Web based Graphical Password Authentication System

Abhijith S[1]
Student,
Dept. Of Computer ScienceMangalam College of Engineering, Kottayam, India

Soja Sam[2]
Student,
Dept. Of Computer ScienceMangalam College of Engineering, Kottayam, India

Sreelekshmi K U[3]
Student,
Dept. Of Computer ScienceMangalam College of Engineering, Kottayam, India

T T Samjeevan[4]
Student,
Dept. Of Computer Science Mangalam College of Engineering, Kottayam, India

Sneha Mathew[5]
Assistant professor,
Dept of Computer ScienceMangalam College of Engineering
Kottayam, India

***Abstract*—Authentication dependent on passwordsis utilized generally in applications for security and protection. Still, human actions, as anexample, choosing bad passwords and contributing passwords in square measuresare viewed as "the most fragile connection" in the Authentication chain. Maybe than discretionary alphanumeric strings, clients will pick passwords either short or significant for simple memorization. With web applications and versatile applications accumulation, individuals can get to these applications whenever and anyplace with various gadgets. This advancement brings extraordinary accommodation yet, in addition, builds the likelihood of presenting passwords to bear riding attacks. Attackers can notice straightforwardly or utilize outside recording gadgets to gather client's qualifications. To avoid this sort of issue, we need another method of confirmation. Here, we can choose a graphical authentication method. The image password offers the best approach to sign on that is simpler thanrecollecting and composing along with simple passwords. You can sign in by tapping the right points or creating the right gestures over an image that you just select in advance.**

Key Terms – Authentication, Graphical Passwords, Image Slicing, Encryption

I. INTRODUCTION

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. Shouldersurfing occurs when someone watches over yourshoulder 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.

II. LITERATURE REVIEW

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 client's 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 [1].

In the paper [2], a novel time-based unique password was contributed to avoiding challenges of using 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 thedynamic password and improves the usability of the system in terms of availability [2].

A strong password authentication scheme wasproposed by Yang Jingbooo. The one-time passwordauthentication 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 W.C Ku‟s 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 [3].

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 [4].

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 topropagate it to another user which he wants to be authenticated [5].

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 asarea numbers from the network, register key qualities that guide esteem to secret password, and attach fakerqualities 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 fromdummy values [6].

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 choseby the client. To reinforce the secret key stockpiling, the proposed framework utilizes the Honeyword 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 areto lure the attack. 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 [7].

III. PROPOSED SYSTEM

Here we develop a web-based application that uses graphical authentication. It uses two layers of security. 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 threemodules.

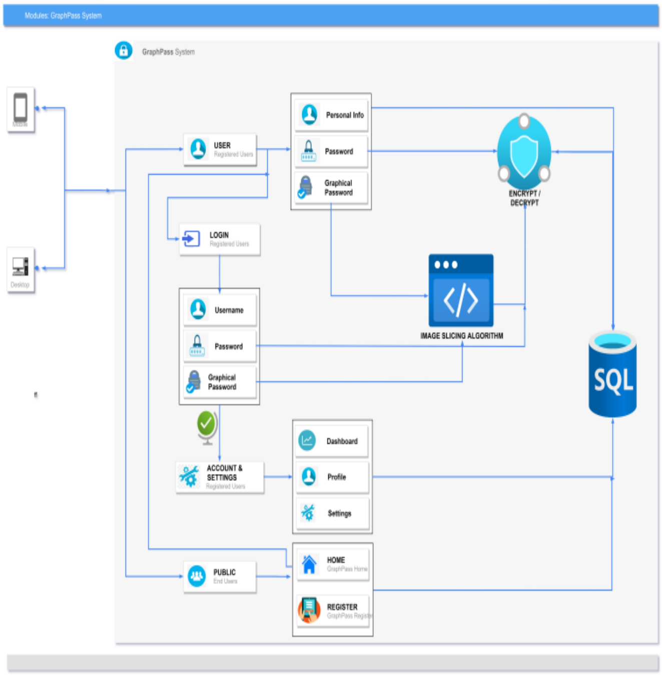


Fig. 1.Modules of Graphical Password System

A. *Public Module*

It is the overall viewing end of an individual website. Anyone with the URL can access this module. It is public however they can't change or alter the information.

B. *User Module*

The registered users are the part of user module. The user module consists of 2 functionalities - Registration and Login. During Registration, the system collects the basic details of the user like name, mobile and email, textual password, and graphical password. These all are encrypted and stored in the database. During the login phase, the user will give the username, textual password, and image password for accessing the resource. It compares the given values with dataalready given by the user at the registration phase. If it matched, then he/she will be logged into the page.

C. *Account and Settings*

This is the third module that contains the client's records and different settings of the computerized web stage. There is a link between the user module and the account module, If the user completes the registration, then the account will be created on the database. Also, the users can change their passwordsat any time. Sign-in data, privacy and security choices, and so on are a benefit of it. Furthermore,clients can get warnings and request support from this part.

IV. SYSTEM ARCHITECTURE

The architecture chooses how the framework should work. Request response time, page loading time, Ability to deal with the various requests, and so onare characterized by the design of the web application. In this manner, for better execution, it is indeed to utilize the best design. Here it utilizes the MVC architecture (Model-View-Control Architecture).

MVC Architecture implies Model-View-Controller architecture, which is an example architecture plan for programming projects.

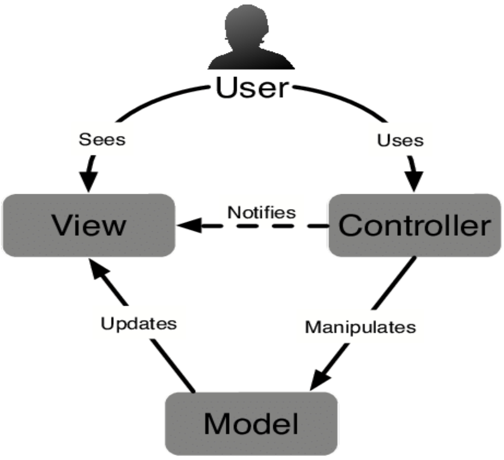


Fig. 2. MVC architecture

The design has 3 parts, they are Model, View, and Controller (Fig 3). These segments make the framework more adjustable.

The primary layer is the Model layer which deals with information and data set associations. The View layer is the viewing layer or result showing Layer in the MVC design. The Controller plays a mediator role among model and view parts, and the data flow is chosen by this segment.Along these lines, it takes information from the client and cycles it with Model segments, and gives it to the View segment.

A. *System Architecture*

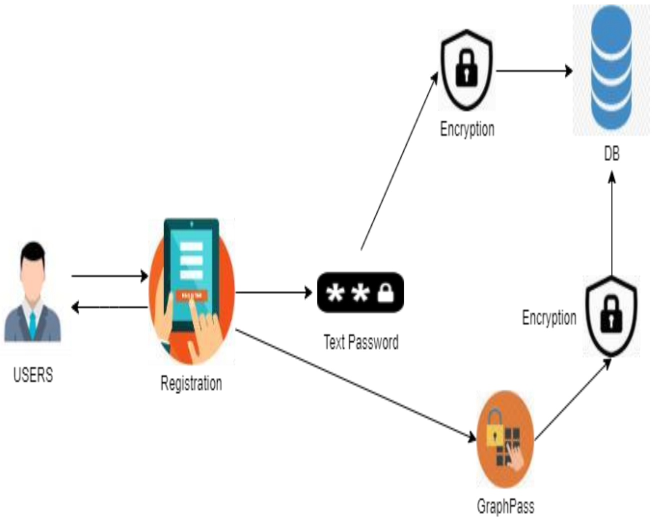


Fig. 3. System Architecture

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 clientsends 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. Thisframework shares figuring assets. Client/serverdesign 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.

B. *Framework Architecture*

On the side of client, we use a PHP framework called CodeIgniter. It is of the MVC architecture – Model View Control architecture. Database operations are managed in the model session.

Like database comparisons and validations takes place in the model session. The overall functions are performed in the control session.

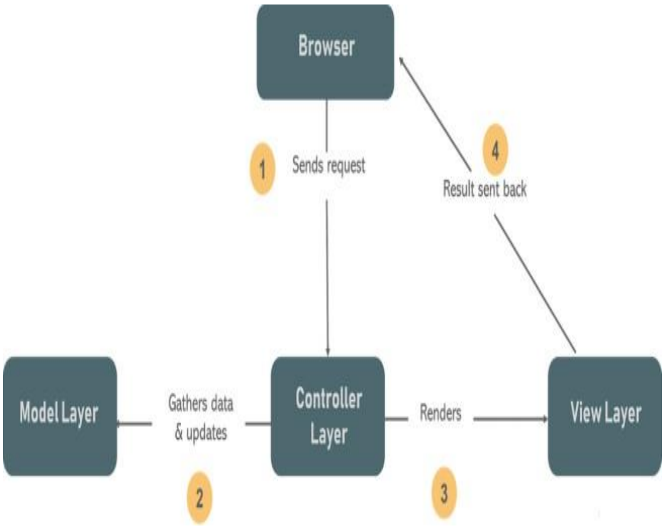


Fig. 4. Framework Architecture

V. IMPLEMENTATION

Tools used for the implementation are:

A. *Software tools*

The text editor used for this development is sublime text. Sublime Text is a shareware cross-platform source code editor with a Python application programming interface (API). It nativelysupports many programming languages and markuplanguages, and functions can be attached by users withplugins, typically community-built and maintained under free-software licenses.

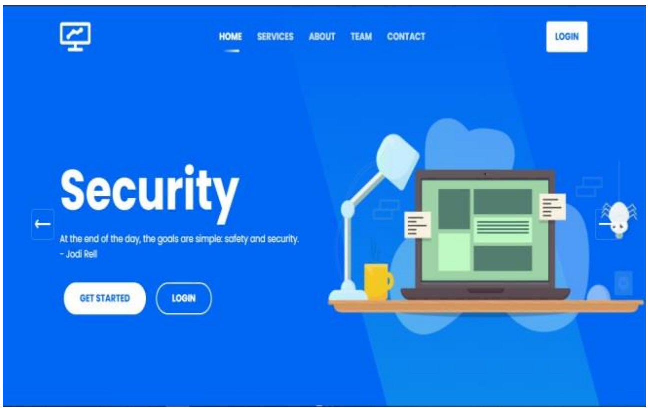
The server setup is done using XAMPP. XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl languages. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible.

SQL represents Structured Query Language, which is utilized to collaborate with databases. It may be utilized for storing, manipulating, and retrieving information in databases.

B. *Hardware tools*

Hardware requirements for this development are an i3+ processor, 4GB+ Ram, and 2GB+ SSD space.

VI. RESULT



Security

At the end of the day, the goals are simple: safety and security.
- Jodi Rell

Fig. 5. Home Page of Graphical PasswordAuthenticator

The above image shows how the graphicalpassword authenticator looks like. User can register an account from this home page and then can enter into his/her profile. The Registration section is secured with 2 layers of security. One is a textual password and another is a graphical one.

User can login to his/her profile by clicking the login button. The login page also includes 2 layers of security as mentioned above.

VII. CONCLUSION

To protect user's 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 overcomethis problem, we proposed a shoulder surfing-resistant authentication system based on graphical passwords.

VIII. ACKNOWLEDGEMENT

The authors wish to express gratitude toward Principal Dr. Manoj George, Dr. Vinod P Vijayan, H.O.D, Computer Science Department for the proper direction, significant help, andsupportive remarks during the editing.

IX. REFERENCES

[1] Wantong zheng, Chunfu Jia,'CombinedPWD: A New Password Authentication Mechanism Using SeparatorsBetween Keystrokes": 2017 13th International Conference on Computational Intelligence and Security (CIS)

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

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

[4] 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

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

[6] M Hamza Zaki, Adil Husain, M Sarosh 'Secure pattern-key based password authentication scheme'2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)

[7] Vasundhara R Pagar, Rohini G Pise, 'Strengthening password security through honeyword and Honey encryptiontechnique', 2017 International Conference on Trends in Electronics and Informatics (ICEI)

[8] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7..

[9] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479–483

[10] A. Bianchi, I. Oakley, and D.S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing System. CHI '10. New York, NY, USA: ACM, 2010, 1089–1092.

[11] E. von Zezschwitz,¬A. De Luca, and H. Hussmann, Honey, shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.