A

SEMINAR REPORT

ON

**GRAPHICAL PASSWPRD AUTHENTICATION.**

*Submitted in partial fulfillment of the requirements for the degree of*

**Bachelor of Technology**

In

**Information Technology**

*By*

Ramandeepkaur Banvat (2054491246044)

Sreepriya Kottilthara (2054491246055)

Vaishali Bhadhane (2054491246059)

Under the guidance

of

**Prof. Niteen Dhutraj**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

SHRI VILE PARLE KELAWANI MANDAL'S

**INSTITUTE OF TECHNOLOGY, DHULE**

Survey No. 499, Plot No. 02, Behind Gurudwara, Mumbai-Agra National Highway, Dhule- 424001, Maharashtra, India.

**Academic Year 2021-22**

SHRI VILE PARLE KELAWANI MANDAL'S

**INSTITUTE OF TECHNOLOGY, DHULE**

Survey No. 499, Plot No. 02, Behind Gurudwara, Mumbai-Agra National Highway, Dhule- 424001, Maharashtra, India.

**Academic Year 2021-22**

****

***CERTIFICATE***

This is to certify that the SY B.TECH. Mini Seminar Report Entitled

**“GRAPHICAL PASSWPRD AUTHENTICATION”**

Submitted by

Ramandeepkaur Banvat (2054491246044)

Sreepriya Kottilthara (2054491246055)

Vaishali Bhadhane (2054491246059)

is a record of bonafide work carried out by him/her, under our guidance, in partial fulfillment of the requirement for the award of Degree of Bachelors of Technology (Information Technology) at Shri Vile Parle Kelawani Mandal's Institute Of Technology, Dhule under the Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra. This work is done during semester IV of Academic year 2021-22.

Date:

Place: SVKM’s IOT, Dhule

Prof. Niteen Dhutraj Dr. Bhushan Chaudhari Dr. Nilesh Salunke

**(Seminar Guide) (Seminar Coordinator) (HOD) (Principal)**

Dept. of IT, SVKM-IOT Dept. of IT, SVKM-IOT Dept. of IT, SVKM-IOT SVKM-IOT, Dhule

Name and Sign with date Name and Sign with date Examiner-1 Examiner-2

**DECLARATION**

We declare that this written submission represents my ideas in our own words and where others ideas or words have been included, we have adequately cited and referenced the sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Signatures

Ramandeepkaur Banvat (2054491246044) \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sreepriya Kottilthara (2054491246055) \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vaishali Bhadhane (2054491246059) \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGMENTS**

### It gives us immense pleasure in expressing sincere sense of gratitude towards our seminar guide Prof. Niteen Dhutraj for the assistance, valuable guidance and co-operation in carrying out this Seminar successfully. It has been a privilege for us to have been associated with Dr. Bhushan Chaudhari, Head of Department, during our seminar work. We have greatly benefited from his valuable suggestions. We express our deep sense of gratitude to him for his valuable guidance, constant encouragement and patience throughout this work.

We are thankful to all people who have contributed in making this seminar success. Particularly, we want to thank Prof Niteen Dhutraj, Seminar Coordinator for our Department for making this process seamless for us and arranging everything so perfectly.

### We take this opportunity to express our heartfelt gratitude towards the Department of Information Technology of Shri Vile Parle Kelvani Mandal’s Institute of Technology, Dhule and Dr. Nilesh Salunkhe, Principle of Shri Vile Parle Kelvani Mandal’s Institute of Technology, Dhule, that gave us an opportunity for the presentation of our mini-seminar in the esteemed organization and for providing the required facilities in completing this seminar. We are greatly thankful to our parents, friends and other faculty members for their motivation, guidance and help whenever needed.

**Names of Team Members:**

1. Ramandeepkaur Banvat
2. Sreepriya Kottilthara
3. Vaishali Bhadane

**ABSTRACT**

**Abstract:** Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login the system. Remembering numerous passwords from various different sites can be difficult for a user. So to provide some flexibility we can provide users a graphical password authentication system where instead of creating a password a user has to select graphical objects in a particular order to keep it as their password.

**Keywords:** **Graphical password, secure, shuffled images, two step verification.**

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **EN** | **Entropy** |
| SMTP | Simple Mail Transfer Protocol. |
| HTML | Hypertext Markup Language. |
| CSS | Cascading Style Sheet |
| PHP | Hypertext Preprocessor |
| SQL | Structered Quere language |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig No.** | **Name of Figure** | **Page No** |
| 3.1.A | Architectural View | 5 |
| 3.1.B | Flow Charts | 11 |
| 4.1.1.A | Rough Model 1 | R |
| 4.1.1.A | Rough Model 2 | 17 |

**INDEX**

|  |  |  |
| --- | --- | --- |
|  | Certificate | II |
|  | Declaration | III |
|  | Acknowlegement | IV |
|  | Abstract | V |
|  | List of Abbreviations | VI |
|  | List of Figures | VII |

|  |  |  |  |
| --- | --- | --- | --- |
| **Chapter No** |  | **Chapter Name** | **PAGE NO.** |
| **1** |  | **Introduction** | 10 |
| 1.1 | Introduction of Seminar | 10 |
| 1.2 | Motivation Of Seminar | 10 |
| 1.3 | Problem Statement and Objective | 10 |
| 1.4 | Scope | 10 |
| **2** |  | **Literature Survey** |  |
| 2.1 | Survey Existing system | 11 |
|  |  |  |
| **3** |  | **Proposed System** |  |
| 3.1 | Analysis/ Framework/ Algorithm / UML diagrams | 11 |
| 3.3 | Methodology (your approach to solve the problem) | 13 |
| **4** |  | **Expereimentation and Results** |  |
| 4.1 | Block by block representation with explanation | 14 |
|  | 4.2 | Advantages and Disadvantages. | 17 |
| **5** |  | **Conclusion and Future Scope** |  |
| 5.1 | Conclusion | 18 |
| 5.2 | Future Scope | 18 |
| 5.3 | Limitation Of seminar |  |
| 6 |  | **References** (must be as per the IEEE citation rules) | 19 |

1. **Introduction :**
   1. **Introduction of seminar :**

Passwords are ubiquitous today on any platform, on possibly any website.​But to remember so difficult passwords and that too on numerous websites seems daunting and therefore you can devise a project illustrating graphical password strategy.​This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login the system**.​** As the name suggests, it uses different types of shapes and images as password. In addition, scientist is saying that it’s easy to remembered a picture for human brain than text. The human brain can easily process images. And image base password, it is resistant of dictionary attack, keylogger, social engineering etc. Alphanumeric password is an old traditional common authentication method. Practically this traditional method is too unsecure system. For example, attacker may choose easily guessed user’s password, if user is not using a strong password. User may use same password for multiple device or site. This are all unsecure characteristic for normal users. And authentication is one of the important security points where user has active responsibility for their personal information security.

* 1. **Motivation of Seminar :**

Graphical passwords (GP) use pictures (Parkinson, 2005) instead of texts and are partially motivated by the fact that humans can remember pictures more easily than a string of characters. ​An important advantage of GP is that they are easier to remember than textual passwords.​Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. An important advantage of Graphical Passwords is that they are easier to remember compared to textual passwords.​Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security.

* 1. **Problem Statement and objective :**

Graphical passwords introduce us to a whole new form of authentication. The most common form of authentication used today is the used of alphanumeric texts and this form of authentication has been proven to be prone to several forms of attacks such as guessing, social engineering, spywares, dictionary attacks, shoulder surfing and even hidden cameras. it is easier to remember pictures than text, graphical passwords tend to enhance security and at the same time make it easier for the user to use.

* 1. **Scope :**

Graphical password is one of process for authentication in computer system. computer security is create a safe zone for our digital devices. Graphical password is a one of the processes to provide our security of digital device or important information. As we know that our human brain can easily store or recall an image or image-based password. It can be used anywhere instead of text-based passwords. You can increase the security of this system by increasing the number of levels used and the number of squared tolerances used. There are many authentication systems that exist today, but they have their pros and cons**.**

1. **Literature Survey :**

* Shraddha M, Leena S. Gawade, and Prathamey K. Rane's "Graphical Password Authentication." They came up with a graphical password strategy where they showed off some of the ineffective techniques, such as the multiple-image base password, which requires the user to choose one or more images from a set of photographs that can be displayed to them. The next grid base scheme is simple and doesn't call for any additional displays. Next Triangle design is difficult to choose from since it has protruding surfaces and nearly identical quantities of images. The most useless part of this essay is the calculation of username basis. So, this innovative plan frequently offers solutions to the system's many problems.
* By Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, and Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing." In this study, the security aspects of graphical authentication are discussed. Different graphical password schemes employ various defence mechanisms to lessen cyberattacks. As you are aware, graphical passwords are easy to remember, highly functional, and highly secure. The security of graphical password schemes is therefore higher than that of text-based passwords. Shoulder surfing, brute force, dictionary attacks, guessing assaults, spyware, and social engineering attacks are some of the defences against graphical password authentication threats. They provide a brief summary and classification of several graphical password schemes in this study, along with details on their flaws and recommendations for further research.

1. **Proposed System :**
   1. **Algorithm :**

1.Start

2.Login page. If yes' goto next step (step3) if no go to step A.1.

3.Enter username and

4.Successfully Logged in go to step 6.

5. If Forget Password go to step B.1

6.Home page

7.End

A1.Signup page

A2.1.Name 2.Email ID 3.Set pass button

A3.Confirm password.If yes goto step A4 else (no)goto step A2.

A4.Successfull Login

A5.Home Page

A6.End

B1.Signup page 2

B2.Enter E-mail Id

B3.Goto step A.1

B4.Password check

B5.Old password cannot be set as new password

B6.Go to step B.4

B7.Home page.

|  |  |
| --- | --- |
| **3.2** | **Details of Hardware &Software** |

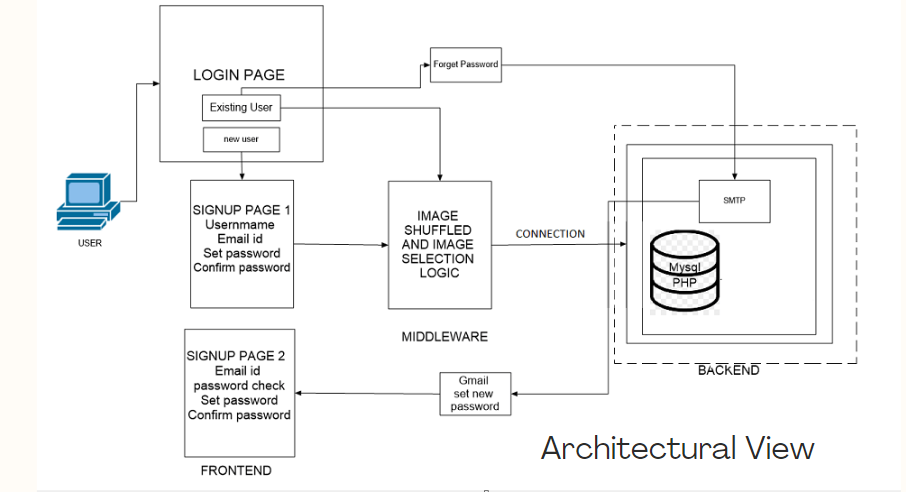


Fig 3.2.A

The above figure shows the architectural view of the proposed system:

* 1. **Flow Charts :**

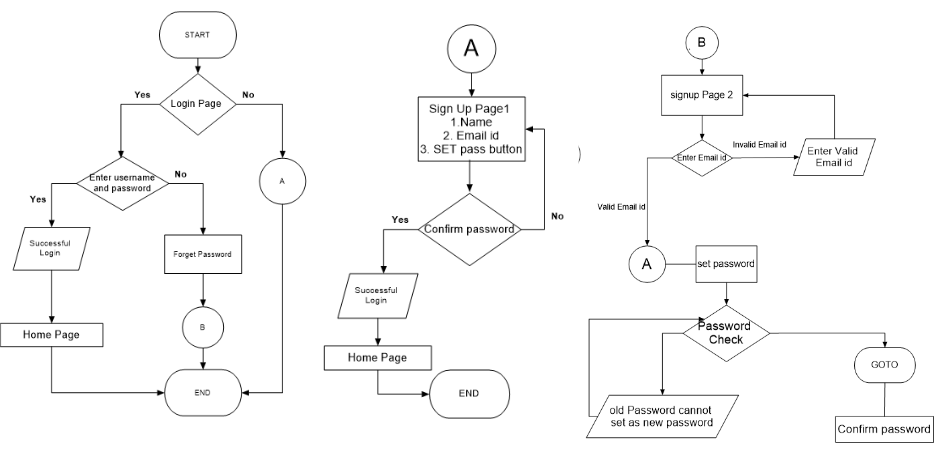


Fig 3.1.B

* 1. **Methodology :**

Sign-in page will contain Sign Up for new Users and log in for existing ones. ​After the successfull sign up when user tries to login, firstly the email will be verified by checking if that email is present in the database if yes then it will check if the given password matches with the password in the database.​

For setting the password the user needs to select any 5 image from the panel. While selecting this images, reshuffling of images takes place. The user has to remember the sequence of selection of images which he or she had selected as their password​ On the Sign In page, the user will be asked to enter their email id and password if they are an existing user, then if the user enters the right email that was already registered before then the entered password will be verified with the password in the database. if it matches the user will be redirected to the webpage.​Forget password will be available to the existing users is available in login form then user need to enter their mail and if the user exists in the data base they will get an email with a link to reset their password, here we will use the SMTP to send the automated email to the user's mail.

1. **Experimentation and Results :**

**4.1.1 Rough Model**

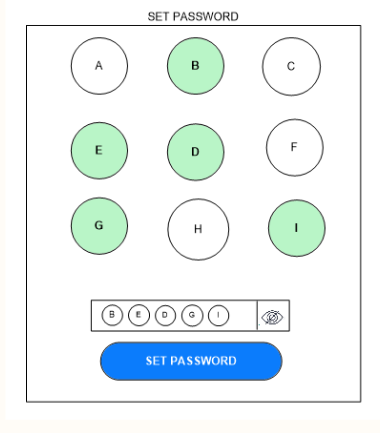


Fig 4.1.1.A

On this page there would be a image grid of 3\*3 containing 9 different images (Displayed as ABCDEFGI in the model)

We allow the user to set a password by choosing a series of 5 images in a desired order.

The user can see the images he/she has choosen by clicking on the show password button.

Once the password is set a new page appears asking a confirmation on the previously entered password.

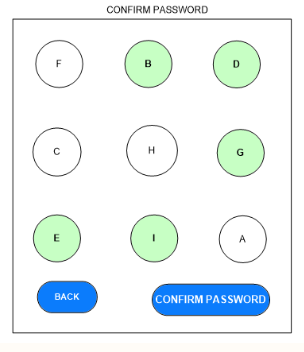


Fig. 4.1.1.B

Confirm Password:

In this page we can see that all the nine images have now been shuffled and the user needs to tap on the same series of images they selected before in the proper order and thus confirm their password. If the user wants to re-enter the password before confirming they can click on the back button and select the images they want.

**1. Sign-in page will contain Sign Up for new Users and log in for existing ones.**

For the front End part we will be using HTML, CSS and Javascript.Users will be asked to enter their Mail-ID and they will be given an option to set their password.The data which we get from the user is stored in database with the help of SQL Queries and we will make use of PHP script to fetch information from the form.The Language used will be PHP & we will use MySQL Database for storing the user data

**2. When a new User makes an entry after sign up the details will be written in the database. After the successfull sign up when user tries to login, firstly the email will be verified by checking if that email is present in the database if yes then it will check if the given password matches with the password in the database.**

LONGBLOB data type is used in database to store selected images from userRetrieve the content of image file by the tmp\_name using PHP file\_get\_contents() function.Insert the binary content of the image in the database using PHP and MySQL.

**3. For setting the password the user needs to select any 5 image from the panel. While selecting this images, reshuffling of images takes place. The user has to remember the sequence of selection of images which he or she had selected as their password.**

We will create a container in which we will place the shuffled images. Then we will create a toggle element to re-perform/reset the shuffle animation.

a. Container is where image are stored in order.

b. Shuffled() method will help us to shuffle images in random order.

c. The data which we get from the user is stored in database with the help of SQL Queeries and we will make use of PHP script to fetch information from the form.

**4. On the Sign In page, the user will be asked to enter their email id and password if they are an existing user, then if the user enters the right email that was already registered before then the entered password will be verified with the password in the database. if it matches the user will be redirected to the webpage**

After storing database fetch help to get username with following condition for image password

var thumbnail = document.images.thmb;

if(thumnail.src)

{ if(thumbnail.onerror)

{ thumbnail.src = "http://blog.lefigaro.fr/bd/img-sanctuaire.png"; }

else

{thumbnail.style.display = "invalid password"; }

**5. Forget password will be available to the existing users is available in login form then user need to enter their mail and if the user exists in the database they will get an email with a link to reset their password, here we will use the SMTP to send the automated email to the user's mail.**

We will make use SMTP (Simple Mail Transfer Protocol) for forget password where user need to enter his/her Register email id to get link of forget passowrd reset

**6. How and when will the page display successful login:**

We will apply the fetch () method and check whether the conditional statement is satisfied with respect to our database record.

If the conditional statements are satisfied then the home page is displayed otherwise it displays an error message and asks the user to go through the process once again.

* 1. **Advantages and Disadvantages :**

Advantages of graphical authentication method:

• The security of the system is very high.

• Graphical password schemes provide a way of making more human-friendly passwords.

• Dictionary attacks and brute force search are infeasible.

Disadvantages of graphical authentication method:

• Require much more storage space than text based passwords.

• Password registration and log-in process take too long.

• Shoulder Surfing: As the name implies, shoulder surfing is watching over people’s shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing

1. **Conclusion and Future Scope :**

Digital devices have become part of our daily lives. Using digital devices, we learn about authentication

process. Validation is an important part of security. Authentication will provide greater security to the customer. Special review articlesresearch in the same area regarding specific attacks discovered during validation. Authentication of the press secret term is very goodtesting device. This is useful and more secure compared to the previous old basic graphical password authentication systems.

One conclusion is drawn that the memorability and security of graphical password are better than that of text-based password. In addition, it's shown that the graphical password scheme has better resistance to major password attacks than others.SinceThe password space is very large, offering security against brute force attacks. It is easy to use. Passwords are easy to create andremember. Randomization of two authentication systems provides strong security against shoulder surfing. Do wellsystem, you need high security and good usability, and this is inseparable. The shoulder navigation attack is subject to safetyprotection. However, proposed methods for the shoulder surfing problem have yet to be developed.This system can also be used to add a higher level of security to a text password system. This system is very cheap compared to a biometric system

**References**

1. T. Y., Yang, P., Shamala, M., Chinniah, and C. F. M., Foozy. “Graphical Password Authentication For Child Personal Storage Application.” In Journal of Physics: Conference Series ,Vol. 1793, No. 1, pp. 012065. IOP Publishing , February , 2021. ​

2. G. K., Jiya, I. O., Oyefolahan, and J. O., Ojeniyi, “Recognition Based Graphical Password Algorithms: A Survey”. 2020 IEEE 2nd International Conference on Cyberspac.​

3. S., Patel, A., Jaiswal, Y., Arora, and B., Sharma, “Survey on Graphical Password Authentication System”. Data Intelligence and Cognitive Informatics, pp. 699-708, 2021.​

4. Prof. K. R. Ingole Paper Id : IJRASET40969 Publish Date : 2022-03-24​

ISSN : 2321-9653 Publisher Name : IJRASET

​

5. Graphical Password Authentication. ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE

6. A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham,

NG8 1BB, U.K