ENGINEERING IN ADVANCED
RESEARCH SCIENCE AND
TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.03
October-2023
Pages: 952-958

A NOVEL DEEP LEARNING AND SVM-BASED MISSING CHILD IDENTIFICATION SYSTEM

*** Ms. ARATHI KASTURI**
*Assistant Professor, Department of CSE, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, TELANGANA, India
G.PAVANI[1], S.INDIRA[2], J.MANOGNA[3], KL NANDHINI[4]
[1,2,3,4] B. Tech Pursuing, Department of CSE, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, TELANGANA, India.

ABSTRACT

Authentication established on passwords is utilized typically in functions for protection and protection. Still, human actions, as an example, deciding on awful passwords and contributing passwords in rectangular measures are considered as "the most fragile connection" in the Authentication chain. Maybe than discretionary alphanumeric strings, consumers will pick out passwords both brief or vast for easy memorization. With net functions and versatile functions accumulation, persons can get to these purposes every time and wherever with a number of gadgets. This development brings first-rate lodging yet, in addition, builds the possibility of offering passwords to undergo driving attacks. Attackers can be aware straightforwardly or make use of outdoor recording devices to collect client's qualifications. To keep away from this type of issue, we want some other approach of confirmation. Here, we can pick out a graphical authentication method. The photograph password affords the exceptional method to signal on that is easier than recollecting and composing alongside with easy passwords. You can signal in by way of tapping the proper factors or growing the proper gestures over an photo that you simply choose in advance.

INDEX TERMS: Authentication, Simple memorization, right gestures.

1. INTRODUCTION

1.User Authentication is an interaction that permits a gadget to approve the character of an individual who associates with network assets.

Commonly textual passwords are the most used form of authentication for all websites and applications. Textual passwords consist of a string of characters which may also include special characters and numbers. In most cases, users may use only one username and password for multiple accounts. But they are not fully secured. So, we should maintain strong passwords, comprising numbers, uppercase, and lowercase letters. Then these textual passwords are considered strong enough to resist brute force attacks. However, a strong textual password is hard to remember and recall. Along these lines clients will in general pick passwords that are either short or from the word reference, instead of irregular alphanumeric strings. Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication. Shoulder surfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device. A strong textual password is hard to memorize and recollects. To avoiding such problems, we are presenting a secure graphical web-based authentication system that protects users from becoming victims of shoulder surfing attacks.

2.LITERATURE SURVEY

Wantong Zheng and Chunfu Jia proposed a method Combined PWD. This scheme proposes an online secret phrase verification component, combined PWD, through embedding separators(e.g., spaces) into the passwords to reinforce the current secret word validation framework. This plan uses the custom of the clients input. In this examination, site clients can embed spaces in their secret word where they need to stop when they register a record and the site back-end records the number of spaces in each hole . A novel time-based unique password was contributed to avoiding challenges ofusing a third party such as one- time password email, test and token device, the client will set an underlying secret word to characterize how the secret key will be changing throughout a characterized time, we tracked down that the framework. Then found that the system retains the strength of the dynamic password and improves the usability of the system in terms of availability.A strong password authentication scheme was proposed by Yang Jingbooo. The one-time password authentication schemes can be divided into two types namely weak- password authentication schemes and strong-password authentication schemes. In this paper, we survey the as of Kus scheme and italso shows an attack against his protocol. And also found that strong passwords have higher strength and easily guessing is not possible. Later, we present a strong password authentication scheme. This paper expands W. C. Ku's plan so that the alteration convention can oppose Stolen-verifier assault. The changed convention is built without loss of effectiveness.Here, we use a picture password for the second authentication. So, no need for complex textual passwords. Users can use any basic textual password. The system is classified into three modules.Hua Wang, Yao Guo proposes another reuse- situated secret phase authentication system, called Desktop Password Authentication Center (DPAC), to reuse counter-measures among applications, along these lines lessening the expense of protecting passwords against dangers. This arrangement can take out a ton of tedious work and reduces the expense essentially, we demonstrate the feasibility ofDPAC by implementing a prototype, in which we migrate the widely used OpenSSH to DPAC and implement two example countermeasures . Password authentication code (PAC) is a very important issue in many applications such as web- sites and database systems etc. Salah Refish proposes a PAC-RMPN scheme. In this paper, PAC between two clients to affirm verification between them has been introduced. This research presents a novel solution to the era-long problem of password authentication at the incoming level. They should discover a strategy to secure this a secret word from anticipated attackers. A legitimate user types his password only and presses enter to propagate it to another user which he wants to be authenticated .

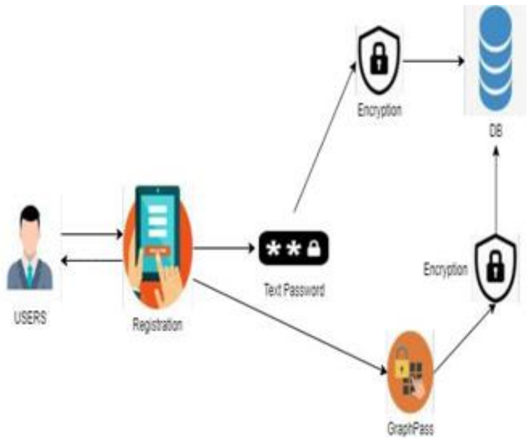
3. EXISTING SYSTEM

The secret key is the fundamental key to get approval however programmers are a lot of fruitful in secret phrase breaking because of the frail secret key chose by the client. To reinforce the secret key stockpiling, the proposed framework utilizes the Honey word procedure alongside Honey encryption. Honeywords are false passwords which are put away with unique secret word to draw the aggressor. The basic idea behind Honeyword is the insertion of false passwords. These are to lure the ttack. To generate the Honeyword of original password different techniques like Chaffing- with- tweaking, Chaffing-with- password model, etc. are available, but in the existing approach .

4. PROPOSED SYSTEM

A secure password authentication scheme is proposed which gives more security. This method uses a combination of pattern, key, and dummy digits. For this, the client needs to perceive and enlist design as area numbers from the network, register key qualities that guide esteem to secret password, and attach faker qualities to misguide the attacker. From that point forward to log in, the client needs to review the example and guides the secret key from design with enrolled key qualities, making a secret word by including sham digits. It minimizes shoulder surfing, brute-force attacks, cross site scripting etc. due to the high complexity of guessing passwords in multi-levels: first from the pattern, then from key, and then from dummy values.

5.SYSTEM ARCHITECTURE



System Architecture

On the border of the client, the user requests the registration. The Registration process includes two encryptions. One for text password, other for Graphical Password. Graph Pass was divided into 4 slices. Encryption takes place in each slice. The user-friendly graphical user interfaces make the task easier. Accordingly, the client doesn't have to think about the programming language and ideas.

The framework strictly follows the rules of Model view controller design (MVC architecture). MVC Architecture implies Model-View-Controller architecture, which is an example architecture plan for programming projects. As well as it needs a more grounded database that can hold a colossal measure of information, Here we utilize the SQL worker for storing all the client information. This is a web-based application that maintains a client-server architecture. Different devices will be connected on the client-side that communicates to the server with the help of the internet/cloud. When the client sends a request to the server, the server returns the corresponding data as the response.

Client-Server Architecture is a processing model in which the worker has, conveys, and oversees the greater part of the assets and administrations to be devoured by the customer. This type of architecture has at least one customer PCs associated with a server over an organization or web association. This framework shares figuring assets. Client/server design is otherwise called a systems administration processing model or customer/worker network since every one of the solicitations and administrations is conveyed over an organization.

6.RESULT

Image pixel based graphical password authentication In this project we are authenticating users via images and this images will be uploaded at signup time and then ask user to click on image 4 times to select 4 different spots and user has to remember those points. It’s difficult for user’s to select correct pixel X and Y location from mouse click so we provide region based authentication for example If user select X = 120 and Y = 240 from mouse click then while authentication I deducted 10 pixels from X value and added 10 more pixels to X values which means If user select X value between 110 to 130 and Y value between 230 and 250 then user get authenticated as actual or original X value 120 and Y value 240 falls between 110 to 130 and 230 to 250
To run project install python 3.7 and MYSQL and then copy content from DB.txt file and paste in MYSQL to create database
To implement this project we have designed following modules

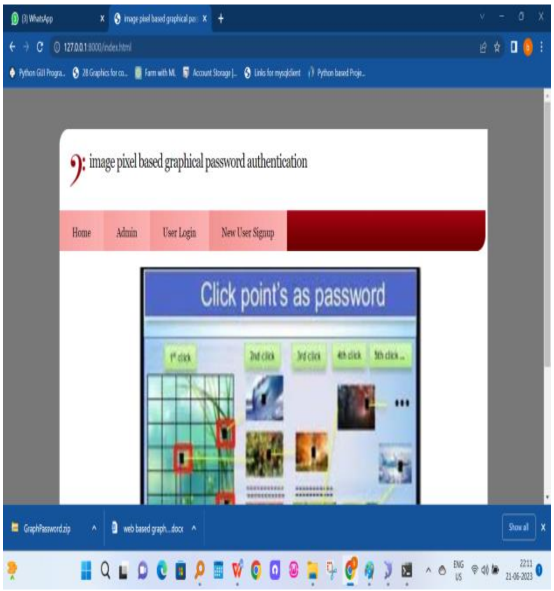
1) Admin Login: using this module admin can login to application using username and password as admin and then after

login can view all registered user details

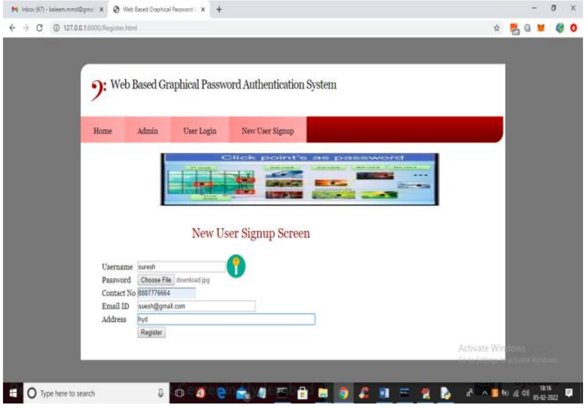
2) New User Signup: using this module user can signup with the application and has to upload image in place of password and then select 4 spots and all this details will saved in database
3) User Login: using this module user can login to application by entering USERNAME and then image will be displayed and user has to select correct spots to get authenticated
4) Reset Password: after login user can update password image and can enter new spots to reset password

SCREEN SHOTS

To run project double click on 'run.bat' file to start DJANGO server like below screen



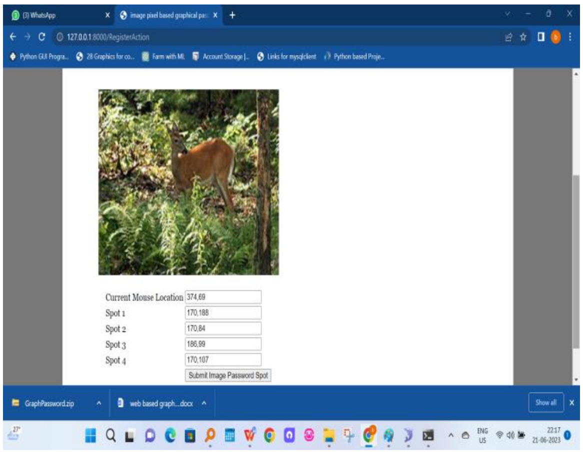
In above screen click on 'New User Signup' link to add new user details


Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password

New User Signup Screen

Username suresh
Password Choose File download.jpg
Contact No 8887776664
Email ID suesh@gmail.com
Address hyd

In above screen after entering all details click on 'Register' button to get below page with image



Current Mouse Location 374,69
Spot 1 170,188
Spot 2 170,84
Spot 3 186,99
Spot 4 170,107

In above screen I selected 4 spots and all those X and Y selected values are filled in the text fields and then press button to get below page

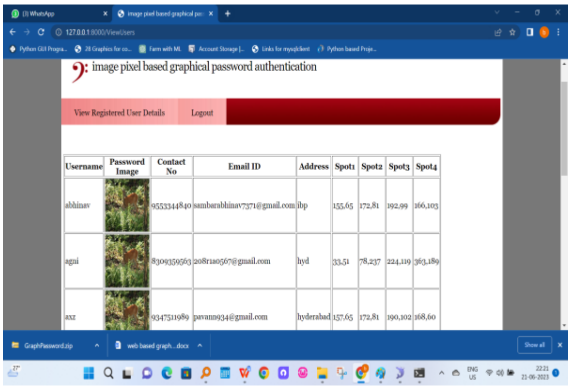


image pixel based graphical password authentication
View Registered User Details
Logout

Username	Password Image	Contact No	Email ID	Address	Spot1	Spot2	Spot3	Spot4
abhinav		9553344840	sambarabhinav7371@gmail.com	ibp	155,65	172,81	192,99	166,103
agni		8309359563	208r1a0567@gmail.com	hyd	33,51	78,237	224,119	363,189
axz		9347511989	pavann934@gmail.com	hyderabad	157,65	172,81	190,102	168,60

7.CONCLUSION

To protect users digital property, authentication is required every time they try toaccess their account and data. Conducting the authentication process in public might result in potential shoulder surfing attacks. Using traditional textual passwords or PIN method, users need totype their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over their shoulder or uses video recording devices such as cell phones. To overcome this problem, we proposed a shoulder surfing-resistant authentication system based on graphical passwords.

8.REFERENCES

[1] Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, User Define Time Based Change Pattern Dynamic Password AuthenticationScheme, 2018 14th InternationalConference on Electronics Computer

[2] Yang Jingbo, Shen Pingping, A secure strong password authentiction protocol, 2010 2nd International Conference on Software Technology and Engineering

[3] Hua Wang, Yao Guo, Xiangqun Chen, DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security, 2008 11th IEEE High Assurance Systems Engineering Symposium

[4] Salah Refish, PAC-RMPN: Password Authentication Code Based RMPN, 2018 International Conference on AdvancedScience and Engineering (ICOASE).

AUTHOR

Ms.Aarthi Kasthuri Assistant Professor,

Department of CSE,MallaReddy Engineering

College for Women,Hyderabad,

mrecwaarati27sep@gmail.com