THREE FACTOR AUTHENTICATION FOR ONLINE TRANSACTIONS

A Project Report submitted under the partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by

V Nikhil Reddy-(121710307054)

Gudla Vishal Reddy-(121710307012)

Komatineni Harshitha -(121710307063)

Dhanala Srivatsava-(121710307010)

Under the esteemed direction of

Mr.A.Yashwant

Assistant Professor

Department of Computer Science and Engineering, GITAM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Deemed university declared under section 3 of the UGC Act, 1956

Rushikonda, Visakhapatnam, AndhraPradesh – 530045, India.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM INSTITUTE OF TECHNOLOGY

GITAM

(Deemed to be University)

VISAKHAPATNAM

DECLARATION

I with this declare that the Project report entitled **“Three Factor Authentication for Online Transactions”** submitted by **V.Nikhil Reddy(121710307054), Gudla.Vishal Reddy(121710307012), Komatineni.Harshitha(121710307063), Dhanala Srivatsava (121710307010)** to GITAM, Deemed to be university for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a result of the original research work carried out in the thesis. We understand that our report can be made electronically available to the public. It is further declared that the project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

Registration No	Student-Signature	Name of the Student
121710307054	V.Nikhil Reddy	V Nikhil Reddy
121710307012	Gudla Vishal Reddy	Gudla Vishal Reddy
121710307063	Komatineni.Harshitha	Komatineni Harshitha
121710307010	Dhanala Srivatsava	Dhanala Srivatsava

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM INSTITUTE OF TECHNOLOGY

GITAM

(Deemed to be University)

VISAKHAPATNAM

CERTIFICATE

This is to certify that Project entitled **“Three Factor Authentication for Online Transactions”** carried out by **V.Nikhil Reddy (121710307054), Gudla Vishal Reddy (121710307012), Komatineni Harshitha (121710307063), Dhanala Srivatsava (121710307010)** submitted in partial fulfillment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering, GITAM -Deemed to be University, Visakhapatnam during the academic year 2017-2021.

PROJECT GUIDE	**HEAD OF THE DEPARTEMENT**
A.Yashwanth	**Dr. R. Sireesha**

ACKNOWLEDGMENT

We take this opportunity to remember and acknowledge the cooperation, goodwill and support both moral and technical extended by several individuals out of which our project has evolved. We shall always cherish our association with them.

We are greatly thankful to Guide, Assistant Professor, **A.Yashwanth** Sir for providing us with all his valuable suggestions and support to make our project a success.

We would like to express thanks and our gratitude to the Head of the Department of Computer Science and Engineering, **Dr. R. Sireesha** Ma'am, whose suggestions and encouragement have immensely helped us in the completion of the project and for their support and valuable suggestions during the dissertation work.

We express our sincere thanks to **Dr. C. Dharma Raj** Sir, I/c Principal & Professor, GITAM Institue of Technology, GITAM for inspiring us to learn new technologies and tools.

We offer our sincere gratitude to our Project reviewer **Dr.R . Sireesha** Ma'am, who has supported us throughout this project with her patience for her valuable guidance and encouragement during our project reviews.

We offer our sincere gratitude to our Project reviewer & A.M.C, **Mr. Bhargav K** Sir, who has supported us throughout this project with his patience for his valuable guidance and encouragement during our project reviews.

We would also like to thank all the supporting staff of the Department of Computer Science and Engineering and all other departments who have been helpful directly or indirectly in making the project a success.

We are extremely grateful to our Parents and Friends for their blessings and prayers for our completion of the project that gave us strength to do our project.

Submitted by,

V Nikhil Reddy -121710307054

Gudla Vishal Reddy -121710307012

Komatineni Harshitha - 121710307063

Dhanala Srivastava - 121710307010

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Motivation:

The motivation of our project is to provide a systematic approach to plan three factor authentication by enhancing security to the user. This three factor authentication based on biometric which will be more secure for any of the online transactions which are done by using OTP.

1.2 Project Objective:

In this new digital age, the efforts for carrying out online transactions (mostly financial) have been reduced through the rise of payment banks like AIRTEL, PAYTM and so on, digital wallets like PHONE PE, GOOGLE PAY and payment processing services like AMAZON PAY, have further reduced the complexities of operating by traditional online banking methods. The provision of security is the biggest challenge faced in the roll out plan for online transaction methods. The parameters involved in ensuring safe transactions include security of browser and various payment gateways along with multiple factor authentication of user

- The security aspects involved in authentication are further improved by using different communication media like the Internet for username and password and phone based short message service (SMS) or email services for one time password (OTP).
- This concept is being followed currently, with the aim of reducing user-based vulnerabilities for occurrence of fraud and has been very successfully implemented with improved security.
- However, online frauds are still being carried out especially in transactions carried out on mobile platforms .Through use of mobile malwares, captured or stolen mobile devices and hacked emails.
- Considering use of OTP and its inherent security benefits, further improvements in generation, transmission and operation on OTP are required to provide better

secure user authentication for online transactions. The work in this project focuses towards these improvements by proposing use of biometric

1.3 Drawbacks for the existing System:

The two foundations on which OTP over SMS is built on cellular networks and mobile handsets which were completely different when the method was introduced. Security depends on the confidentiality of text messages and the security of the network, neither of which can be guaranteed.

Hackers have created specialized Trojans to get around OTP over SMS security. These trojans hijack mobile phones.

● Can Be Spoofed

On-demand delivery methods are susceptible to spoofing, a phishing technique that hackers use to trick users into giving them account information or codes by pretending to be a legitimate source. An attacker simply visits the login page and requests a "reset password" 2 Factor Authentication code be sent. Then, the attacker sends the victim an SMS message or email that appears to be from a legitimate source and says something along the lines of: "Suspicious activity has been detected on your account. Respond with the code you received in order to prevent unauthorized access." If the victim forwards the code, the attacker is able to gain easy access to the account.

● Phone Accounts Can Be Hijacked

Phone accounts can be hijacked in what's known as a SIM card swap attack. This is when hackers with some knowledge of their victims, such as the last four digits of their Social Security number, call the victim's phone carrier and have the victim's phone number moved to a new device that's in the hacker's possession, so that the OTPs can be intercepted. In one recent case, a hacker used publicly available information to persuade AT&T(American Telephone and Telegraph) to reassign the victim's phone number, then accessed the victim's PayPal account using SMS 2 Factor Authentication.

● Codes Can Be Intercepted

Hackers can exploit vulnerabilities in Signaling System No. 7 (SS7), an international telecommunications standard that facilitates SMS delivery—this isn't as difficult or expensive as one might think. Attackers can gain access to the SS7 network for as little as $500 a month. This occurred in 2017 when attackers exploited this vulnerability to intercept SMS messages with OTP codes tied to victims' bank accounts.

● Codes Are Sent in Plain Text

SMS and email messages are sent in plain text, meaning anyone who manages to intercept or get access to them can clearly read the OTP.

CHAPTER 2

LITERATURE REVIEW

2.1. Two-factor authentication using biometric based quantum operations:

The work in this paper tells about security concerns due to the static nature of shared secrets and pattern discovery of OTP generation and proposes a method to implement two factor authentication using quantum computing to generate QOTP and user biometrics for authenticating the user. The paper describes three use cases defining various capabilities of users related to the quantum environment, which are based on operation, measurement and communication of qubits. The security analysis for the three use cases are carried out individually against a single threat model. Their possible implementation has been proven with mathematical concepts and successfully conducted experiments for implementing.

2.2.Incorporating Touch Biometrics to Mobile One-Time Passwords:

The work in this paper evaluates the advantages and potential of incorporating fingerprint biometrics to mobile one-time passwords . The new e-BioDigit database which

experiments reported in this work. Data was collected in two sessions with a time gap of at least three weeks between them for a total of 93 subjects. Handwritten numerical digits were acquired using the finger touch as the writing input on a Samsung Galaxy Note 10.1 general purpose tablet device. The following three different experiments are considered in this paper: 1) a Baseline System comprised of a set of simple and fixed time functions for all numerical digits in order to make our work easily reproducible; 2) an study of the best features for each handwritten numerical digit through the SFFS algorithm on the development dataset; and 3) an analysis of the OTP system regarding which are the most discriminative handwritten digits and how robust the system is when increasing the number of digits included in the OTP.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Hardware Requirements

1. 4GB RAM
2. i3 Processor
3. Fingerprint scanner

3.2 Software Requirements

1. Metasploit :- The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7
2. Kali Linux :- Kali Linux is a Debian-derived Linux operating system distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.
3. (Hacking apps).apk
4. XAMPP :- XAMPP is the most popular PHP development environment. XAMPP is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl.
5. Android studio :- Android Studio is the official integrated development environment for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development
6. Sublime editor

CHAPTER 4

SYSTEM DESIGN

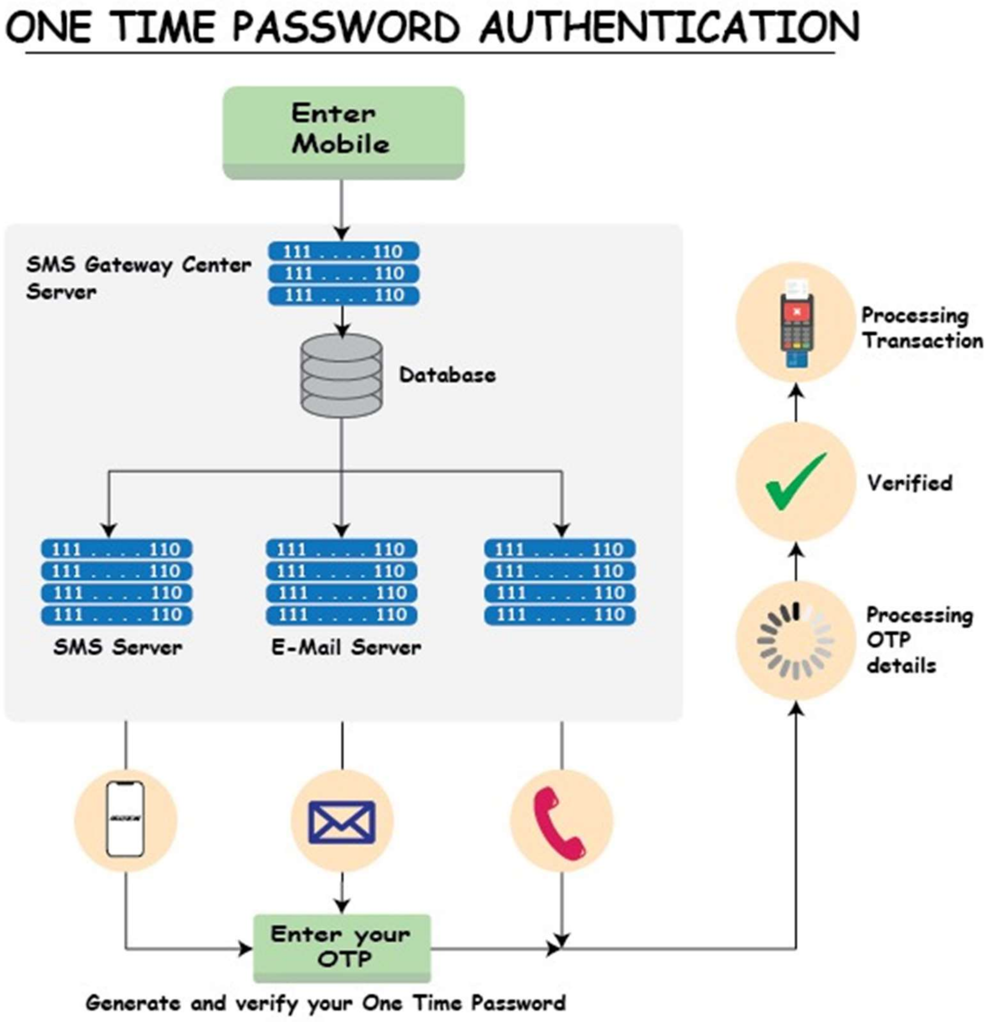
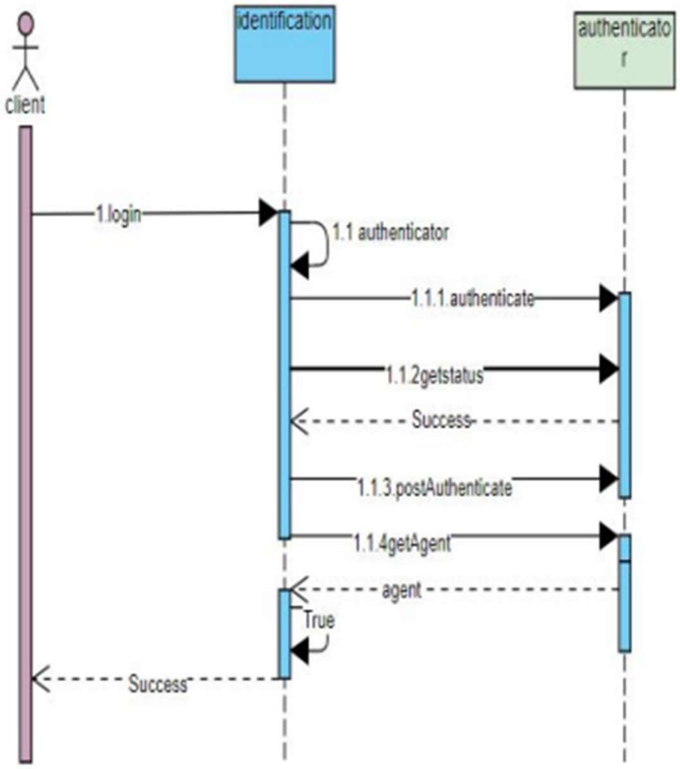


Fig : Flowchart for OTP Transactions.

4.1 UNIFIED MODELING LANGUAGE DIAGRAMS

4.1.1. SEQUENCE DIAGRAM FOR ONLINE TRANSACTIONS



1 - The user invokes the login() method of the Identity bean.

1.1 - The Identity bean (after performing a couple of validations) invokes its own authenticate() method.

1.1.1 - Next the Identity bean invokes the Authenticator bean's authenticate() method (which has a return value of void).

1.1.2 - To determine whether authentication was successful, the Identity bean invokes the Authenticator's getStatus() method, which returns a SUCCESS.

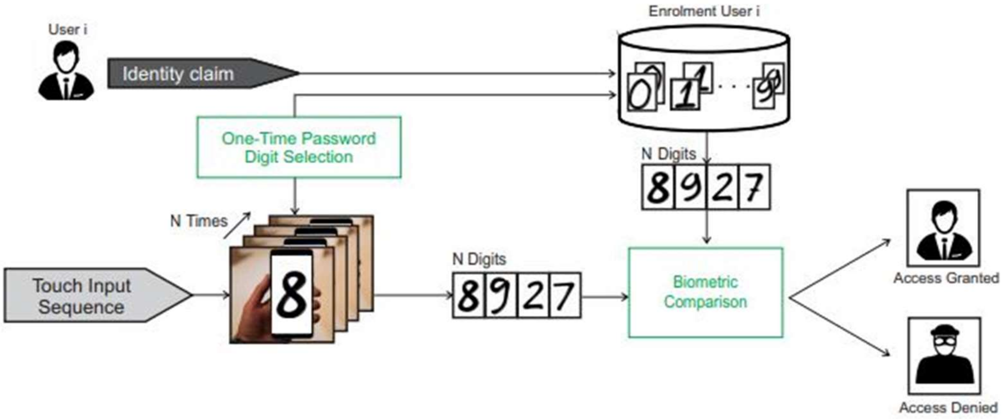
1.1.3 - Upon a successful authentication, the Identity bean then invokes the Authenticator's postAuthenticate() method to perform any post-authentication logic.

1.1.4 - The Identity bean then invokes the Authenticator's getAccount() method, which returns an Account object representing the authenticated agent, which is then stored as a private field in the Identity

CHAPTER 5

METHODOLOGY

In this work, we propose an OTP framework that incorporates contact biometrics for portable situations. In our proposed approach, users' biometric data (fingerprints) will be stored in his personal device . The digit will be then assigned to the each fingerprint of users choice which can be changed by users if they want. While logging in, the user will receive the mathematical digits from the OTP generator on the screen . As per the received OTP user should verify the biometrics in their device in the specific order . If the OTP is 4 digit then the system will compare 4 fingerprints with every digit if they are placed in the correct order of the OTP and then access will be granted to the user.



CHAPTER 6

SAMPLE CODES

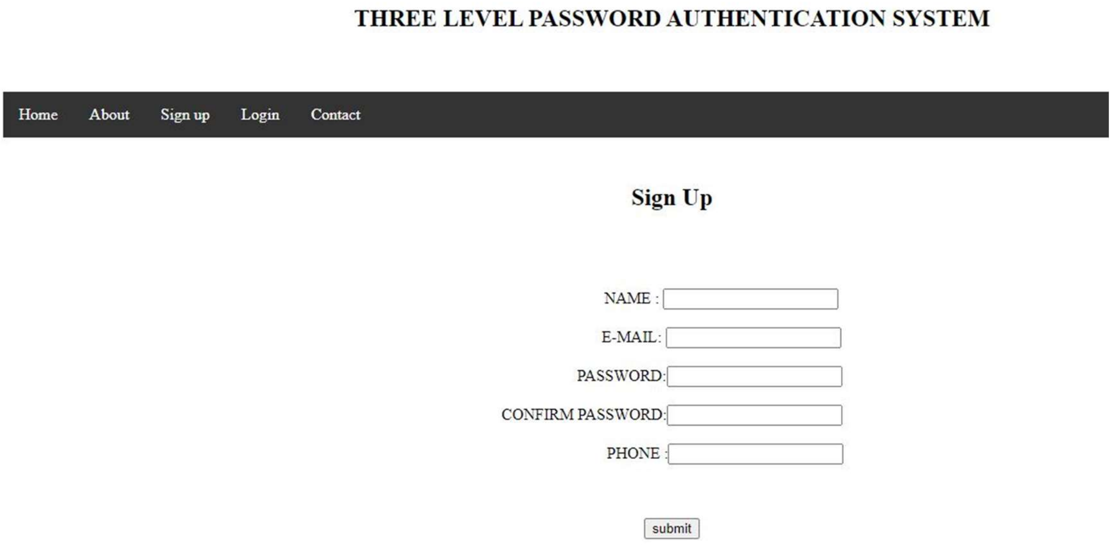
6.1 SIGN UP PAGE:

```
<?php

if (!isset($_SERVER['HTTP_REFERER'])){

?>

<script>

alert('no cheating dude');

document.location = "login.html"

</script>

<?php

}

session_start();

$name=$_POST['name'];

$email=$_POST['email'];

$_SESSION['login_user'] = $email;

$password=$_POST['password'];

$confirm_password=$_POST['confirm_password'];

$phone=$_POST['phone'];
```

```
$conn=new mysqli("localhost","root","","authentication")or die("mysqli_error()");

$c=mysqli_select_db($conn,"authentication")or die("mysqli_error()");

if (empty($name))

{

  ?>



<script>

 alert('enter all the details');!

 document.location="signup.html"

 </script>

<?php

}




elseif (empty($email))

{

    ?>

<script>

 alert('enter all the details');

 document.location="signup.html"

 </script>;

<?php

}
```

```
elseif (empty($password))
{
    ?>
<script>
  alert('enter all the details');
  document.location="signup.html"
  </script>;
<?php
}

elseif (empty($confirm_password))
{
     ?>
<script>
  alert('enter all the details');
  document.location="signup.html"
  </script>;
<?php
}

elseif (empty($phone))
{
    ?>
<script>
  alert('enter all the details');
  document.location="signup.html"
  </script>;
  <?php
}

else
{
if($password==$confirm_password)
    {
        $sql_crt = "CREATE TABLE IF NOT EXISTS register ( `id` INT(100) NOT
NULL AUTO_INCREMENT , `username` VARCHAR(100) NOT NULL , `email`
VARCHAR(100) NOT NULL , `password` VARCHAR(100) NOT NULL , `phone`
VARCHAR(15) NOT NULL , `checkotp` TINYINT(1) NOT NULL DEFAULT '0' ,
PRIMARY KEY (`id`, `email`), UNIQUE (`phone`)) ENGINE = InnoDB;";
  mysqli_query($conn,$sql_crt);
  $sql= "INSERT into register(username, email, password, phone) val-
ues('$name','$email','$password','$phone')";
if(mysqli_query($conn,$sql))

        ?>
<script>
```

```
  alert('Congratulations! Registration Successful');

  document.location="pattern.php"

  </script>;

<?php

}

    else

    {

?>

<script>

  alert('password and confirm password do not match');

  document.location="signup.html"

  </script>;

 <?php

        //echo "confirm the password correctly";

        //header("Location:signup.html");


    }

}

?>
```



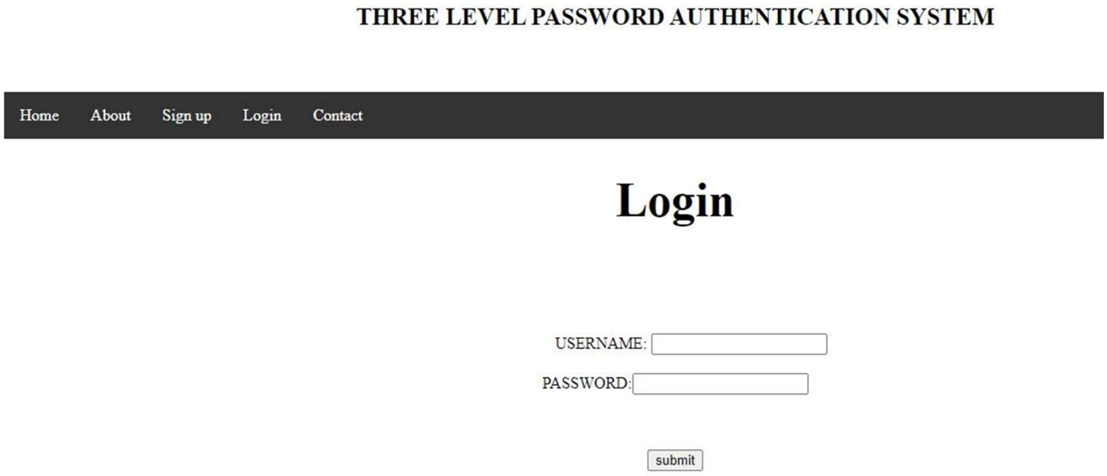
6.2 LOGIN PAGE:

```
<?php

if (!isset($_SERVER['HTTP_REFERER'])){

?>

<script>

alert('no cheating dude');

document.location = "login.html"

</script>

<?php

}

session_start();

//Your authentication key

$authKey = "202216A5QenzYQYP5aa6171d";

//Multiple mobiles numbers separated by comma
```

```
$mobileNumber = $_POST["phone"];

//datebase connection

$conn=new mysqli("localhost","root","","authentication")or die("mysqli_error()");

//$c=mysqli_select_db($conn,"login")or die("mysqli_error()");//anything happens it just die

//fethcing the data from database through quering

$username = $_SESSION['login_user'];

$sql = "SELECT * FROM register WHERE email = '$username'";

$result = mysqli_query($conn,$sql);//to prevent sql injection

$rowcount = mysqli_num_rows($result);

if($rowcount){

$rows = mysqli_fetch_array($result, MYSQLI_ASSOC);

if($rows['phone'] == $mobileNumber){

//Sender ID,While using route4 sender id should be 6 characters long.

$senderId = "MSGIND";

//Your message to send, Add URL encoding here.

$rndno=rand(10000, 99999);

$message = urlencode("otp number.".$rndno);

//Define route

$route = "route=4";

//Prepare you post parameters

$postData = array(
'authkey' => $authKey,

'mobiles' => $mobileNumber,

'message' => $message,

'sender' => $senderId,

'route' => $route

);

//API URL

$url="https://control.msg91.com/api/sendhttp.php";

// init the resource

$ch = curl_init();

curl_setopt_array($ch, array(

CURLOPT_URL => $url,

CURLOPT_RETURNTRANSFER => true,

CURLOPT_POST => true,

CURLOPT_POSTFIELDS => $postData

//,CURLOPT_FOLLOWLOCATION => true

));

//Ignore SSL certificate verification

curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);

curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);

//get response

$output = curl_exec($ch);

//Print error if any
```

```
if(curl_errno($ch))

{

echo 'error:' . curl_error($ch);

}

curl_close($ch);

if(isset($_POST['btn-save']))

{

$_SESSION['phone']=$_POST['phone'];

$_SESSION['otp']=$rndno;

header( "Location: verifylogin.php" ); }

}

}

else{

?>

<script>

alert('invalid mobile number')

document.location = "login.html"

</script>

<?php
```

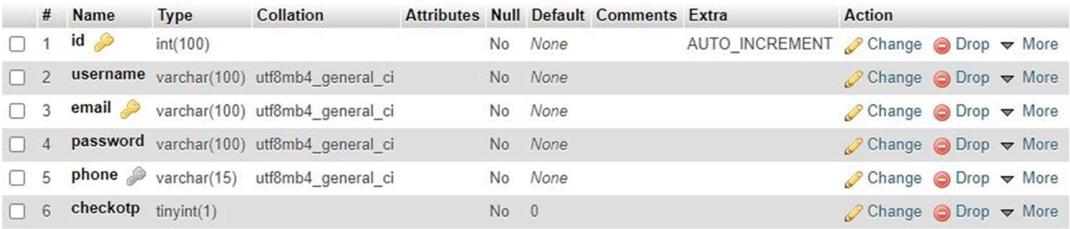
```
}                                                               ?>
```



6.3 OTP VERIFICATION:

```
<?php

if (!isset($_SERVER['HTTP_REFERER'])){

?>

<script>

alert('no cheating');

document.location = "login.html"

</script>

<?php

}

session_start();

if($_SERVER["REQUEST_METHOD"] == "POST") {

$entered_otp = $_POST['otpverify'];
$generated_otp = $_SESSION['otp'];

if($entered_otp == $generated_otp)

{

?>

<script>

alert("OTP verificatin success");

document.location = "thankyou.php"

</script>

<?php

}

else{

?>

<script>

alert('OTP verificatin failed');


                                                   document.location="l
ogin.html"

</script>

<?php

}

}

session_destroy();

?>
```

6.4 DATABASE TABLE:



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	id	int(100)			No	*None*		AUTO_INCREMENT	Change Drop More
□	2	username	varchar(100)	utf8mb4_general_ci		No	*None*			Change Drop More
□	3	email	varchar(100)	utf8mb4_general_ci		No	*None*			Change Drop More
□	4	password	varchar(100)	utf8mb4_general_ci		No	*None*			Change Drop More
□	5	phone	varchar(15)	utf8mb4_general_ci		No	*None*			Change Drop More
□	6	checkotp	tinyint(1)			No	0			Change Drop More

6.5 APPLICATION CODE:

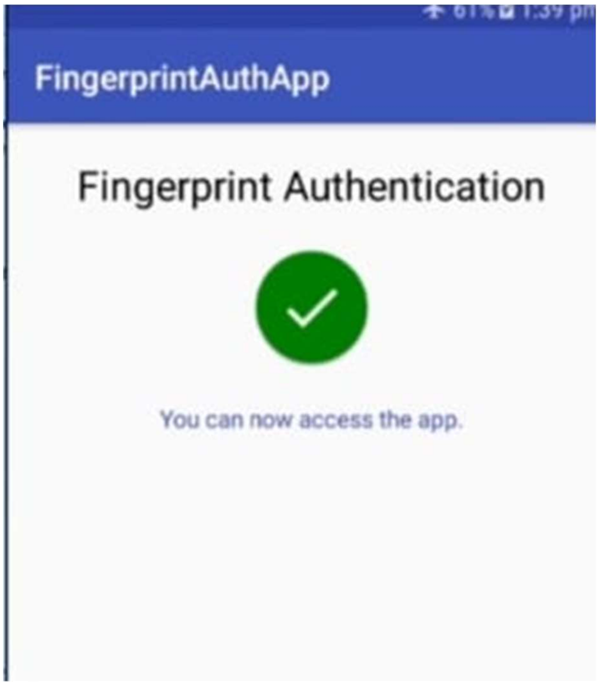
```
package in.tvac.nikhiljh.fingerprintauthapp;


import android.Manifest;

import android.annotation.TargetApi;

import android.app.KeyguardManager;

import android.content.pm.PackageManager;

import android.hardware.fingerprint.FingerprintManager;

import android.media.Image;

import android.os.Build;

import android.security.keystore.KeyGenParameterSpec;

import android.security.keystore.KeyPermanentlyInvalidatedException;

import android.security.keystore.KeyProperties;

import android.support.v4.content.ContextCompat;

import android.support.v7.app.AppCompatActivity;

import android.os.Bundle;

import android.widget.ImageView;

import android.widget.TextView;


import java.io.IOException;

import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.Key;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.UnrecoverableKeyException;
import java.security.cert.CertificateException;

import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;

public class MainActivity extends AppCompatActivity {


    private TextView mHeadingLabel;
    private ImageView mFingerprintImage;
    private TextView mParaLabel;

    private FingerprintManager fingerprintManager;
    private KeyguardManager keyguardManager;

    private KeyStore keyStore;
    private Cipher cipher;
    private String KEY_NAME = "AndroidKey";
```

```
   @Override
   protected void onCreate(Bundle savedInstanceState)
{
     super.onCreate(savedInstanceState);
     setContentView(R.layout.activity_main);

       mHeadingLabel = (TextView) findViewById(R.id.headingLabel);
       mFingerprintImage = (ImageView) findViewById(R.id.fingerprintImage);
       mParaLabel = (TextView) findViewById(R.id.paraLabel);



       if(Build.VERSION.SDK_INT >= Build.VERSION_CODES.M) {
fingerprintManager=(FingerprintManager)
getSystemService(FINGERPRINT_SERVICE);
keyguardManager=(KeyguardManager)
getSystemService(KEYGUARD_SERVICE);

 if(!fingerprintManager.isHardwareDetected()){
mParaLabel.setText("Fingerprint Scanner not detected in Device");
}
elseif
(ContextCompat.checkSelfPermission(this,
manifest.permission.USE_FINGERPRINT)!=
packageManager.PERMISSION_GRANTED){

 mParaLabel.setText("Permission not granted to use Fingerprint Scanner");
} else if (!keyguardManager.isKeyguardSecure()){
mParaLabel.setText("Add Lock to your Phone in Settings");
} else if (!fingerprintManager.hasEnrolledFingerprints()){
mParaLabel.setText("You should add atleast 1 Fingerprint to use this Feature");
} else {
 mParaLabel.setText("Place your Finger on Scanner to Access the App.");
              generateKey();


               if (cipherInit()){


FingerprintManager.CryptoObject cryptoObject = new
FingerprintManager.CryptoObject(cipher);
  FingerprintHandler fingerprintHandler = new FingerprintHandler(this);
   fingerprintHandler.startAuth(fingerprintManager, cryptoObject);


               }
           }


       }


    }


    @TargetApi(Build.VERSION_CODES.M)
    private void generateKey() {


        try {
```

```
      keyStore = KeyStore.getInstance("AndroidKeyStore");
KeyGenerator keyGenerator =
KeyGenerator.getInstance(KeyProperties.KEY_ALGORITHM_AES,
"AndroidKeyStore");


      keyStore.load(null);

      keyGenerator.init(new

          KeyGenParameterSpec.Builder(KEY_NAME,

          KeyProperties.PURPOSE_ENCRYPT |

              KeyProperties.PURPOSE_DECRYPT)

          .setBlockModes(KeyProperties.BLOCK_MODE_CBC)

          .setUserAuthenticationRequired(true)

          .setEncryptionPaddings(

              KeyProperties.ENCRYPTION_PADDING_PKCS7)

          .build());

      keyGenerator.generateKey();


    } catch (KeyStoreException | IOException | CertificateException

        | NoSuchAlgorithmException | InvalidAlgorithmParameterException

        | NoSuchProviderException e) {


      e.printStackTrace();


    }


  }
```

```
   @TargetApi(Build.VERSION_CODES.M)

   public boolean cipherInit() {

      try {

         cipher = Cipher.getInstance(KeyProperties.KEY_ALGORITHM_AES + "/" +
KeyProperties.BLOCK_MODE_CBC + "/" +
KeyProperties.ENCRYPTION_PADDING_PKCS7);

      } catch (NoSuchAlgorithmException | NoSuchPaddingException e) {

         throw new RuntimeException("Failed to get Cipher", e);

      }




      try {


         keyStore.load(null);


         SecretKey key = (SecretKey) keyStore.getKey(KEY_NAME,

               null);


         cipher.init(Cipher.ENCRYPT_MODE, key);


         return true;


      } catch (KeyPermanentlyInvalidatedException e) {

         return false;

      } catch (KeyStoreException | CertificateException | UnrecoverableKeyException
| IOException | NoSuchAlgorithmException | InvalidKeyException e) {

         throw new RuntimeException("Failed to init Cipher", e);

      }
```

```
    }
}
```



FingerprintAuthApp

Fingerprint Authentication

You can now access the app.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

In this project, we have fashioned a program to generate an OTP with PHP, a rudimentary website to take data to be verified using apache-server, a database to store user login data, created using MySQL on XAMPP, and another application that can take biometric images from the user through his or her smartphone fingerprint sensor to be authenticated with the corresponding OTP digit.

Once we have permission to use the fingerprint sensor on the smartphone to take biometric images for authenticating the user with the corresponding digit of the OTP upon successful authentication, the app will post a response to the website; for this happen, we need to run the app and website on a server continuously for which we do not have the adequate resources as of right now. We could not find a free messenger API to send the generated OTP that we could use.

The presented model can be further improved by increasing security measures like limiting or restricting authentication to specific pre-registered personal devices of the user.

CHAPTER 8

REFERENCES

[1]Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez and Javier Ortega.“ Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits ”

[2]JesudossA,Subramaniam.P(2014),“A SURVEY ON AUTHENTICATION ATTACKS AND COUNTERMEASURES IN A DISTRIBUTED ENVIRONMENT”In the Indian Journal of Computer Science and Engineering (IJCSE)”

[3]https://economictimes.indiatimes.com/definition/authentication

[4]https://en.wikipedia.org/wiki/One-time_password

[5]https://searchsecurity.techtarget.com/definition/one-time-password-OTP
[6]https://blog.identityautomation.com/two-factor-authentication-2fa-explained-email-and-sms-otps

[7]https://www.onelogin.com/learn/otp-totp-hotp#:~:text=There%20are%20two%20types%20of%20OTP%3A%20HOTP%20and%20TOT

[8]https://medium.com/@tapasfun/list-of-top-sms-apis-to-send-bulk-sms-otp-sms-worldwide-updated-on-2020-19abc955998b

[9]https://docs.jboss.org/picketlink/2/latest/reference/html/sect-The_Authentication_Process.html

[10] https://maraphones.com/blog/is-face-recognition-safer-than-a-fingerprint/

[11]https://cybernews.com/privacy/fingerprint-vs-face-id-which-is-safer/

[12]https://biometrictoday.com/25-advantages-disadvantages-iris-recognition/

[13]https://www.bayometric.com/iris-recognition-scanners-vs-fingerprint-scanners/

[14]https://www.cgdev.org/blog/iris-recognition-better-fingerprints-and-falling-price

[15]https://www.androidauthority.com/how-fingerprint-scanners-work-670934/amp/

[16]https://dl.acm.org/doi/abs/10.1145/3190618

[17]https://ieeexplore.ieee.org/abstract/document/8835065

[18]https://ieeexplore.ieee.org/abstract/document/9086771

[19]https://www.mdpi.com/2073-8994/11/2/141

[20]https://www.sciencedirect.com/science/article/abs/pii/S0031320319301694