphical Passwords Project" Funded by the NSF Cyber Trust Program. ¡http://clam.rutgers.edu/ birget/grPssw/¿

[2]. Ragavendra .A, Jeysree .J, "GRAPHICAL PASSWORD AU- THENTICATION USING CaRP", International Journal of Ad- vancedResearchinComputerEngineeringTechnology(IJARCET)

[3].IbrahimFurkanInce,IlkerYengin,YucelBatuSalman,Hwan-GueCho,Tae-CheonYang,"DESIGNINGIMAGEALGORITHM: SPLITTINGANDROTATINGTHEIMAGESAGAINSTOCRs",

Third 2008 International Conference on Convergence and Hybrid Information Technology

[4].Ahmet Emir Dirik, Nasir Memon,Jean-CamilleBirget," Mod- eling user choice in the Pass Points graphical password scheme"

[5] https://cups.cs.cmu.edu/soups/2007/proceedings/p20$_d$irik.pdf ⟩

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 🟢 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details