VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Winter Semester- 2021-22

MTech (Software Engineering)

CSE3502-INFORMATION SECURITY MANAGEMENT

FACULTY: GANESAN K

Project Title:

Three level password authentication and person verification for E- services portal

J. Tharaka

18MIS0292

Problem Statement:

Background study:

The project is an authentication system that validates user for accessing the system only when they have input correct password. The project involves three levels of user authentication. There are varieties of password systems available, many of which have failed due to bot attacks while few have sustained it but to a limit. In short, almost all the passwords available today can be broken to a limit. Hence this project is aimed to achieve the highest security in authenticating users.

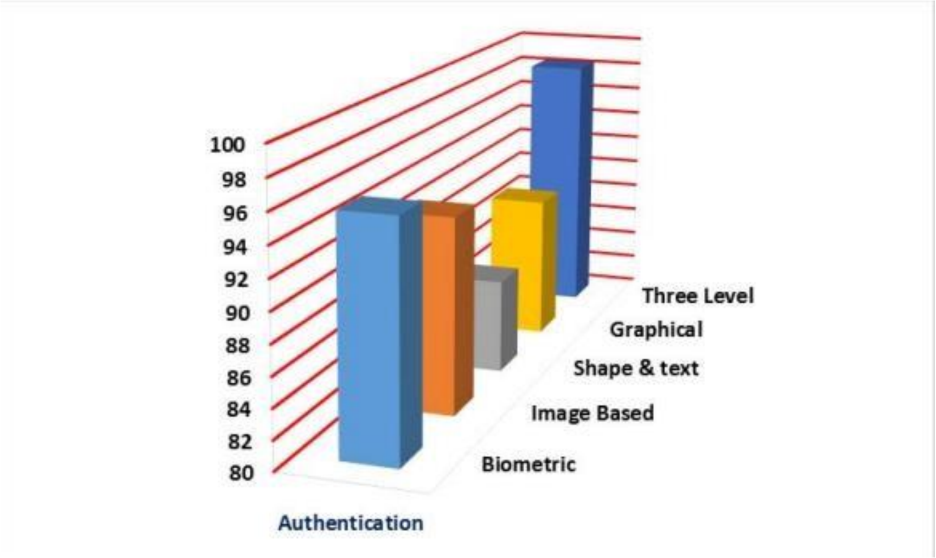


Fig1. Comparison of Authentication Systems

Problem Statement:

Our project aim is to have three different kinds of password system. The password difficulty increases with each level. Users have to input correct password for successful login. Users would be given privilege to set passwords according to their wish. The project comprises of text password i.e. pass phrase, image -based segmentation password and graphical password for the three levels respectively. This way there would be negligible chances of bot or anyone to crack passwords even if they have cracked the first level or second level, it would be impossible to crack the third one. Hence while creating the technology the emphasis was put on the use of innovative and nontraditional methods. Many users find the most widespread text-based password systems unfriendly, so in the case of three level password we tried creating a simple user interface and providing users with the best possible comfort in solving password.

Novelty:

In earlier proposed methods they have used picture based authentication as one factor of authentication. In those methods user have to choose the pre-defined images given in the site or app and should choose the pattern among them. But this may be easily cracked by using brute force attacks and shoulder surfing attacks. So in our proposed system we have given privilege to user to choose the picture from his system and he/she needs to choose pattern from the split parts of the picture he/she uploaded from the system. By this methods we can somewhat reduce brute force attacks since the attacker don't know the picture user has chosen.

Dataset:

Not applicable for our project

Related Works:

Literature Survey:

RESEARCH PAPERS	METHODS USED	ADVANTAGES	ISSUES
1.A Novel Graphical Password Authentication Mechanism [1]	This authentication mechanism involves alphanumeric passwords, images as passwords, CATCHA and also a random number generator for security purposes.	As human beings have the ability to remember pictures easily, this method will make the authentication process much easier to an extent.	A major drawback of using alpha numeric password is the dictionary attack
2.Multi-Level Authentication System [2]	The project comprises a Login and Registration form with AES	The system is userfriendly and has simple interface.	The only disadvantage is if users forget the

	Encryption and Decryption where the user id and password will be encrypted.		password, it cannot retrieve it.
3. Strong password authentication protocols [3]	The SPAS is resistant to Dos attacks, replay attacks and stolen-verifier attacks.	It expects SPAS can be employed in application scenarios where lightweight and secure user authentication scheme is required.	Existing password authentication scheme can be categorized into two types: weakpassword authentication schemes
4. THREE – LEVEL PASSWORD AUTHENTICATIO N [4]	Techniques used include token based, biometric based as well as knowledge based. Despite these, no single mechanism is efficient and effective to provide adequate security	The proposed system in this paper would provide more secure authentication technique than existing one, overcome the drawbacks	Limitations of previously existing systems (such as textual password, graphical password. etc) and combine more than one authentication techniques.
5. Password- based Authentication in Computer Security: Why is it still there? [5]	Exploring the flaws of the dominating usernamepassword security measure, and focusing on the alternative authentication and authorization techniques	Password-based authentication has several applications and it is deployed in cloud computing but it will face numerous drawbacks	Limitations when it is considered for Fog computing: -It takes an extensive computation to process.
6. THREE LEVEL PASSWORD AUTHENTICATIO N [6]	The project comprises of text password i.e. passphrase, image based password and graphical	This way there would be negligible chances of bot or anyone to crack passwords even if they	The only disadvantage isif users forget the password, it cannot retrieve it.

	password for the three levels respectively	have cracked the first level or second level	
7. Two Way Authentication Scheme for Mobile Applications and Web Application [7]	The Inherent Based Authentication category, Token Based Authentication, Knowledge Based Authentication	A user authentication protocol that involves user's telephone and short message service to stop counter sign stealing and utilize attacks.	True textual authentication which uses a surname and password has inherent weaknesses and drawbacks
8. Three Level Password authentication System [8]	The project comprises of text password i.e. pass phrase, image based segmentation password and graphical password for the three levels respectively.	Users can set or upload their own images. Protects systems vulnerable to attacks	The only disadvantage is. if users forget password, he cannot retrieve it
9. Password insecure communication [9]	The method assumes a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal.	The system is userfriendly and has simple interface. Provides strong security against bot attacks or hackers	A major drawback of using alpha numeric password is the dictionary attack
10. Secured authentication stealing and utilize extensive Function	This research significantly enhances security level in password-based authentication using anonymity features and PBKDF2 to	A user authentication protocol that involves user's telephone and short message service to stop counter sign stealing and utilize attacks.	Limitations when it is considered for Fog computing: -It takes an extensive computation to process.

	preserve user’s privacy and to resist from any attack vulnerabilities.		
11. Three Level Authentication for Student Attendance Management System	This paper involves three levels of the user authentication. This paper comprises of RFID system, Biometric system, and password -based system	The system developed is user friendly and has simple interface. It provides strong security for the data.	Hardware components required are NI MYRIO, RFID readers and tags, finger print sensor, USB port, and male to female pin connectors-cost.
12.Secure Authentication With 3D Password For Data Transmission	3d password scheme is a new strategy recognition patterns, textual passwords, biometrics and graphical passwords	The 3D password is very user-friendly, and very interesting way of authentication process	Token base authentication there is possibility of fraud, loss, and theft.
13. Efficient and Secure Authenticated Key Exchange Using Weak Passwords	We propose a 3- round protocol for password-only authenticated key exchange, and provide a rigorous proof of security for our protocol based on the decisional DiffieHellman assumption	A user authentication protocol that involves user's telephone and short message service to stop counter sign stealing and utilize attacks.	Human users cannot remember or securely store long, high-entropy keys.
14. (Password) Authenticated Key Establishment: From 2-Party To Group	A protocol compiler is described, that transforms any provably secure authenticated 2- party key establishment into a	Users can set or upload their own images. Protects systems vulnerable to attacks	A major drawback of using alpha numeric password is the dictionary attack

	provably secure authenticated group key establishment with 2 more rounds of communication.		
15.Dual-work factor Encrypted Key Exchange: Efficiently Preventing Password Chaining and Dictionary Attacks	This paper presents an extension of their ideas called /dual-work factor encrypted key exchange/ that preserves EKE's strength against dictionary attacks	It is provides security. Implementation of the system is easy.	A lot of program coding requirement.

2.2 Comparative study:

S.No	Research paper	Author	Limitations
1	three – level password authentication	GS Mishra,PK Mishra	Limitations of previously existing systems (such as textual password, graphical password. etc) and combine more thanone authentication

S.No	Research paper	Author	Limitations
2	Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication	Surabhi Anand, Priya Jain	The effort has been made to prevent Shoulder Attack, Storm Attack, and Brute-force attacks on the client side, using a unique image set in the IBA Program was not clearly mentioned.
3	Key Exchange Using Weak Passwords	Jonathan Katz	Human users cannot remember or securely store long, high- entropy keys.
4	Text and Image: A new hybrid authentication Scheme	AA abdulhmalem ,Arifin	This research shows weaknesses related to shoulder surfing attack against textual password, the existing of the other graphical password as the next stage Authentication is more than enough to prevent the an authorized accessing
5	TwoWay Authentication Scheme for Mobile Applications and Web Application [7]	P subhadra,MGA Anasazi	True textual authentication which uses a surname and password has inherent weaknesses and drawbacks

S.No	**Research paper**	**Author**	**Limitations**
6	THREE STAGE GRAPHICAL PASSWORD AUTHENTICATION SCHEME	S RajaRan ,M Prabhu	There is a difficulty with schemes that involve selection of points on images. Users face difficulty with remembering and precisely clicking on the click points. The usual strategy for this issue is to allow a tolerance range so that users may even click on points that are slightly away from the actual positions but are within the tolerance range. But it is still troublesome to the users
7	Cryptanalysis of Threshold Password Authentication Against Guessing Attacks in Ad Hoc Networks	Chun-Ta Li, Min-Shiang Hwang,Yen-Ping Chu	This research paper consists of threshold password authentication scheme to address the issues like passive attack

S.No	Research paper	Author	Limitations
8	Graphics password authentication system	Ahmed Almulhem	There is a difficulty with schemes that involve selection of points on images. Users face difficulty with remembering and precisely clicking on the click points. The usual strategy for this issue is to allow a tolerance range so that users may even click on points that are slightly away from the actual positions but are within the tolerance range
9	A remote password authentication scheme for multiserver architecture using neural networks	Li Hua Li,Luon-Chang Lin	As It is a remote password it can be easily hacked by others.

S.No	Research paper	Author	Limitations
10	Enhancement of password authentication system using graphical images	Amol Brand,vibhav Desale	There is a difficulty with schemes that involve selection of points on images. Users face difficulty with remembering and precisely clicking on the click points. The usual strategy for this issue is to allow a tolerance range so that users may even click on points that are slightly away from the actual positions but are within the tolerance range

Hardware Requirements:

- Processor – i3
- Hard Disk – 5 GB
- Memory – 1GB RAM

Software Requirements:

- Sublime Text Editor
- Xamp
- OS-windows 7 and above

System Design:

High level design:

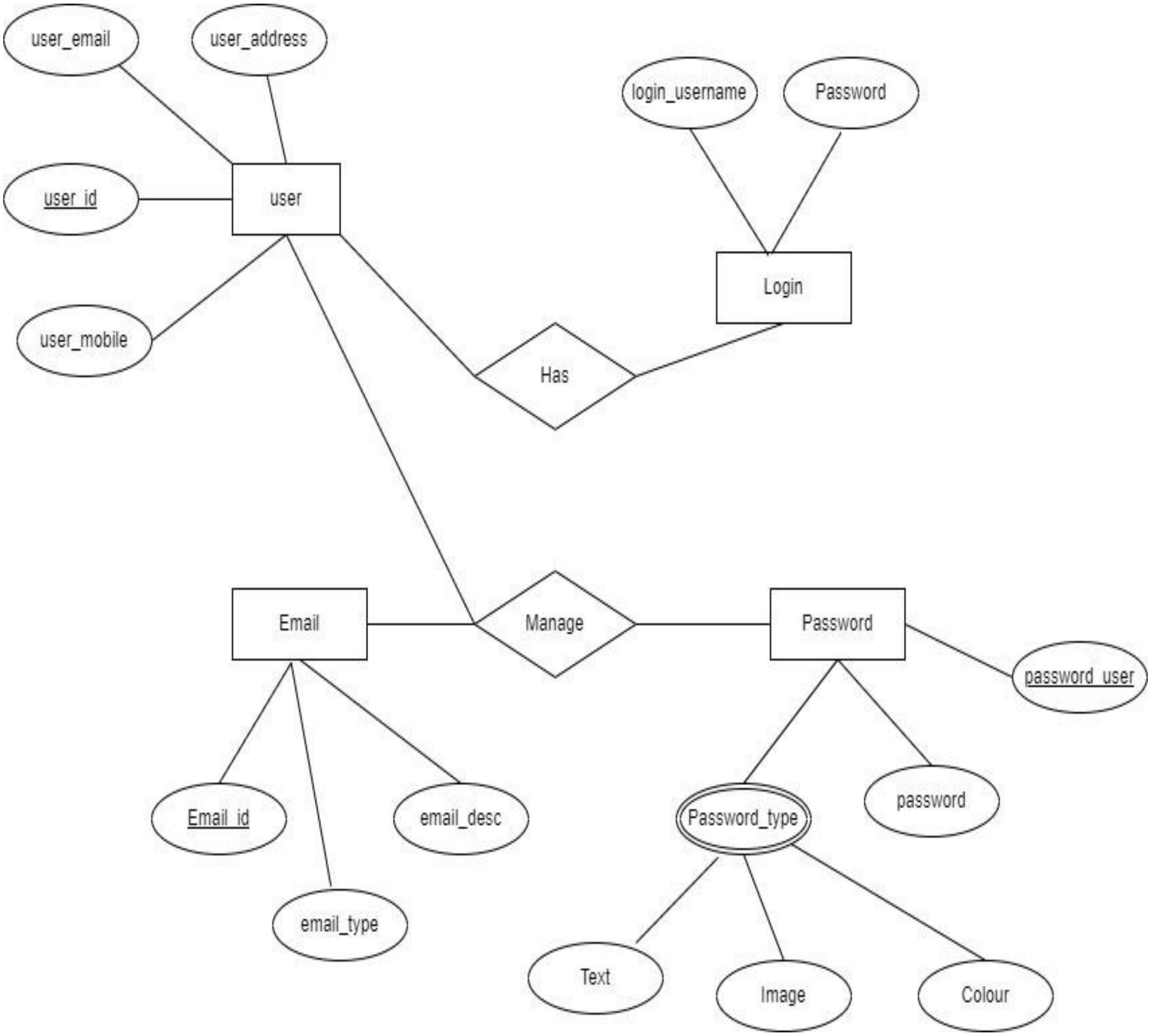


Fig3. High level design

Low level Design:

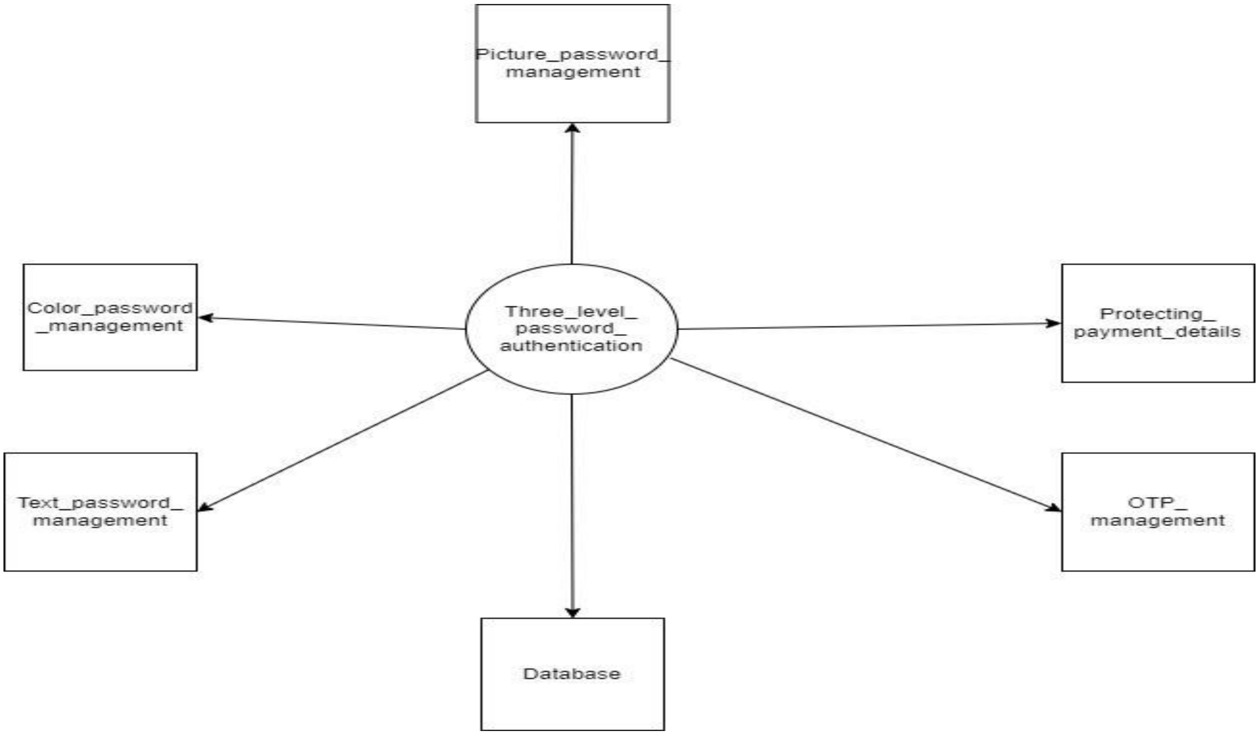


Fig 4: Low level Design

System Implementation:

Algorithms Used:

PERSUASIVE CUED (PC):

We have used PC algorithm in image-based password authentication, In persuasive cued algorithm image is split into grid and user needs to choose the pattern from this split images.

Algorithm steps:

1. User Registration: User chooses user name and set of split images of images that user provided as password for first time.

2. Login: At the time of login user enters same user name and split image pattern as password which was stored in database at time of registration to get log-in.

3. Verification: After submitting pattern of images choosed are matched with database for checking whether they are valid or not.

4.Confirmation: After verification is done on the basis of that it is confirmed whether to give access to user or not

Module:

Signup Module:

In signup module user needs sign in to the system by providing text based password at first and in second level user need to give 5 images from his device and after that he/she needs to choose the pattern from split images that he will choose in the given 5 images. In 3rd level he/she needs to choose color based password from the given colors. After that he can login into the system.

Login module:

To use the login module first user needs to signup into the system. While logging in to the system he/she has to go through the three level of authentication that is text based, picture based, color based password authentication

Admin module:

In admin module admin has some privileges like adding technician into the system, adding works into the system etc. He can also can change the status of the ordered work by the user.

4.3.4 Implementation:

Index page:

```
<!DOCTYPE html>
<html>
<head>
<title>Homyneeds</title>
<link rel="icon"  href="logo.png" type="image/x-icon">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css"
rel="stylesheet" integrity="sha384-
KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8CA5QIVfZOJ3BCsw2P0p/We"
crossorigin="anonymous">
```

```
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5awsuZVVFIhvj"
crossorigin="anonymous"></script>
<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.5.0/font/bootstrap-
icons.css">
</head>
<body style="background-color: #f5f5f5;">
<div class="container mt-5 text-center">
<h2 class="pt-5 mt-5 fs-1">Welcome To Homy Needs </h2>
<div class="row row-cols-1 row-cols-sm-2 row-cols-md-3 g-3 mt-3 mx-auto">
<div class="col">
<a href="login.php" style="text-decoration: none;"><div class="card mx-auto me-3 ms-3"
style="border-radius: 5px;border: 2px solid gray;">
  <img src="login.jpg" alt="login" style="width:auto ; height:220px">
    <h4><b>Login</b></h4>
</div></a>
</div>
<div class="col">
<a href="signup.php" style="text-decoration: none;">
<div class="card mx-auto me-3 ms-3" style="border-radius: 5px;border: 2px solid gray;">
  <img src="signup.jpg" alt="signup" style="width:auto ; height:220px">
    <h4><b>Signup</b></h4>
</div></a>
</div>
<div class="col">
<a href="admin.php" style="text-decoration: none;">
<div class="card mx-auto me-3 ms-3" style="border-radius: 5px;border: 2px solid gray;">
  <img src="admin.jpg" alt="admin" style="width:auto ; height:220px">
    <h4><b>Admin Login</b></h4>
</div></a>
```

```
</div>
</body>
</html>
```

Signup form:

```
<form  method="post">
  <div class="card" style="width:25rem;">
  <?php if(strlen($_SESSION['error'])!=0){?>
    <div class="alert alert-danger d-flex alert-dismissible" role="alert">
    <svg class="bi flex-shrink-0 me-2" width="24" height="24" role="img" aria-label="Danger:"><use xlink:href="#exclamation-triangle-fill"/>
    <div>
    <?php echo $_SESSION['error']; ?>
    </div></svg>
    <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
    </div>
    <?php }?>
  <div class="card-body">
    <div class="text-center">
    </div>
    <h1 class="card-title" align="center">Signup</h1>
    <div class="form-floating mt-3">
    <input type="text" placeholder="Enter username" name="username" class="form-control" id="username" required>
    <label for="username"><b>Username</b></label>
    </div>
    <div class="form-floating mt-3">
    <input type="text" placeholder="Enter E-mail" name="email" class="form-control" id="email" required>
    <label for="email"><b>E-mail</b></label>
    </div>
    <div class="form-floating mt-4 mb-3">
    <input type="password" placeholder="Enter Password" name="password_1" class="form-control" pattern="(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{8,}" title="Must contain at least one number and one uppercase and lowercase letter, and at least 8 or more characters" required>
    <label for="password_1"><b>Password</b></label>
    </div>
    <div class="mb-3">
    <button type="submit" onclick="validate()" class="w-100 btn btn-lg btn-primary" name="reg_user">Sign up</button>
    </div>
  <div>
    <a href="index.php"><button type="button" class="btn btn-danger">Cancel</button></a>
  </div>
  <div class="mt-2">
  <span>If existing user<a href="login.php" style="text-decoration: none;"> click here?</a></span>
  </div>
</div>
</form>
```

Server Page:

```
session_start();
    $username = "";
    $email    = "";
    $errors = array();
    $_SESSION['success'] = "";
    include ('connect.php');
        //signup part
    if (isset($_POST['reg_user'])) {
        $username = $_POST['username'];
        $email = $_POST['email'];
        $password_1 = $_POST['password_1'];
        $_SESSION['a'][0]=$username;
        $_SESSION['a'][2]=$password_1;
        $_SESSION['a'][1]=$email;
        header('Location:reg_upload.php');
```

Reg_upload page:

```
<?php
session_start();
if(isset($_POST['upload'])){
    extract($_POST);
    $time = date("d-m-Y")."-".date("h-i-s");

        // here we set it to the image name
        $i1 = $_FILES['img1']['name'];
        $i1 = $time."-".$i1 ;
        $i2 = $_FILES['img2']['name'];
        $i2 = $time."-".$i2 ;
        $i3 = $_FILES['img3']['name'];
        $i3 = $time."-".$i3 ;
        $i4 = $_FILES['img4']['name'];
        $i4 = $time."-".$i4 ;
        $i5 = $_FILES['img5']['name'];
        $i5 = $time."-".$i5 ;

        // upload that image into the directory name: images
        move_uploaded_file($_FILES['img1']['tmp_name'],$i1);
        move_uploaded_file($_FILES['img2']['tmp_name'],$i2);
        move_uploaded_file($_FILES['img3']['tmp_name'],$i3);
        move_uploaded_file($_FILES['img4']['tmp_name'],$i4);
        move_uploaded_file($_FILES['img5']['tmp_name'],$i5);
        $_SESSION['i1']=$i1;
        $_SESSION['i2']=$i2;
        $_SESSION['i3']=$i3;
        $_SESSION['i4']=$i4;
        $_SESSION['i5']=$i5;
        header('Location:registration_img1.php');
}
?>
<!DOCTYPE html>
<html>
<head>
      <title>Register</title>
      <meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css"
rel="stylesheet" integrity="sha384-
KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8CA5QIVfZOJ3BCsw2P0p/We"
crossorigin="anonymous">
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5awsuZVVFIhvj"
crossorigin="anonymous"></script>
<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.5.0/font/bootstrap-
icons.css">
</head>
<body style="background-color: #f5f5f5;">
<!-- signup form -->
<div class="signupform">
    <div class="container">
        <div class="agile_info">
            <div class="login_info mt-5">
                <form method="POST" enctype="multipart/form-data">
                <center>
                    <div class="mb-3 w-25">
  <label for="formFile" class="form-label">Image-1</label>
  <input class="form-control" type="file" id="formFile" name="img1">
</div>
<div class="mb-3 w-25">
  <label for="formFile" class="form-label">Image-2</label>
  <input class="form-control" type="file" id="formFile" name="img2">
</div>
<div class="w-25 mb-3">
  <label for="formFile" class="form-label">Image-3</label>
  <input class="form-control" type="file" id="formFile" name="img3">
</div>
<div class="w-25 mb-3">
  <label for="formFile" class="form-label">Image-4</label>
  <input class="form-control" type="file" id="formFile" name="img4">
</div>
<div class="w-25 mb-3">
  <label for="formFile" class="form-label">Image-5</label>
  <input class="form-control" type="file" id="formFile" name="img5">
</div>
<div class="col-12">
    <button type="submit" class="btn btn-primary" name="upload">Upload</button>
  </div>
                </center>
            </form>
            </div>
        </div>
    </div>
</div>
</body>
</html>
```

Image Display:

```
<?php
session_start();
?>
<!DOCTYPE html>
<html>
<head>
    <title>Register</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css"
rel="stylesheet" integrity="sha384-
KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8CA5QIVfZOJ3BCsw2P0p/We"
crossorigin="anonymous">
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5awsuZVVFIhvj"
crossorigin="anonymous"></script>
<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.5.0/font/bootstrap-
icons.css">
    <script>
    // passing the selected image reference to slice the image
    function changeIt(img)
    {
        var name = img.src;
        console.log(name);
        window.location.href = "reg_slice1.php?var="+name;
    }
    </script>
    <style>
    img{
      margin:10px;
      padding:10px;
    }
    </style>
</head>
<body style="background-color: #f5f5f5;">
<!-- signup form -->
<div class="signupform">
    <div class="container">
        <div class="agile_info">
            <div class="login_info">
                <h2>Create New Account</h2>
                <p class="account1">Select the 1st image for the graphical password.</p>
                <center>
                <img class="im" src="<?php echo $_SESSION['i1'];?>" onclick="changeIt(this)" height="200" width="200">
                <img class="im" src="<?php echo $_SESSION['i2'];?>" onclick="changeIt(this)" height="200" width="200">
                <img class="im" src="<?php echo $_SESSION['i3'];?>" onclick="changeIt(this)" height="200" width="200">
                <img class="im" src="<?php echo $_SESSION['i4'];?>" onclick="changeIt(this)" height="200" width="200">
                <img class="im" src="<?php echo $_SESSION['i5'];?>" onclick="changeIt(this)" height="200" width="200">
                </center>
            </div>
        </div>
    </div>
</div>
</body>
</html>
```

Image_sclice_page:

```
<?php
session_start();
ob_start();
?>
<html>
<head>
    <title>Register</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/bootstrap.min.css"
rel="stylesheet" integrity="sha384-
KyZXEAg3QhqLMpG8r+8fhAXLRk2vvoC2f3B09zVXn8CA5QIVfZOJ3BCsw2P0p/We"
crossorigin="anonymous">
<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
U1DAWAznBHeqEIlVSCgzq+c9gqGAJn5c/t99JyeKa9xxaYpSvHU5awsuZVVFIhvj"
crossorigin="anonymous"></script>
<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.5.0/font/bootstrap-
icons.css">
    <script src="slice1.js"></script>
    <style>
    img{
       margin:10px;
       padding:10px;
    }
    </style>
</head>

<?php

    $var=$_GET['var'];
    $_SESSION['a'][5]=$_GET['var'];
      $_SESSION['layer1']=$_GET['var'];
?>
<body style="background-color: #f5f5f5;">
<div class="signupform">
    <div class="container">
        <div class="agile_info">
            <div class="login_info">
                <h2>Create New Account</h2>
                <p class="account1">Following is the 1st image you chose.</p>
                <img src="<?php echo $var; ?>" onload="changeIt(this)" height="200" width="200">
                <p class="account">Select one from below four parts.</p>
                <center><div class="test mx-5 my-5" id="test"></div></center>
            </div>
        </div>
    </div>

</div>
</body>
</html>
```

Sclicing_js:

```
// slicing the image to four parts
function changeIt(img)
{
    var name = img.src;
    console.log(name);

    var canvas = document.createElement('canvas');
    ctx = canvas.getContext('2d');
    images=[],
    parts = [],
    img = new Image();
    img.onload = split_4;
    function split_4()
    {
        var w2 = img.width / 2,
        h2 = img.height / 2;
        for(i=0; i<4; i++){
            var x = (-w2*i) % (w2*2),
            y = (h2*i)<=h2? 0 : -h2;
            canvas.width = w2;
            canvas.height = h2;
            ctx.drawImage(this, x, y);
            parts.push( canvas.toDataURL() );
            //for test div
            var slicedImage = document.createElement('img')
            images.push(slicedImage);
            slicedImage.src = parts[i];
            var div = document.getElementById('test')
            div.appendChild(slicedImage);
        }
        for (var i = 0; i < 4; i++) (function(i){
            images[i].onclick=function(){
            changeIt2(i);
            }
        })(i);
    }
    img.src = name;
}
// passing the selected image slice
function changeIt2(i)
{
    var name = i;
    console.log(name);
    window.location.href = "registration_img2.php?var="+name;
}
```

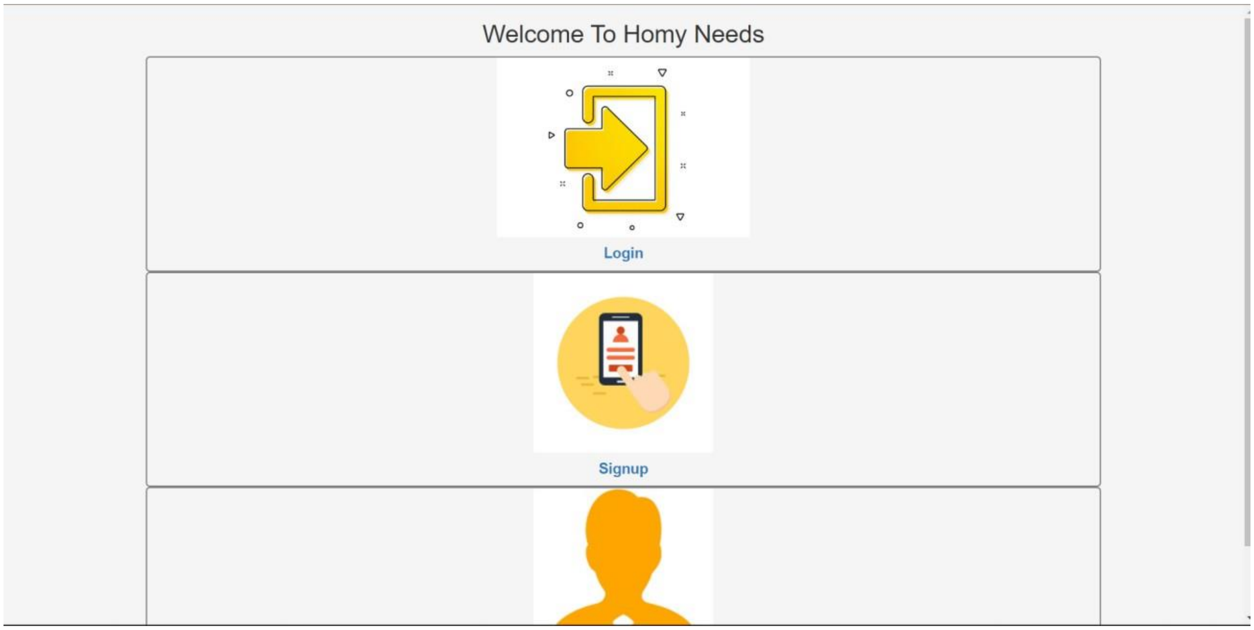
Color_reg:

```
<form method ="POST">
        <input type="hidden" id="value1" value="<?php echo $value1; ?>" name="value1">
        <input type="hidden" id="value2" value="<?php echo $value2; ?>" name="value2">
        <input type="hidden" id="value3" value="<?php echo $value3; ?>" name="value3">
        <input type="hidden" id="value4" value="<?php echo $value4; ?>" name="value4">
        <div class="form-floating mt-3 mb-5" style="width:250px;">
    <input type="text" id = "input1" name = "input1" value="" class="form-control" required
placeholder = "just enter the colors shown">
    <label for="input1"><b>Select your pattern:</b></label>
    </div>
        <input class = "btn Green mx-2 mt-2" type="button" value="green" name="button"
onclick="populateTextareaone()">
        <input class = "btn Orange  mx-2 mt-2" type="button" value="Orange" name="button"
onclick="populateTextareatwo()">
        <input class = "btn Pink  mx-2 mt-2"  type="button" value="Pink" name="button"
onclick="populateTextareathree()">
        <input class = "btn Red mx-2 mt-2" type="button" value="Red" name="button"
onclick="populateTextareafour()">
        <br>
        <br>
        <input class = "btn btn-danger" type="button" value="clear" name="button"
onclick="clearit()">
        <input class = "btn btn-primary" type="submit" value="submit" name="submit" required >
</form>
```

Database_link_page:

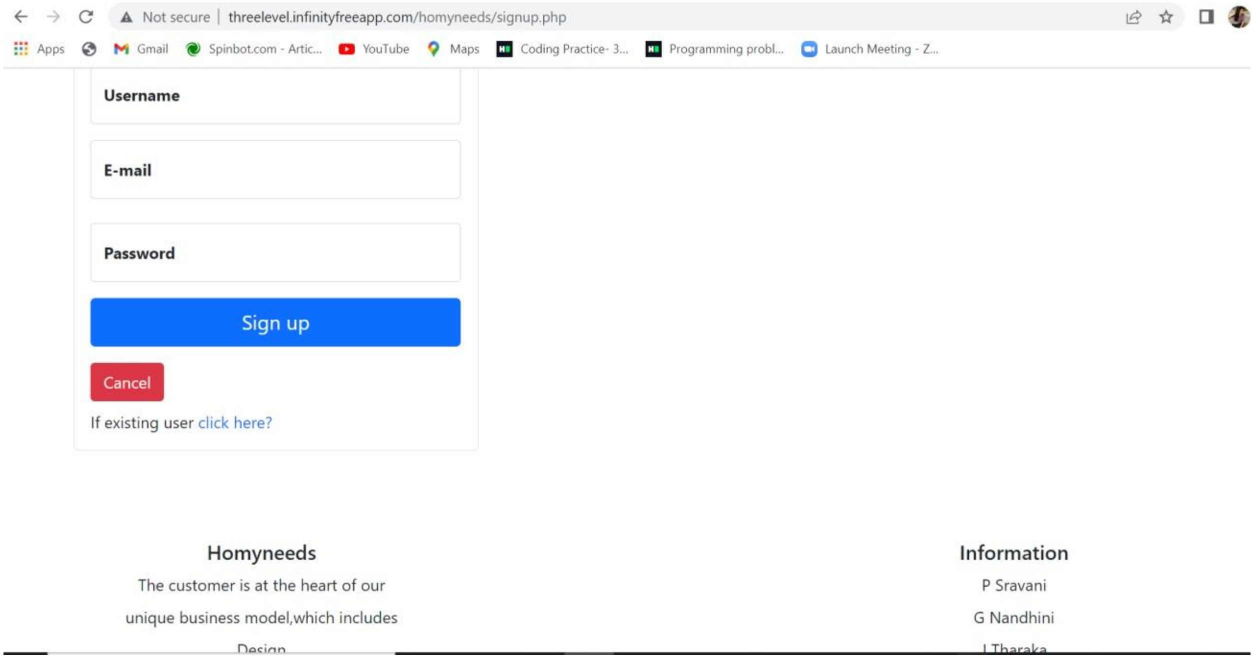
```
<?php
include('connect.php');
$i1=$_SESSION['i1'];
$i2=$_SESSION['i2'];
$i3=$_SESSION['i3'];
$i4=$_SESSION['i4'];
$i5=$_SESSION['i5'];
$username=$_SESSION['a'][0];
$password=$_SESSION['a'][2];
$email=$_SESSION['a'][1];
$image1=$_SESSION['a'][5];
$slice1=$_SESSION['a'][6];
$image2=$_SESSION['a'][7];
$slice2=$_SESSION['a'][8];
$image3=$_SESSION['a'][9];
$slice3=$_SESSION['a'][10];
$pattern=$_GET['pattern'];
$_SESSION['name']=$_SESSION['a'][0];
$query="INSERT into
users(username,email,password,image1,slice1,image2,slice2,image3,slice3,pattern)
values('$username','$email','$password','$image1','$slice1','$image2','$slice2','$image3','$slice3','
$pattern')";
$result=mysqli_query($con, $query);
$query1="INSERT into regusers(username,email,password,i1,i2,i3,i4,i5)
values('$username','$email','$password','$i1','$i2','$i3','$i4','$i5')";
$result1=mysqli_query($con, $query1);
header('Location:home.php');
?>
```

Home page:



Welcome To Homy Needs

Text Based authentication:



If existing user click here?

Homyneeds

The customer is at the heart of our unique business model,which includes Design

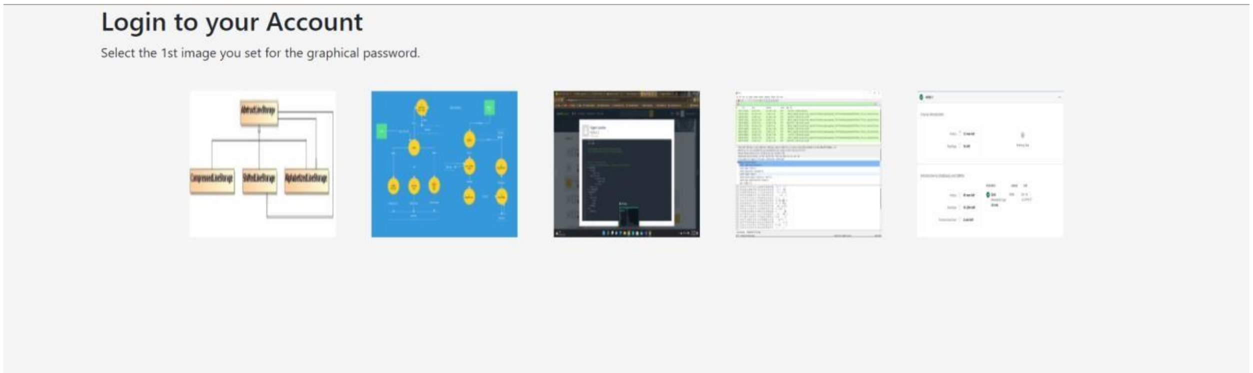
Information

P Sravani

G Nandhini

J Tharaka

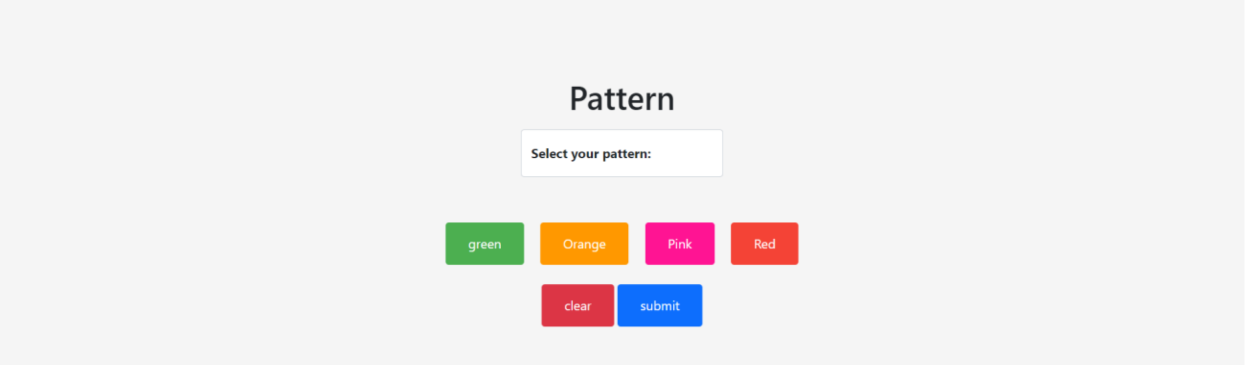
Picture Based Authentication:



Login to your Account

Select the 1st image you set for the graphical password.

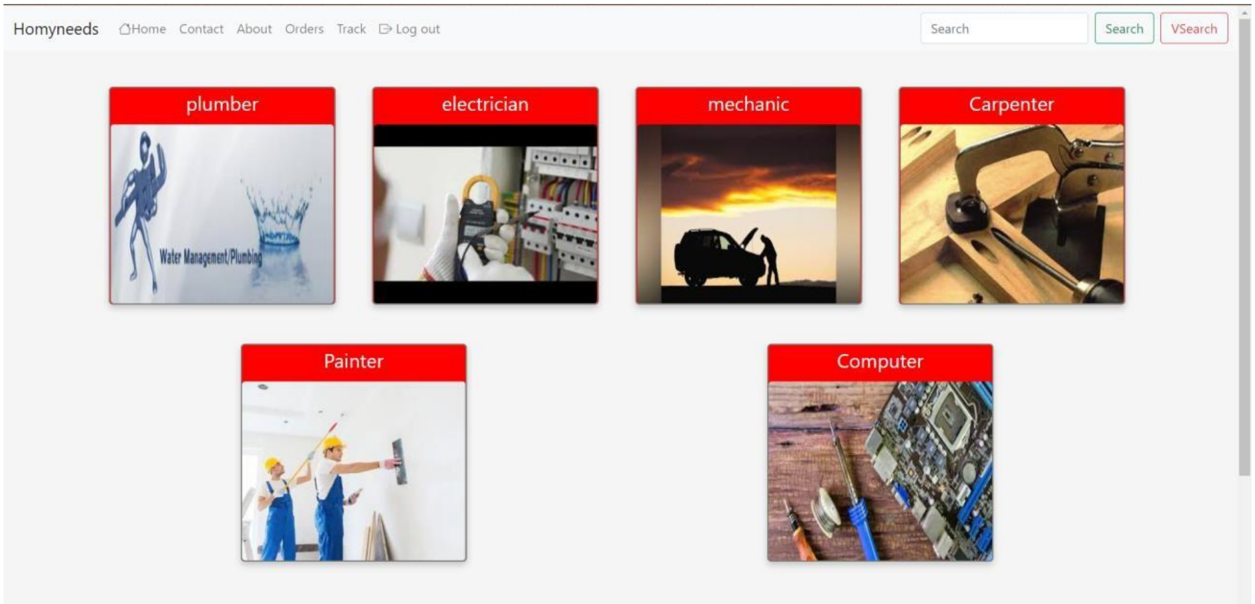
Color Based Authentication:



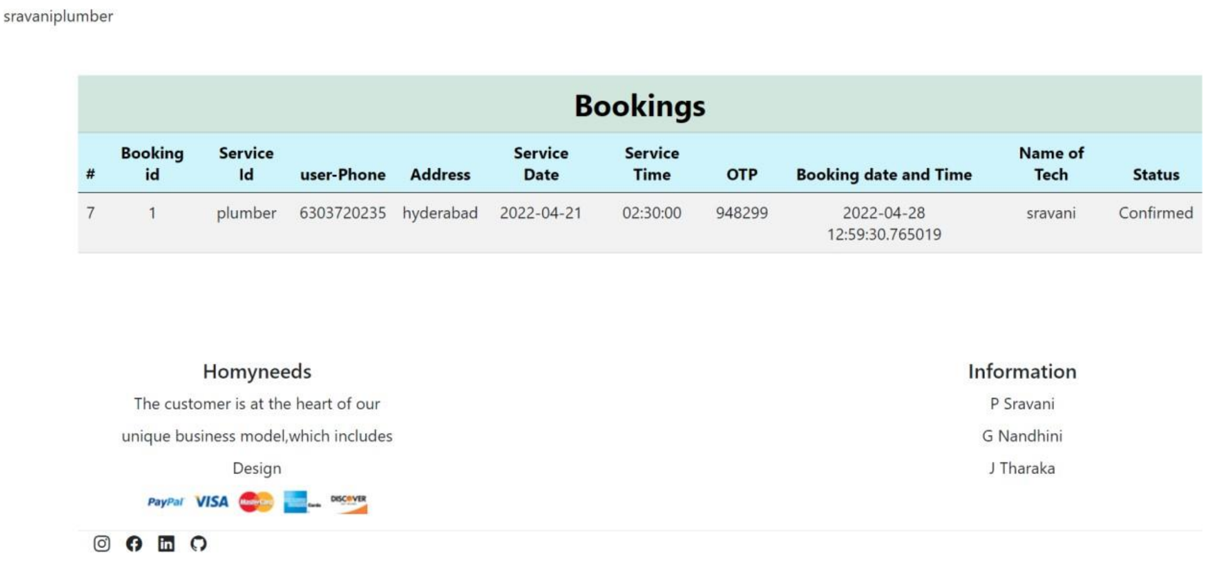
Pattern

Select your pattern:

Website:



Booking Conformations:



sravaniplumber

Bookings

#	Booking id	Service Id	user-Phone	Address	Service Date	Service Time	OTP	Booking date and Time	Name of Tech	Status
7	1	plumber	6303720235	hyderabad	2022-04-21	02:30:00	948299	2022-04-28 12:59:30.765019	sravani	Confirmed

Homyneeds

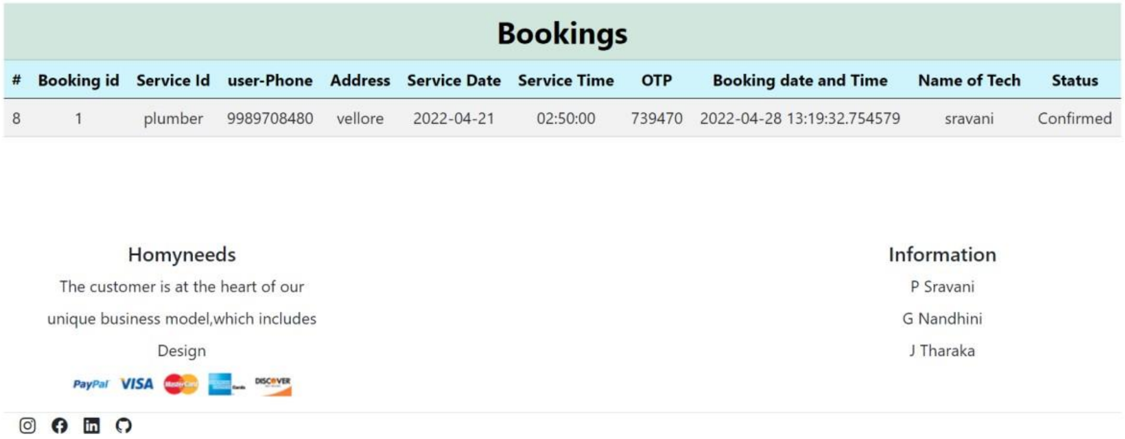
The customer is at the heart of our unique business model,which includes Design

Information

P Sravani

G Nandhini

J Tharaka



Bookings

#	Booking id	Service Id	user-Phone	Address	Service Date	Service Time	OTP	Booking date and Time	Name of Tech	Status
8	1	plumber	9989708480	vellore	2022-04-21	02:50:00	739470	2022-04-28 13:19:32.754579	sravani	Confirmed

Homyneeds

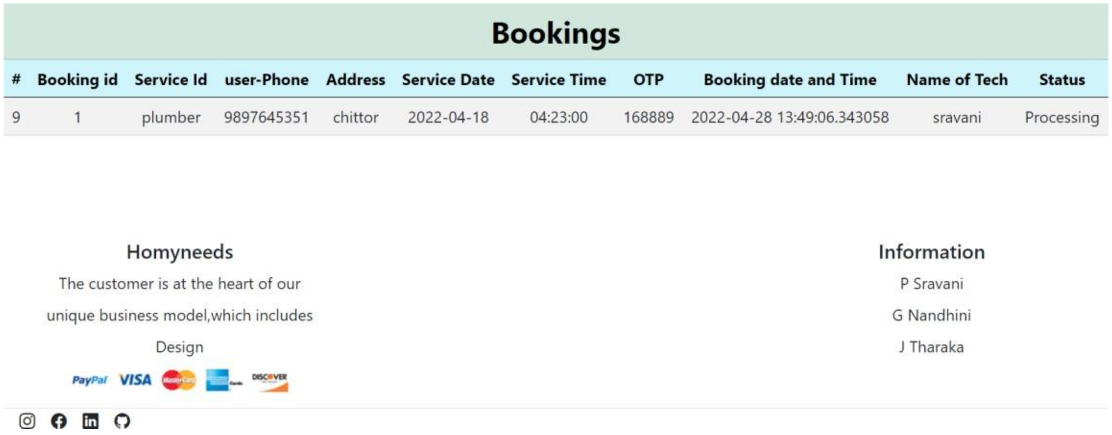
The customer is at the heart of our unique business model,which includes Design

Information

P Sravani

G Nandhini

J Tharaka



Bookings

#	Booking id	Service Id	user-Phone	Address	Service Date	Service Time	OTP	Booking date and Time	Name of Tech	Status
9	1	plumber	9897645351	chittor	2022-04-18	04:23:00	168889	2022-04-28 13:49:06.343058	sravani	Processing

Homyneeds

The customer is at the heart of our unique business model,which includes Design

Information

P Sravani

G Nandhini

J Tharaka

Mapping the results with problem statement and existing systems

The final system can result as a three-password authentication application that provides the users to access the webpage with associate degree ease the application will have a sign up and login page through which the user will register and login themselves. The project is an authentication system that validates user for accessing the system only when they have input correct password. The project involves three levels of user authentication. There are varieties of password systems available, many of which have failed due to bot attacks while few have sustained it but to a limit. In short, almost all the passwords available today can be broken to a limit. Hence this project is aimed to achieve the highest security in authenticating users.

It contains three logins having three different kinds of password system. The password difficulty increases with each level. Users have to input correct password for successful login. Users would be given privilege to set passwords according to their wish. The First level contains text based password system and the Second level contains Image segmentation password system and the Third one contains colour based authentication. Other than that we created a website called homey needs where we can confirm the booking with an advance payment .To protect this through OTP .The OTP should match with admins in admins column .This is how the web application works using Three Level Password Authentication.

Conclusion and Future Developments:

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.

References:

[1] Mishra, Gouri Sankar, et al. "User Authentication: A Three Level Password Authentication Mechanism." Journal of Physics: Conference Series. Vol. 1712. No. 1. IOP Publishing, 2020.

[2] Mulwani K, Naik S, Gurnani N, Giri N, Sengupta S. 3LAS (three level authentication scheme). International Journal of Emerging Technology and Advanced Engineering. 2013;3:1037.

[3] Chhetri B. Novel Approach towards Authentication using Multi Level Password System. International Journal of Computer Applications & Information Technology. 2020;12(1):292-7

[4] Xie Q, Zhao J, Yu X. Chaotic maps-based three-party password-authenticated key agreement scheme. Nonlinear Dynamics. 2013 Dec;74(4):1021-7.

[5] Zhao H, Li X. S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In21st international conference on advanced information networking and applications workshops (AINAW'07) 2007 May 21 (Vol. 2, pp. 467-472). IEEE.

[6] Jiang Q, Ma J, Li G, Li X. Improvement of robust smart-card-based password authentication scheme. International Journal of Communication Systems. 2015 Jan 25;28(2):383-93.

[7] Shen JJ, Lin CW, Hwang MS. Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security. 2003 Oct 1;22(7):591-5.

[8] Chan CK, Cheng LM. Cryptanalysis of a timestamp-based password authentication scheme. Computers & Security. 2001 Jan 1;21(1):74-6.

[9] Chiasson S, Van Oorschot PC, Biddle R. Graphical password authentication using cued click points. InEuropean Symposium on Research in Computer Security 2007 Sep 24 (pp. 359-374). Springer, Berlin, Heidelberg.

[10] Gurav SM, Gawade LS, Rane PK, Khochare NR. Graphical password authentication: Cloud securing scheme. In2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies 2014 Jan 9 (pp. 479-483). IEEE