International Journal of
Electrical and Computer System Design
ISSN: 2582-8134 www.ijecsd.com

A Graphical Password Authentication in a Secure Storage System

Riasudheen H*[1], Selvamani K[2], Jayalakshmi S[3],

*[1]Teaching Fellow, DIST, CEG, Anna University, Chennai, India, riasudheen@gmail.com.

[2]Associate Professor, DCSE, CEG, Anna University, Chennai, India, selvamaniau@gmail.com.

[3]PG student, DIST, CEG, Anna University, Chennai, India,sjayalakshmi2019202018@gmail.com.

Abstract: In recent trends IT sector are concentrating more to develop a product that provides high-level security to the user. Information security is crucial for protecting all types of data from unauthorized access. So, authentication is an entry point for every hacker who is trying to hack the system and sniff the entire data from the product. To avoid unwanted user access to a system, a strong authentication mechanism is required. Authentication is classified into many types, but the most popular way to authenticate a system is done using the alpha-numerical. Traditional text based authentication is vulnerable to many attack like phishing and social engineering. If the password is too easy and obvious while using an alpha-numeric password authentication mechanism, there is a risk of being vulnerable so an innovative approach has been presented using images for passwords. To overcome the vulnerability in text-based authentication, the proposed method called graphical password authentication, which uses an image and the coordinate of the images can be set as password. This method of authentication is easy and more secure than the text based authentication because human brain is very effective while handling the image. In graphical password authentication is done simply by clicking and dragging on an image rather than memorizing the combination of alphanumeric values. So it can be the best alternative approach to the textual password for authentication into the secure storage system.

Keywords: Attack, Cyber, Graphical password, Authentication, Password Management.

1. Introduction

The process of recognizing a user's identity through authentication involves using several authentication technologies. The authentication procedure in a secured system verifies the data supplied by the user against the database [1]. The user is given access to the security system if the credentials match the data in the database. There are three common variables used for verification at the initial step of access control, known as validation: something you know, something you have, and something you are [2].

Most often, whatever you know requires users to provide their login and password in order to access the system. You have a situation where the user authenticates with a smart card. When obtaining access control, the user employs biometrics techniques based on what they are [1,2]. Users can access the system using any form of authentication technique, but each one functions differently.

Token-based authentication, biometric-based authentication, and knowledge-based authentication are the three categories used to categorize the authentication process [3]. Most web applications use knowledge-based authentication that requires a password of alphanumeric characters. There are two types of alphanumeric password authentication: weak passwords and strong password authentications. A dated, conventional, and common authentication mechanism is an alphanumeric password. This conventional approach is an unacceptably unsafe system. For instance, if a user is not using a strong password, an attacker may pick an easily guessable user's password. The same password can be used on several computers or websites by users [4].

When there are several networks and personal accounts in the ever-evolving world of today, some type of simple authentication schema must be offered [3,4]. So the proposed system is, a graphical password method for secure and easy authentication. One method for ensuring the security of digital devices or important information is the use of a graphic password. An alphanumeric password is less secure than a graphical password. The user can add more images to a page using this manner, and a password is chosen from among all of these selectable images. Because each case's images are unique, it would take a very long time for hackers to try matching every possible combination to discover the right password [5,7].

The majority of contemporary graphical password generators are vulnerable to shoulder surfing, a known security vulnerability where an attacker can steal a password by watching them directly or by capturing the

Proceeding of "Technology Integration for Sustainable Development: An International E-Conference on Electrical, Electronics, Computer Science and Mechanical Engineering. (EECM-2023)". Organized by SJUIT.

authentication process. The issue of shoulder-surfing with graphical passwords is made worse by the optical interface. Many solutions to this issue have been created, however they all have substantial usability flaws, most often in the time and effort required to log in, which makes them less suited for everyday authentication [6,12].

Major drawback of the graphical password authentication system is outweighed by Cued Click Point. Simply clicking five points from five photos, one point each image, constitutes CCP. The graphical password authentication system benefits from being expanded. Additionally, it develops the easiest method for users to utilize as well as a recognizable and remembered system [9]. With the aid of a clever GUI, cued click point makes it very easy for the user to remember and recognize the password. It stays away from the infamous hot spot issue with the previous graphical password authentication mechanism. We wanted to do rid of all the drawbacks associated with the older online authentication systems' techniques. It was absurd for a user to establish many passwords for various accounts and memorize them because text passwords have a thread to be cracked by hackers [8,9].

So, a straightforward method of making a straightforward graphical password that is simple to remember, understand, and hard for hackers to guess was offered [11]. We'll employ the Cued Click Point system in this system. The user can choose an image from the database or submit his or her own images in nearly any format for registration. The user must choose an image and give their email address upon registering. Click the image's points in accordance with the chosen image. The user ID and password must be entered while signing in, and this cued click point mechanism greatly secures them on the second level. [12,13].

Furthermore, a picture or image-based password is simple for the human brain to retain or recall. Therefore, this system includes graphical passwords for users who can register at random with pixel points, which are extremely safe and easy to remember [10]. This authentication controls customer security assurance at the data access point. It is a procedure that allows in a specific situation while requiring the client to. Images and the points in an image can be processed by the human brain with ease. The image base password is resistant to a dictionary attack, key-logger, social engineering, and shoulder surfing attack [14,15].

In this paper the idea is to create a system that can protect data which consists of encryption and decryption processes and to fully design a system securely. The goals of this research paper includes the following

- ✓ To implement graphical password authentication instead of alphanumerical passwords.
- ✓ To understand the pixel’s concepts in an image.
- ✓ To implement the logic for retrieving and displaying the image file which is stored in binary format.

The remainder section of this paper is structured as follows: the literature survey is presents about detailed methodologies used in various research works and their limitations in Section 2. Section 3 explain about the proposed methodologies of graphical password authentication. Section 4 describe out the real-time testing about the password authentications. Finally, section 5 describe about the conclusion and future enhancement in the research work.

2. Related Works

Shraddha M et al. [2] When presenting some of the ineffective graphical password techniques, such as the multiple image base password, which requires the user to choose one or more images from a set of photographs created a graphical password strategy. The following grid-based scheme is simple and doesn't require any additional displays. The following Triangle design is difficult to choose from because it has a protruding surface and almost the same number of images shown. The calculation of the username basis is the weakest part of this work. So, this innovative approach frequently offers solutions to the system's many problems [1,2].

The creation of a graphical password system fully integrated with various authentication systems was the main topic of discussion in Bhand et al [5]. Additionally, the primary goal of this strategy is to provide stronger security using a user-friendly method that is harder for hackers to decipher. Consequently, they create three different types of authentication methods. Pass point, Cued Click Point and Persuasive Cued Click Points.

Deshmukh et al. and Elham [3,4] discusses the security features of graphical authentication. Different graphical password schemes employ various defense mechanisms to lessen cyberattacks. As you are aware, graphical passwords are simple to remember and offer excellent benefits and high security. As a result, graphical password schemes have stricter security requirements than text-based ones. Shoulder surfing, brute force, dictionary, guessing, malware, and social engineering assaults are a few of the graphical password authentication attacks. This article discusses the risks associated with several graphical password schemes, followed by information about those schemes themselves and recommendations for further improvement [5,6].

An innovative method of graphical authentication that is robust to numerous attacks was employed by Waghmareb et al. [5]. They combined the two well-known varieties recognition-based and recall-based to develop a password that is immune to two phases of verification based on the conceptual assumption that a graphical password is more memorable than a textual password. Users should select a few photographs from a set of 25 images during the enrollment step as their initial authentication. After then, users are presented with three

questions to answer, and they must choose three points to Region of Answer (ROA) [7,8].

Users should choose the appropriate images for the first phase of authentication before choosing three regions from the already chosen images for the second phase. In the second step, the system's cued recalled-based strategy aids users in remembering things more quickly. In order to make it impossible for onlookers to memorize the relationship between questions and points, the system at this stage randomizes the question numbers in a three-digit format [9,10].

The two-step authentication methodology employs non-systematic in both processes to make it more difficult for onlookers, but it is not yet complete for those with keen eyes because the system would eventually become liable to them. Additionally, malicious software that aims to record mouse clicks and take screenshots puts this machine at danger. Users should try their best to remember the questions that are associated in the second phase. For instance, the number 123 denotes the questions' numbers in a different sequence every time, but the application of these numbers to the question list may be slightly disremembered. [11].

According to Aickelin et al. [12], the proposed technique has a number of benefits, including the fact that HOTSPOTS would be eliminated utilizing the viewport and shuffle button and that it will be challenging for attackers to guess the password thanks to a PCCP function for pattern formation assaults. By include the secret drawing feature in PCCP, attackers are made unaware that there is a secret drawing technique being used between these images. Even if they are aware of secret drawing, they are unable to determine precisely which image needs to be secret. Another benefit is that the message indicating whether a password is correct or wrong is only displayed after the final click; as a result, it will be challenging for attackers to determine which image to target [13].

Johnson et al. explain the various form of using the text password with the implementation of color. This proposed has a combination of set password with length of 8 and choose a color length of 8. His decoy colors are the remaining seven colors that the user did not select. Additionally, in order to reactivate his account after entering a bad password, the user must register an email address [14].

The registration process for this program ought to have taken place in a setting free from shoulder surfing. Additionally, a secure connection should be established using SSL/TLS or another secure transmission method between the system and the user during the registration process. The password table entry for each user contains their textual password, which the system saves and encrypts with the system key. In summary, during the registration process, the user enters a text password and chooses one color from a palette of eight [14,15].

3. Proposed Techniques

A graphical password authentication system follows a micro service architecture which is shortly called MVC architecture Figure1. A micro service is one of the architectural development styles that enables creating applications as a group of little autonomous services created for a business domain. Additionally, it aids in organizing applications as a group of loosely coupled services. The MVC design includes services with lightweight, fine-grained protocols. To develop a micro service system, all need a micro service-supported framework so we are using a spring-boot framework. The model view controller component of the spring framework, known as Spring Boot MVC, combines all the benefits of the MVC design with the spring boot simplicity. By using the servlet dispatcher, the front controller will be implemented by spring boot MVC with the pattern. The principal controller for routing the request to its final destination will be represented by the servlet dispatcher. The application data and view, which were distinguished by distinct engines of templates, are contained in the spring boot model. Spring Boot MVC can be used with several template engines. The components of this framework will be as follows:

Model:

- ✓ The object or set of objects that includes the application data is contained in the model.
- ✓ Model is a crucial element while creating applications.

View:

- ✓ The view component is used to display the user information, and this user information will be presented in a particular format.
- ✓ The spring boot will, as is well known, support a number of technologies, including velocity, thyme leaf, and free maker.
- ✓ By utilizing this component, we may display the specific user information.

Controller:

- ✓ This component will house the application's logical framework.
- ✓ We're using the controller annotation to identify our work class as a controller.

The secure storage system starts with the user authentication phase, for authentication two modules are designed the registration modules and login module in which the user can set their graphical password to secure their file. Once the user passed in an authentication phase then comes a dashboard.

In dashboard module there are three sub module profile, change password, add a file, view a file. profile module update or save the user personal information. Change password module are used to update their password. Then Add a file module helps

user to upload a list or single file into a storage system. Once the files are uploaded it can be displayed in view file module.

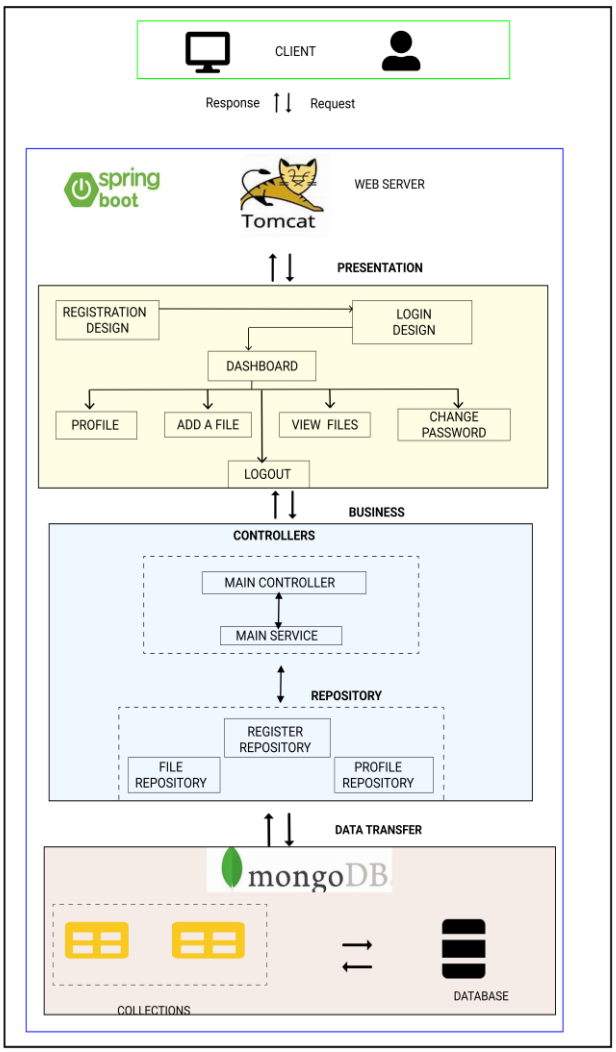

Fig 1. System Architecture.

In order to avoid people becoming mired down in complicated details too early, a system's graphical representation must only employ one process to represent the complete system and purposefully avoids specifying all the processes. Since a context diagram is a level 0 data flow diagram (DFD), explaining this is simple. This is the most fundamental form of DFD, in which each process and piece of storage is represented by a separate process. Figure 2 tells an overview of the authentication management system where the user gets verified that he/she can able to access and store the data in the database.

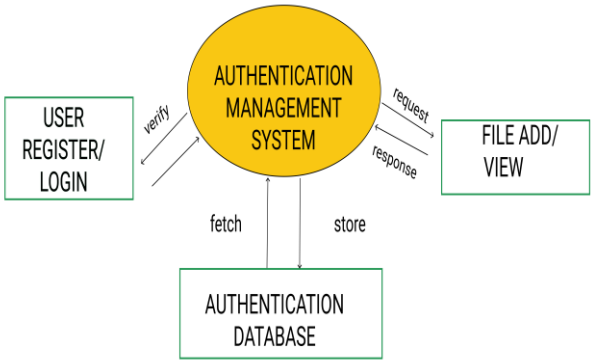

Fig 2. System context flow diagram.

Figure 3. the data-flow diagram for the authentication system elaborated on the high-level process of login and registration using graphical passwords. In addition to displaying the system as a single high-level process with its relationship to external username, password, and registration entities, it is intended to provide a quick overview of changing passwords.

3.1 Registration phase:

The registration phase is the most important phase in a graphical authentication system because it is the entry point of all the upcoming phases in a system. In this article, there are two alternatives offered to users who attempt to visit the home page: register and log in. You must select the register option if you haven't registered already. Steps to be followed during registration phase were mention in following points.

STEP 1: The register page will appear, the user has to provide an email-id, the provided email-id must be unique.
STEP 2: After the email-id is verified the user can select the image to set password
STEP 3: Image will be displayed in a canvas container.
STEP 4: Mark a point of interest within a canvas container
STEP 5: Pass the credentials into the collections.
STEP 6: Store collections in mongoDB.

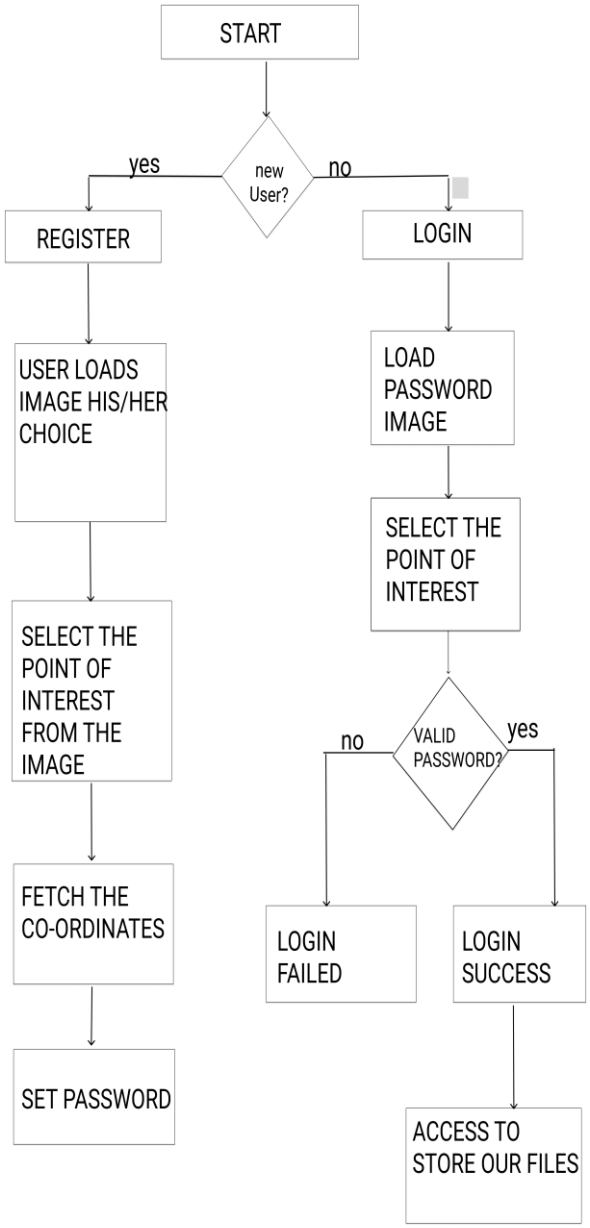

Fig 3. Data flow diagram.

3.2 Login phase:

This phase is also called as authentication phase where you have to prove to the system that you are a valid user to access the storage system. If you are an existing user of the system, then you can directly enter into the login phase from the homepage. Steps to be followed during Login phase were mention in following points.

STEP 1: Enter your email-id which is given at the time of registration

STEP 2: Image and number of points are displayed in canvas container.

STEP 3: Click on a same point which is given at the time of registration.

STEP 4: If the points match with the existing points authentication is successes.

3.3 Dash Board:

Once the user authentication is successful, Then the page redirect dashboard. The dashboard consists of four modules, they are as follows

- ✓ Profile: This module is used to keep track of user personal details. When the profile module is loaded it fetches the user's personal data from the database and displays it in a form. By clicking the update button user can update your personal details.
- ✓ Change Password: If user wish to change the existing password the change password module allows you to change the existing password and update the new password. It not only supports the image updating but also the number of the point of interest updating. By clicking the update password button user can easily update the new image and new point of interest values into a MongoDB collection the same register model is used to store the data because at the time of logging the user needs to log in with the updated password.
- ✓ Add file: In this module allows the user to upload a single file or a list of files in the mongo database through the set of collections. The main motive of this module is to enhance the file storage in the NoSQL-database
- ✓ View an update file: This module helps you to get the information about the files which is loaded into the database. The template displays the file id and files name list for each user separately.

4. Results and discussion

The real-time graphical password authentication system was implemented using the java 8.1 and Eclipse. In which the final result and output screenshot of graphical password authentication in a secure storage system is successfully implemented. This result screenshot gives us a real-time work experience on graphical password authentication to secure our files. The system flow starts from the homepage, the registration page, then the login page if the login is successful then goes to a dashboard page, or else it will

redirect to the homepage. It will not authenticate until the user gives the correct credentials

Algorithm 1: Graphical Password Management.

Input: Selecting the points in the image X & Y.

Output: Authenticated image password.

1. Start.
2. Fetch the file from file-input tag & store the file in a variable.
3. Declare a canvas type and assign the value to canvas type. // *convert the image file into canvas*
4. Fetch the X and Y coordinates from a user click.
5. Store the coordinates into the list data type along with the user unique id. //*storing the coordinates*.
6. Create a profile table with a same unique id and store the image in a binary format.
7. Fetch the X and Y coordinates from a user click and store the coordinates in a string pass it to controller. // *authentication*
8. Split the string and store it in list data type and fetch the existing list using the user's unique id.
9. Compare the list and return the authentication result.
10. Upload a file from local storage and pass the file into controller // *file storage*
11. Use a Mongo Template to store a file and Split the file into two parts fs. chunks and fs. File.
12. Send file storage request to File repository and Save the file into collation through Model Class.
13. END.

In the Above algorithm 1 discussed about the various features of graphical password authentication systems like image conversion, storing a coordinates, file storage and authentication.

4.1 Home page

The homepage consists of two buttons one for new users and another for existing users. If the new user has to be create the new profile for first time enrollment into the home page by selecting 'Registration' button and the existing user can login into the system by selecting the button 'Login' shown in figure 4.

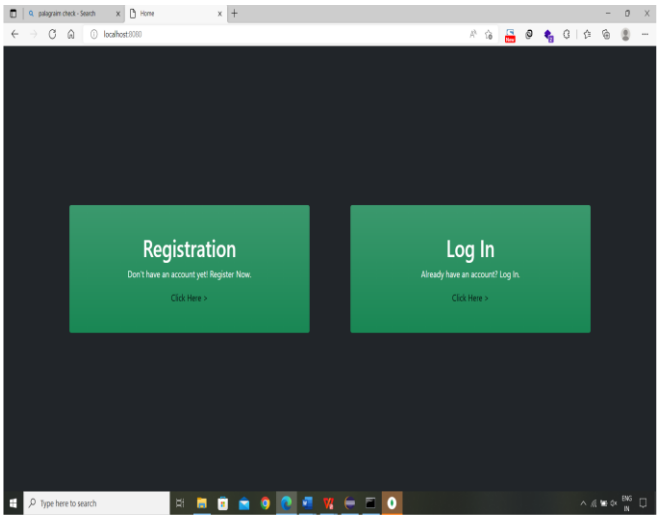

Fig 4. Home Page

4.2 Registration Page

To store the files securely first user needs to register in an authentication system. Once the user enters the user's valid email-id and they can select their image to set as password for authentication shown in figure 5.

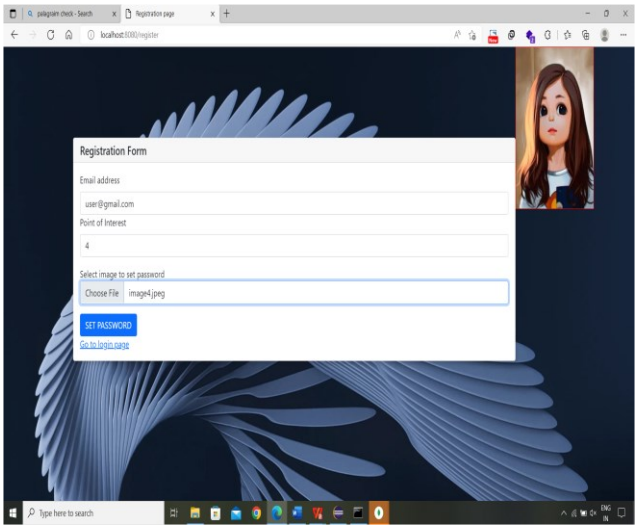

Fig 5. Registration Page

4.3 Password Selection:

The password selection was done by the user, by selecting the 4 various points in the image as per the user interest. There is no restriction to select the image its purely based on the user interest and easy to remembrance shown in figure 6. Additionally, if the user inputs a valid user email address, the system automatically gets the photographs and points that were saved during registration.

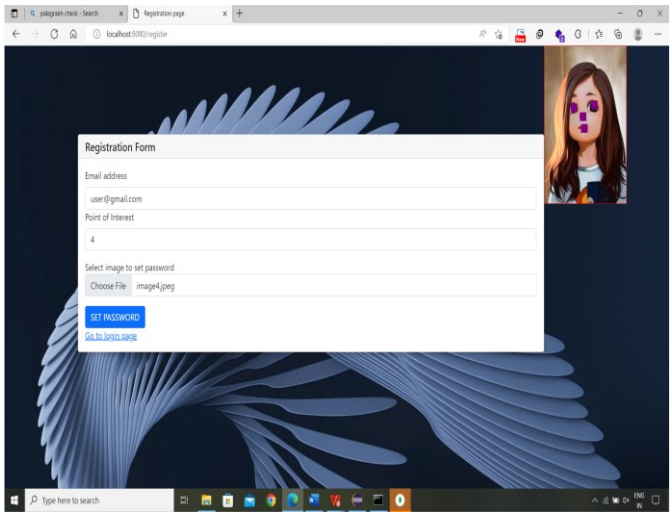

Fig 6. Click point of interest.

4.4 Dash Board:

In the dashboard, there are 4 components file upload, File view, profile, and change password. In the file upload component, multiple files can be uploaded at the same time. Once the files are uploaded the user can see the list of files with the file id in view file component. The user can also update his/her profile details in update profile component shown in figure 7.

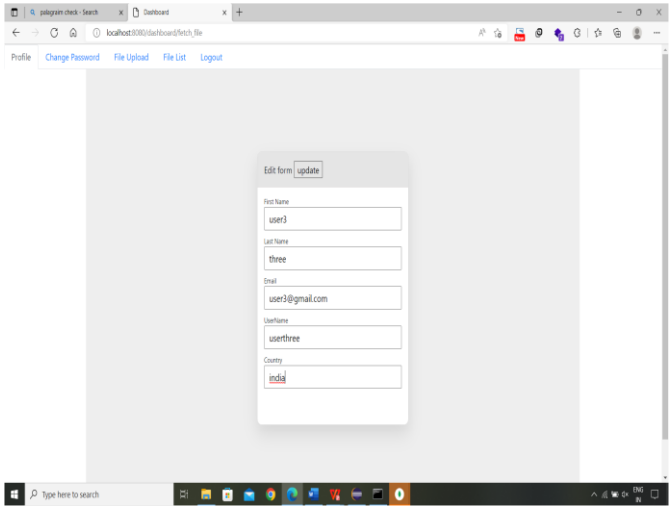

Fig. 7 Dash Board.

4.5 Changing Password:

If the user wishes to change the password, the system allows doing by using the change password component and also user can even change the number of points of interest and images simultaneously. Once the user submitted the password change it will be updated to the database was shown in figure 8 and 9.

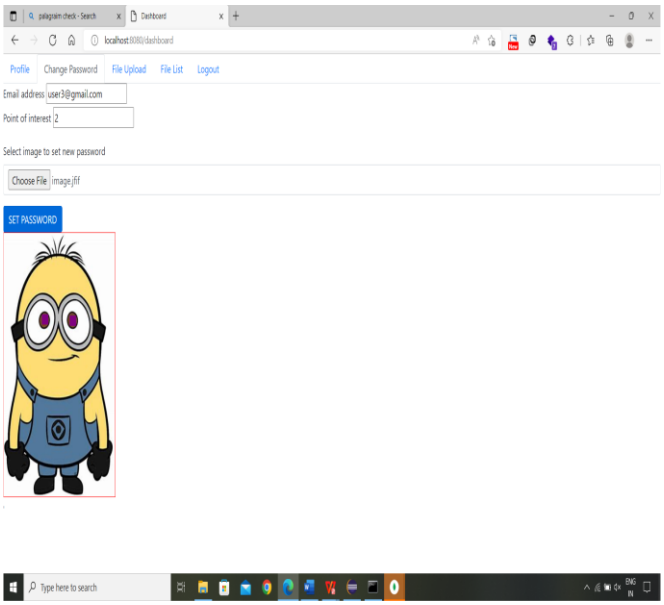

Fig 8. Change Password.

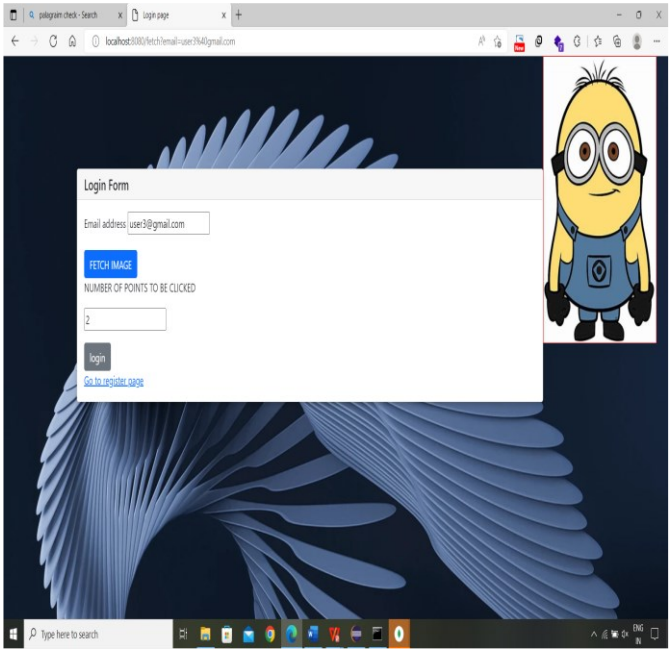

Fig 9. Update Password.

5. Conclusion and Future Work

Compared to conventional password authentication, graphical password authentication is more secure. Although graphical password authentication has its own drawbacks is not vulnerable to any the attacks like social engineering, or phishing. By implementing the clued clicked points method shoulder surfing attack can also be avoided. But graphical password techniques are still immature. Instead of alphanumerical authentication, all data management

systems must implement the graphical authentication. By implementing other special geometric configurations like different shaped images, and movable frames, one can achieve more security. Apply asymmetric cryptography methodologies to provide more security to data was an another way to future work.

Acknowledgement:
This research project was supported by Department of Information science and technology, CEG campus, Anna University, Chennai-25, We hole heartily thank for the opportunity and utilization provided by the department.

References:

1. Junaid Ahsenali Chaudry Robert G. Rittenhouse and Malrey Lee (2013). Security in Graphical Authentication. International Journal of Security and its Applications, Vol. 7, No. 3, pp. 347-356.
2. Leena S. Gawade Shraddha M. Gurav (2014). Graphical Password Authentication. International Journal of Engineering Research and Technology, Vol. 7, DOI: **10.1109/ICESC.2014.90.**
3. Prof. Awadesh Kumar, Mr. S. B. Deshmukh, Prof. S. K. Sonkar, Prof R. L. Paikrao. (2014) Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme. International Journal of Engineering Research Technology, Vol. 3, DOI: **10.1109/ISNE.2014.6512317.**
4. Elham Darbanian. (2015), A Graphical Password Against Spyware and Shoulder-surfing Attacks. International Symposium on Computer Science and Software Engineering, Vol. 8, DOI. 10.1109/CSICSSE.2015.7369239.
5. Amol Bhand. (2015) "Enhancement of Password Authentication System Using Graphical Images". International Journal of Computer Science, 55, Vol. 15, DOI. 10.1109/INFOP.2015.7489381.
6. Prof. Vijaya S.Waghmareb. Aakansha S. Gokhalea (2017), The Shoulder Surfing Resistant Graphical Password Authentication Technique. International Journal of Computer Science, pp. 490-498, DOI. 10.1016/j.procs.2016.03.063.
7. Sidra Malik Saneeha Amir Khazima Irfan, Agha Anas (2018), Text based Graphical Password System to Obscure Shoulder Surfing. 15th International Bhurban Conference on Applied Sciences and Technology, DOI. 10.1109/IBCAST.2018.8312258.
8. Azween Abdullah Teoh joo Fong (2019), A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices. International Journal of Advanced Computer Science and Applications, DOI. 10.14569/IJACSA.2019.0100140.
9. P. C. Golar and B. Khandelwal (2020), Study of Usability Parameter for Graphical Based Authentication System. 9th International Conference System Modelling and Advancement in Research Trends (SMART), DOI. 10.1109/SMART50582.2020.9337116.
10. R. K. Kushwaha H. Arora, G. K. Soni and P. Prasoo (2021), Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption. International Conference on Communication and Electronics Systems (ICCES), DOI. 10.1109/ICCES51350.2021.9488973.
11. R. Verma R. Pathak C. A. S. Murty, H. Rana and P. H. Rughani. (2021), A Review of Web Application Security Risks: Auditing and Assessment of the Dark Web. International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICEC), 2021, DOI. 10.1109/ICECCME52200.2021.9591031.
12. Uwe Aickelin. (2010), A New Graphical Password Scheme Resistant to Shoulder-Surfing. International Conference on Cyber worlds, 2010. DOI. 10.48550/arXiv.1306.2882.
13. K. Renaud. (2009), Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security, vol. 3, pp. 6085, 2009. DOI. 10.1504/IJICS.2009.026621.
14. G. Johnson and K. Renaud. (2009), Exploring the feasibility of graphical authentication systems, International Journal of Information and Computer Security, 2009. Vol. 63, pp. 128-152, DOI. 10.1016/J.IJHCS.2005.04.020.
15. A. Bhargav-Spantzel B.-L. Tai J.Cook K.-P. L. Vu, R. Proctor and E. Schultz. (2007), Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies vol. 65, pp. 744757, 2007. DOI. 10.1016/j.ijhcs.2007.03.007.

Authors Biography

H. Riasudheen is a Teaching fellow in the department of information science and technology, CEG campus, Anna university, Chennai-25.
Dr. K. Selvamani is working as an Associate Professor in Department of Computer Science & Engineering, CEG campus, Anna university, Chennai-25.
JAYALAKSHMI S is a PG student of Department of information science and technology, CEG Campus, Anna university, Chennai-25.