A Project Report
on

E-Authentication System in banking to Allow multiple identities

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

BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE & ENGINEERING

Under the Supervision of

Janarthanan.S

Assistant Professor

Submitted By:

Ritwik Sinha

19SCSE1010400

Madhav Kumar

19SCSE1010033

IN

SCHOOL OF COMPUTING SCIENCE & ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING GALGOTIAS UNIVERSITY, GREATER NOIDA INDIA

DECEMBER 2021

ACKNOWLEDGEMENT

Janarthanan.S, for their valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of our project.

We deeply express our sincere thanks to our Head of Department for encouraging and allowing us to present the project on the topic "E-**Authentication System in baking to Allow multiple identities**" at our department SCSE for the partial fulfillment of the requirements leading to the award of BTech Degre.

We pay our respects and love to our parents and all other family members and friends for their love and encouragement throughout our career. Last but not the least we express our thanks to our friends for their cooperation and support.

1. RITWIK SINHA
   19SCSE1010400

2. MADHAV KUMAR
   19SCSE1010033

ABSTRACT

With the growing population people are working and making money and saving in the personal bank accounts but the problem is that we have not the proper secure system by which we can authenticate users to particular dashboard. Currently whenever a user signs up to any secure portal and after login he/she will navigate to proper dashboard. But what if the password got hacked by decrypt module in programming language, this can be led to delete the user dashboard, account or some important documents.For navigation users to particular dashboard and with a advanced system we can make this happen. We are goanna developing a portal where user should sign up and login, after signing up and logging up theuser will be redirected to a page where we gave him/her two options, the first option will be otp generationand the second will be QR Code generation. If he/her chooses for OTP them he/she has to give that phonenumber which was used at the time of sign up and if/she chooses for qr code generation then he/she has to give that email id which was given at the time of sign up.We are goanna using React, CSS and JavaScript to develop the user interface and after that we are goannamaking backend using firebase and we have a module in react called qr code generator by which we are goanna implementing that feature in that. After getting backend done, we should host the application on Heroku, netlify etc. So that everyone can access it.

CHAPTER NO. **Table of Contents**

	Abstract
1	Introduction
1 .1History	
	Objective of the project
	Use of the project
2	Theoretical Background
	2.1 Intro to E-Authentication
	2.2Methodology
3	System Analysis and planning
	3.1 steps in requirement analysis process
4	System Design
	flow chart
	data flow diagram
	Activity diagram
5	System Implementation Details
	5.1 Modules
6	Conclusion and suggestion
	Reference

CHAPTER-1
INTRODUCTION

HISTORY:

The need for authentication has been prevalent throughout history. In ancient times, people would identify each other through eye contact and physical appearance. The Sumerians in ancient Mesopotamia attested to the authenticity of their writings by using seals embellished with identifying symbols. As time moved on, the most common way to provide authentication would be the handwritten signature.

OBJECTIVE OF THE PROJECT

The main purpose of our E-authentication system using QR codes and OTP is to provide secured login systems which also performs online transactions.This system is basically aimed to provide the customer the system more compliable for the imposters and more reliable for the users, by using the electronic authentication approach.The objective of our project is to come up with banking website and online shopping website that implement and demonstrate how QR codes and OTP can be used with encryption algorithms to ensure data security as it provides dual security.

USE OF THE PROJECT

In the proposed scheme, the user can easily and efficiently login into the system. We analyse the security and usability of the proposed scheme, and show the resistance of the proposed scheme to hacking of login credentials, shoulder surfing and accidental login. The shoulder surfing attack can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. Since, we have come up with a secure system scheme with different degrees of resistance to shoulder surfing have been proposed. In order to use this authentication system, user need to first register himself into this system by filing up the basic registration details. After a successful registration, user can access the login module where he/she need to first authenticate the account by entering the email id and password which was entered while registration. Once the email id and password is authenticated, the user may proceed with next authentication section where he/she need to select the type of authentication as QR (Quick Response) Code or OTP (One Time Password). Once the user selects the authentication type as QR Code, then system will generate a QR Code and send it to user's mail id over internet. If user select's OTP, then SMS will be sent on his/her registered mobile number. If the user passes the authentication, then system will redirect to the main page. The QR Code and OTP are randomly generated by the system at the time of login.One of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders.Psychology studies have revealed that the human brain is better at recognizing and recalling graphical images than text Computer security systems must also consider the human factors such as ease of use and accessibility Current secure systems suffer because these mostly ignore the importance of human factors in security.An ideal security system considers security, reliability, usability, and human factors. All current security systems have flaws which make them specific for well trained and skilled users only.We analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to hacking of login credentials, shoulder surfing and accidental login.The shoulder surfing attack can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. Since, we have come up with a secure system scheme with different degrees of resistance to shoulder surfing have been proposed.In order to use this authentication system, user need to first register himself into this system by filing up the basic registration details.After a successful registration, user can access the login module where he/she need to first authenticate the account by entering the email id and password which was entered while registration.Once the email id and password are authenticated, the user may proceed with next

authentication section where he/she need to select the type of authentication as QR (Quick Response) Code or OTP (One Time Password).Once the user selects the authentication type as QR Code, then system will generate a QR Code and send it to user's mail id over internet.If user selects OTP, then SMS will be sent on his/her registered mobile number. If the user passes the authentication, then system will redirect to the main page. The QR Code and OTP are randomly generated by the system at the time of login

CHAPTER-2
THEORETICAL BACKGROUND

Introduction to E-Authentication

Despite of wide use of current e-authentication system, it has many security holes as it's based on traditional password-based model, no mutual authentication between user and bank server which leads to threats like phishing (stealing passwords and using them for transactions), intercepting communication lines, database hacking, etc. To make transactions more secure but also keeping them easy for user, following authentication system can be useful.In our proposed scheme, we assume the secure communication between the user (PC) service providers and service provider's certification authority.The proposed authentication system ensures the user authentication and digital signatures using authorized certificates by using https communication between user and server.Using user's transfer information (TI), requested transfer time (T) and the serial number (SN) of user's mobile device instead of security card, we generate QR-code, display it on user screen and decode it with user's mobile device to generate OTP. OTP is generated on server side also and OTP generated by user device and by server are verified to proceed. User database should also be encrypted to prevent data leakage.The authentication process of proposed system. Shown below:

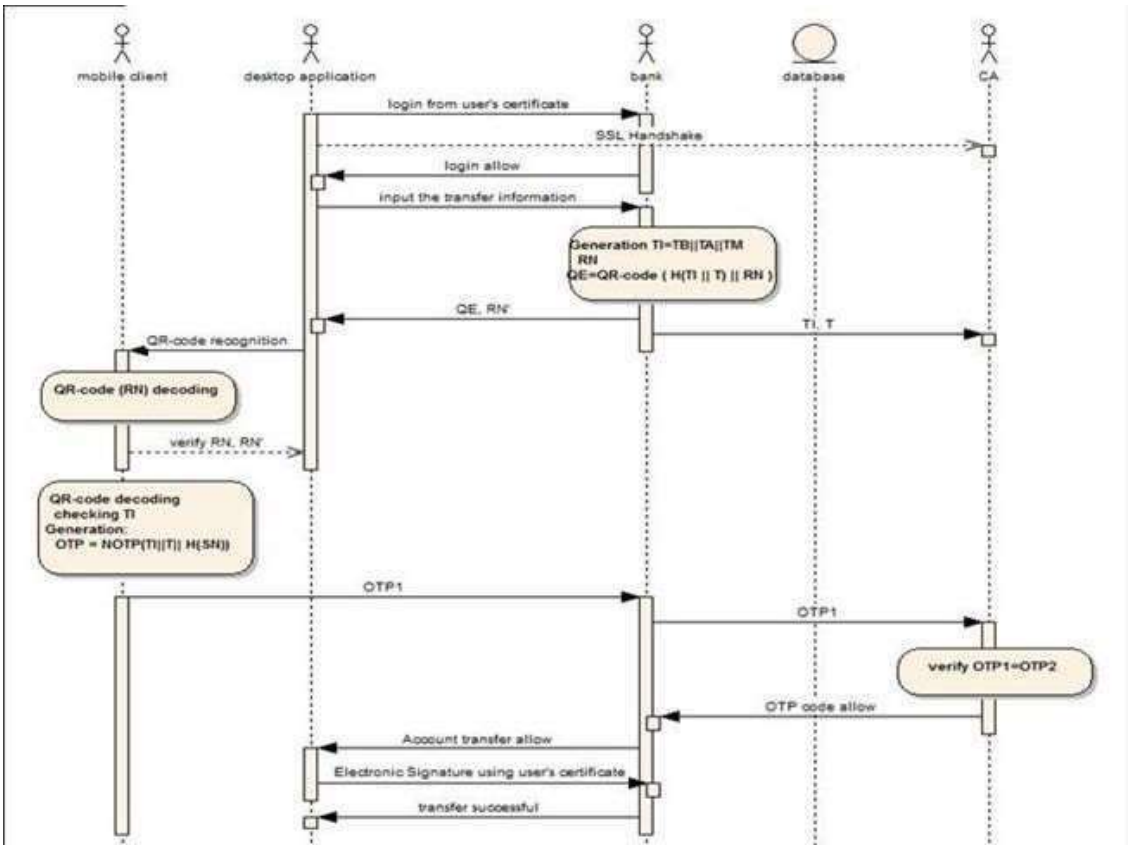


Fig.. Working scenario for e-authentication system

Methodology

As we know, number of Internet users are increasing drastically. Now, people are using different online services provided by banks, colleges/schools, hospitals, online utility, bill payment and online shopping sites. To access online services, text-based authentication system is in use. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. The core element of computational trust is identity. The aim of the paper is to make the system more compliable for the imposters and more reliable for the users, by using the graphical authentication approach. In this paper, we are using the more powerful tool of encoding the options in graphical QR format and also there will be the acknowledgment which will send to the user's mobile for final verification. The main methodology depends upon the encryption option and final verification by confirming a set of pass phrase on the legal users, the outcome of the result is very powerful as it only gives the result at once when the process is successfully done. All processes are cross linked serially as the output of the 1st process, is the input of the 2nd and so on. The system is a combination of recognition and pure recall-based technique. Presented scheme is useful for devices like PDAs, iPod, phone etc. which are handier and more convenient to use than traditional desktop computer systems.

CHAPTER-3

SYSTEM ANALYSIS AND PLANNING

System analysis and design refers to the process of examining a business situation with the intent of improving it through better procedure and method. System development can generally be thought of as having two major components: -System analysis and system design.

System design is a process of planning a new system or replace or complement an existing system. But before this planning can be done, we must thoroughly understand the existing system and determine how computer can best be used to make its operation more effective. System analysis, then, is the process of gathering and interpreting facts, diagnosing problems and using the information to recommend improvement to the system

3.1. Steps in Requirement Analysis Process

1. Fix system boundaries
2. Identify the customer
3. Requirement
4. Elicitation
5. Requirement analysis
6. process Requirement's
7. specification
8. Requirement
9. management

CHAPTER-4
SYSTEM DESIGN

Software design is a process of problem solving and planning for a software solution. After the purpose and specifications of software are determined, software developers build design or employ designers to develop a plan for a solution. It includes low-level component and algorithm implementation issues as well as the architectural view. Software design can be considered as putting solution to the problem(s) in hand using the available capabilities.Hence the main difference software analysis and design is that the output of the analysis of a software problem will be smaller problems to solve and it should deviate so much even if it is conducted by different team members or even by entirely different groups. But since design depends on the capabilities, we can have different designs for the same problem depending on the capabilities of the environment that will host the solution. The solution will depend also on the used development Environment.

USER-PROXY-based authentication is well-developed and widely used, and both are effective and efficient in user authentication [17], [19], [23], [40]. However, the growing theft of user certification from proxy-based verification and growing security requirements have prompted further verification [29], [55]. The central verification theme is to verify users using features that are internally connected to human users rather than certain external features [29]. A promising direction from this effort is biometrics [30]. Currently, the increased acceptance of biometrics is limited to the safety of users' biometric templates extracted from the biometric authentication process: they cannot be replaced once damaged, and actual biometric data can be reconstructed from biometric templates [10].

4.1 Flow Chart

A flowchart is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows. Process operations are represented in these boxes, and arrows; rather, they are implied by the sequencing of operations. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.The two most common types of boxes in a flowchart are:

- A processing step, usually called activity, and denoted as a rectangular box
- A decision usually denoted as a diamond.

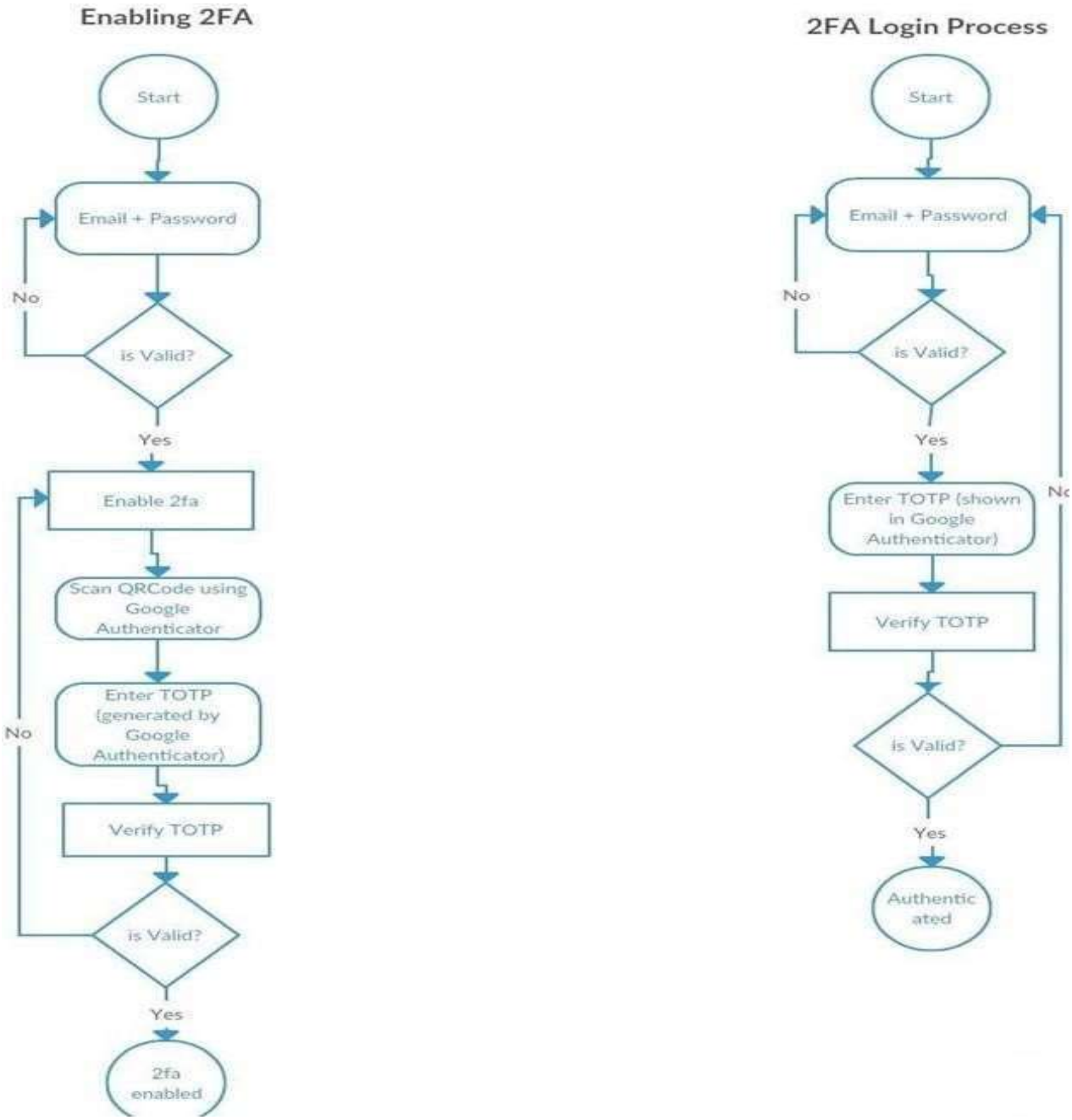


Fig: Flow Chart of E-Authentication Login Process

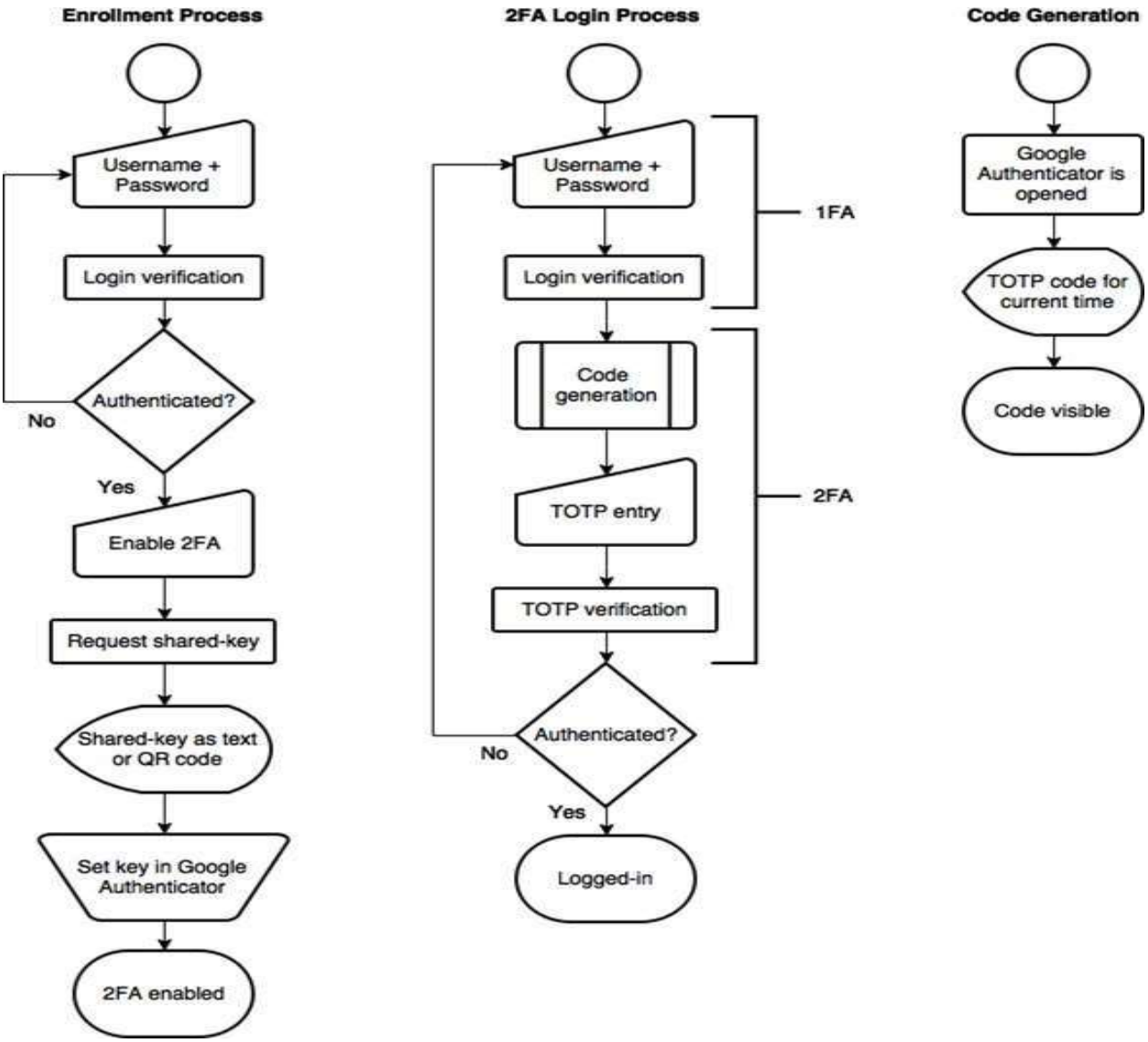
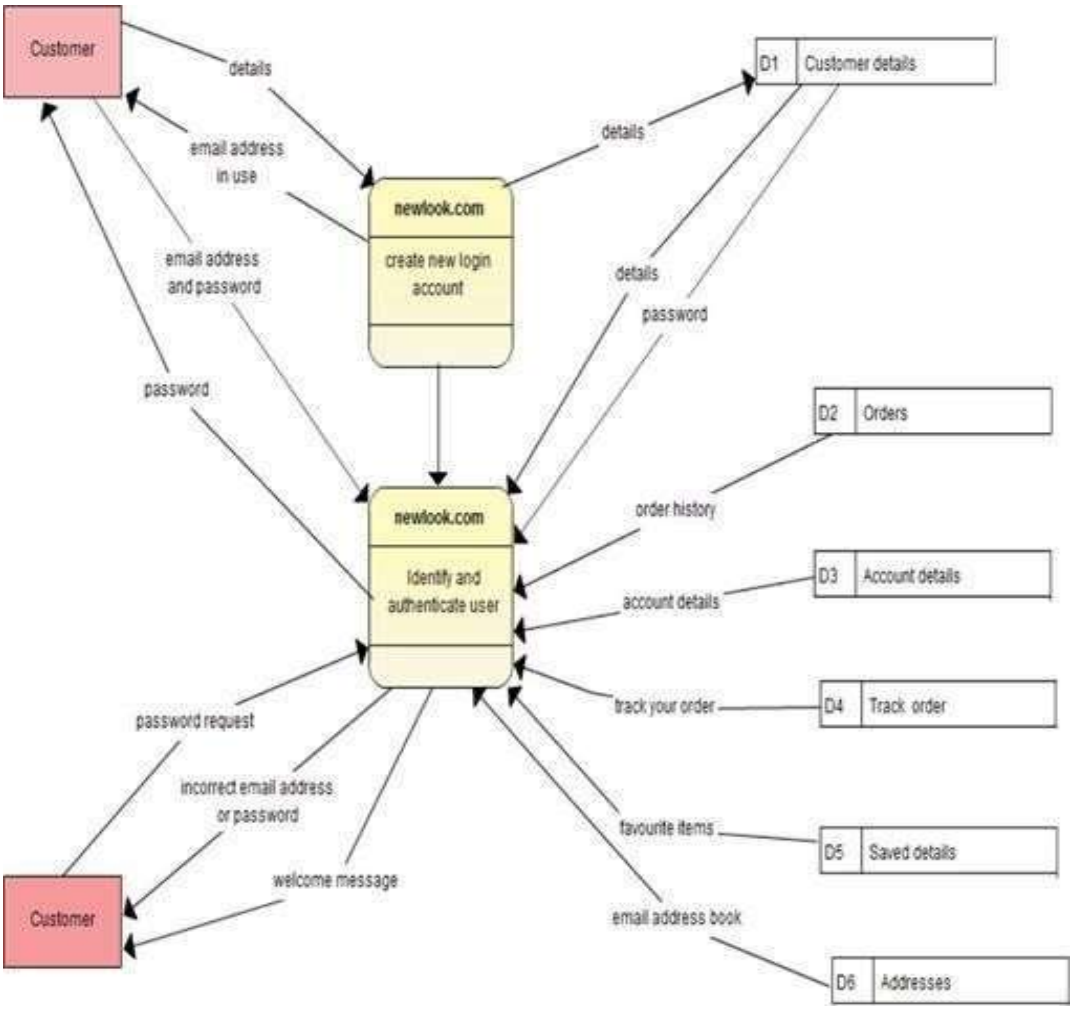


Fig: Flow Chart of E-Authentication Login and Code Generation Process

4.1 Data Flow Diagram

DFD is used to show how data flows through the system and the processes that transform the input data into output. Data flow diagrams are a way of expressing system requirements in a graphical manner. DFD represents one of the most ingenious tools used for structured analysis. It is also known as a bubble chart.

The DFD at simplest level is referred to as a CONTEXT ANALYSIS DIAGRAM. These are expended by level, each explaining its process in detail. Processes are numbered for easy identification and are normally labeled in block letters.



Activity Diagram

Activity diagrams are a loosely defined diagram technique for showing workflows of stepwise activities and actions, with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control. They consist of:

- Initial node.
- Activity final node.
- Activities

The starting point of the diagram is the initial node, and the activity final node is the ending.

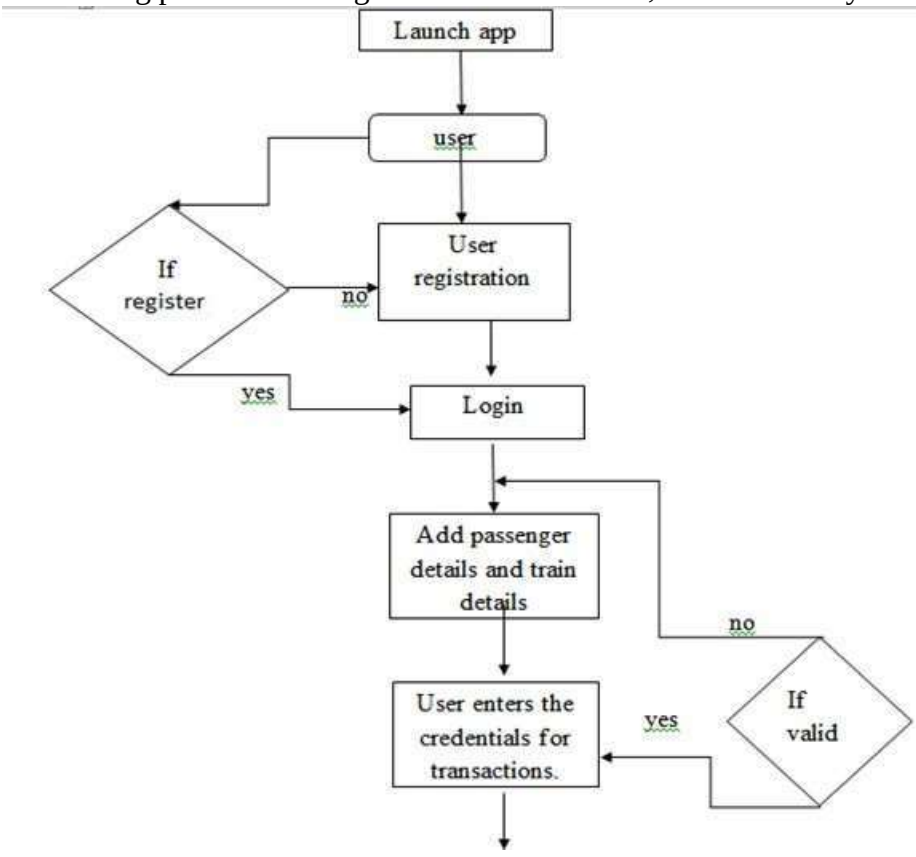


FIG-ACTIVITY DIGRAM

CHAPTER-5

SYSTEM IMPLEMENTATION DETAILS

MODULES:

This project contains following modules:

1. Registration
2. Login
3. OTP Verification
4. Scan QR codes
5. Main page access

MODULE DESCRIPTION:

REGISTRATION

To access the system, user need to first register by entering the basic registration details like name, email id, mobile number, gender, etc.

LOGIN

Here, user need to enter the login credentials to access the system.If the login credentials are validated by the system, the page will be redirected to user authentication page where user need to select any one authentication type as **OTP** or **QR Code.**

OTP VERIFICATION

If user select's OTP authentication, then system will send an OTP in the form of SMS on the registered mobile number which was provided by the user at the time of registration

SCAN QR CODE

If user select's QR code, then code is generated in backend and sent on the user's email id.User need to scan the QR Code using system webcam to validate the QR Code sent over the mail.

MAIN PAGE ACCESS

If the user passes the authentication process, then the page will be redirected to Main Page else, it will redirect to login page

6 Conclusions & Suggestions

In our project we have proposed a secure and reliable authentication scheme for net-banking through QR codes and OTPs. In recent years there has been a steep increase in the number of net-banking users.Hence the proposed system satisfies the high security requirements of the online users and protect them against various security attacks. Also, the system does not require any technical pre- requisite and this makes it very user friendly.Hence E-Authentication system proves to be versatile at the same time beneficial for both the customers in terms of security and for vendors in terms of increasing their efficiency. Hence it is most widely used to advertise and market the products by most businesses.OTPs are transmitted in the form of an image which makes it complex for intruder to detect the presence of secured information. OTP is sent to the concerned user through an email message. Net-banking users can conveniently access their email accounts and obtain the QR code containing the encrypted OTP. Hence under a secure transmission of the QR code it can only be interpreted by application software deployed by the bank with the QR image. Usage of AES algorithm for encrypting one-time password further enhances the security of the system. Proposed scheme has higher degree of complexity than all existing systems and clearly the time required to crack the scheme will be more than the useful lifetime of OTPs. OTPs are generated for a session and have a short lifetime. It's not possible to use the OTP after their expiry. Popularity of QR codes makes the method user friendly. Even a trivial user having basic understanding of using a computer system can adapt to it.

Reference

[1] http://ajast.net/data/uploads/4ajast-9.pdf

[2] http://ijesc.org/upload/15de67d580745fa9233dd990 6e322d67.QR%20Code%20Security%20and%20Soluti on.pdf

[3] http://academicscience.co.in/admin/resources/projec t/paper/f201405051399309076.pdf

[4] https://searchsecurity.techtarget.com/definition/onetime-password-OTP

[5] https://connect.cognex.com/India-Cognex-IndustrialBarcode-Readers-LP?src=0ebcb667-3333-e911-9137-00505693004d&cm_campid=0ebcb667-3333-e911- 913700505693004d&gclid=CjwKCAjwkPX0BRBKEiwA 7THxiL82xcb7QTpjhbnWReptsAWy_uGGwYQZ5XWEvt IipgKVdKuLHN-ihoCQ84QAvD_BwE

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

[7] https://en.wikipedia.org/wiki/Barcode

[8] https://ieeexplore.ieee.org/document/5711134

[9] http://en.wikipedia.org/wiki/Usability, 2013.

[10] http://iris.nist/gov/ice/, 2013.

[11] A. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 165-179, July/Sept. 2007.

[12] T. Boult, "Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens," Proc. Seventh

[13] E. Chang, R. Shen, and F. Teo, "Finding the Original Point set Hidden Among Chaff," Proc. ACM Symp. Information, Computer and Comm Security (ASIACCS '06), pp. 182-188, 2006. 914 IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 4, APRIL 2014

[14] K. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You, "Revealing the Secret of Facehashing," Proc. Int'l Conf. Advances in Biometrics, pp. 106-112, 2006.

[15] K. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H. Lam, "An Analysis on Accuracy of Cancellable Biometrics Based on Biohashing," Proc. Ninth Int'l Conf. Knowledge-Based Intelligent Information and Eng. Systems (KES '05), pp. 1168-1172, 2005.

[16] C. Chin, A. Jin, and D. Ling, "High Security Iris Verification System Based on Random Secret Integration," Computer Vision and Image Understanding, vol. 102, no. 2, pp. 169-177, May 2006.

[17] A. Ciaramella, P. D'Arco, A. De Santis, C. Galdi, and R. Tagliaferri, "Neural Network Techniques for Proactive Password Checking," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 327-339, Oct./Dec. 2006.

[18] J. Dai, J. Feng, and J. Zhou, "Robust and Efficient Ridge-Based Palmprint Matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 34, no. 8, pp. 1618-1632, Aug. 2012.

[19] P. D'Arco and A. De Santis, "On Ultralightweight RFID Authentication Protocols," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 4, pp. 548-563, July/Aug. 2011.

[20] J. Daugman, "How Iris Recognition Works," IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, Jan. 2004.

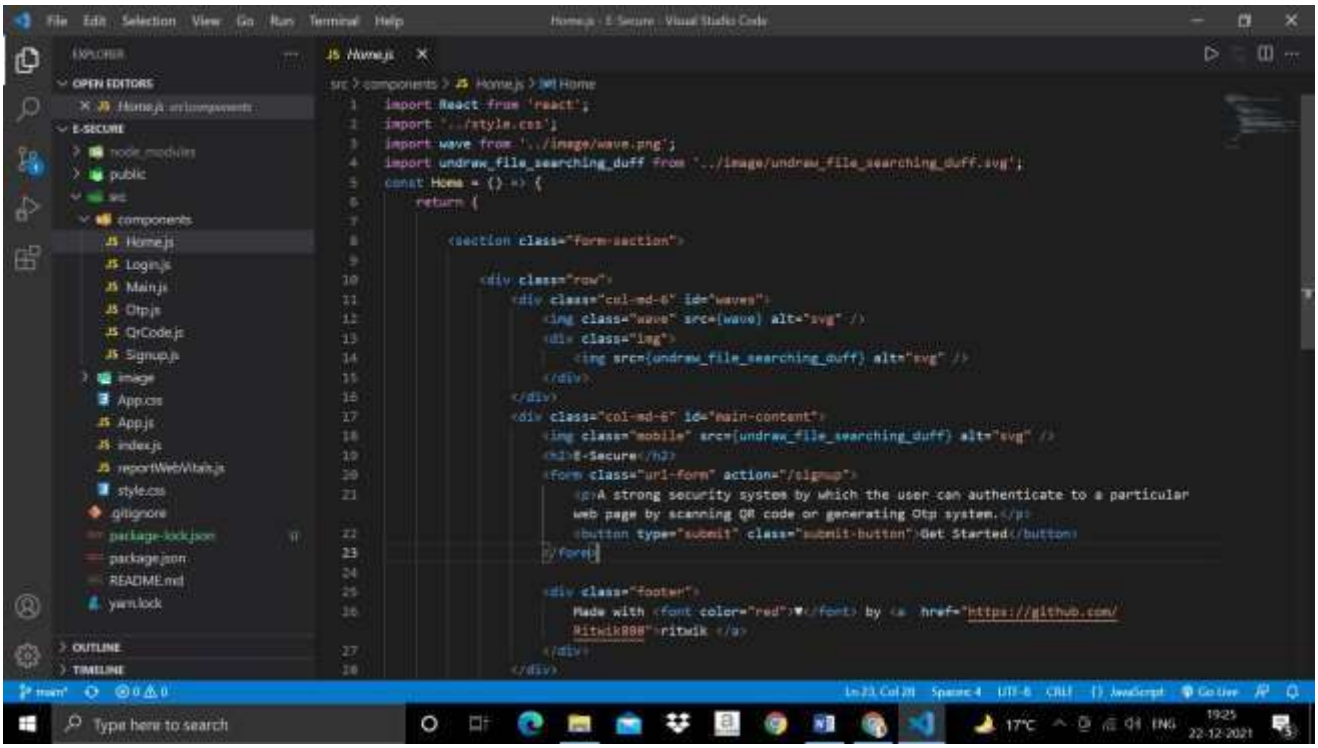
[21] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Advances in Cryptology (Eurocrypt), vol. 3027, pp. 523-540, 2004.

[22] Y. Du, R. Ives, D. Etter, and T. Welch, "Use of One-Dimensional Iris Signatures to Rank Iris Pattern Similarities," Optical Eng., vol. 45, no. 3, 2006.

[23] G. Duggan, H. Johnson, and B. Grawemeyer, "Rational Security: Modelling Everyday Password Use," Int'l J. Human-Computer Studies, vol. 70, no. 6, pp. 415-431, 2012.

[24] L. Faria, V. Sa, and S. de Magalhaes, "Multimodal Cognitive Biometrics," Proc. Sixth Iberian Conf. Information Systems and Technologies (CISTI), pp. 1-6, June 2011.

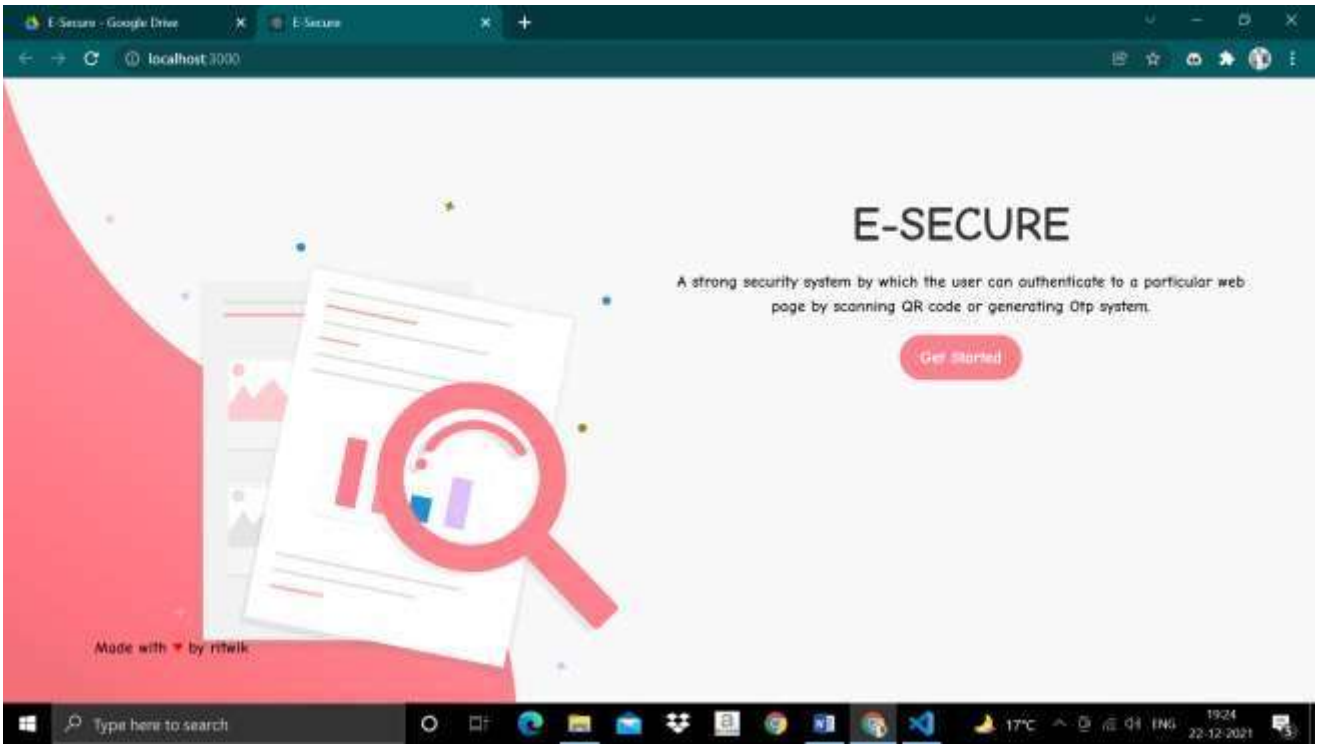
Source Code

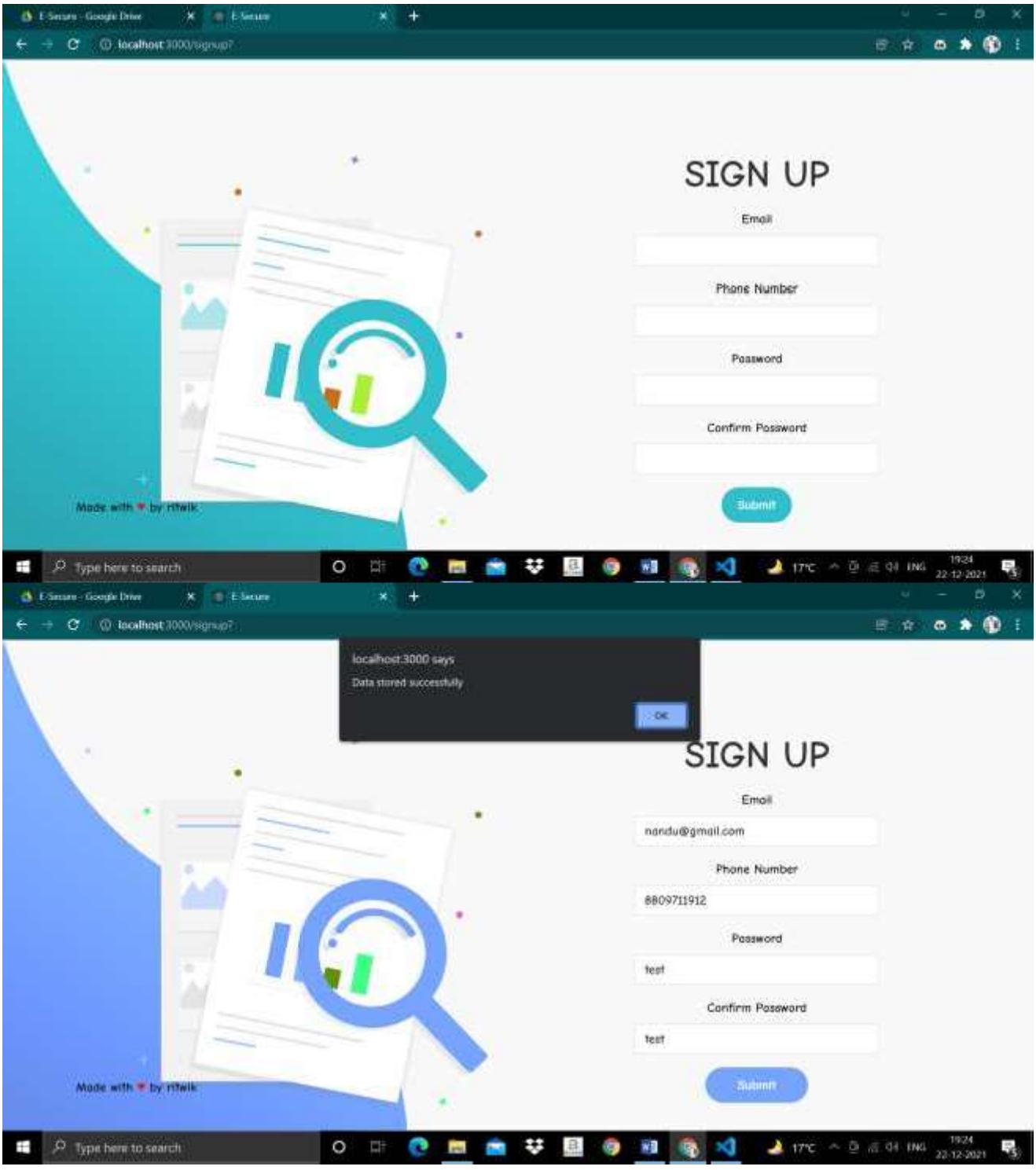

File Edit Selection View Go Run Terminal Help
Home.js - E-Secure - Visual Studio Code
EXPLORER
OPEN EDITORS
Home.js src\components
E-SECURE
node_modules
public
src
components
Home.js
Login.js
Main.js
Otp.js
QrCode.js
Signup.js
image
App.css
App.js
index.js
reportWebVitals.js
style.css
.gitignore
package-lock.json
package.json
README.md
yarn.lock
OUTLINE
TIMELINE
Home.js
src > components > Home.js > Home
import React from 'react';
import '../style.css';
import wave from '../image/wave.png';
import undraw_file_searching_duff from '../image/undraw_file_searching_duff.svg';
const Home = () => {
return (
<section class="form-section">

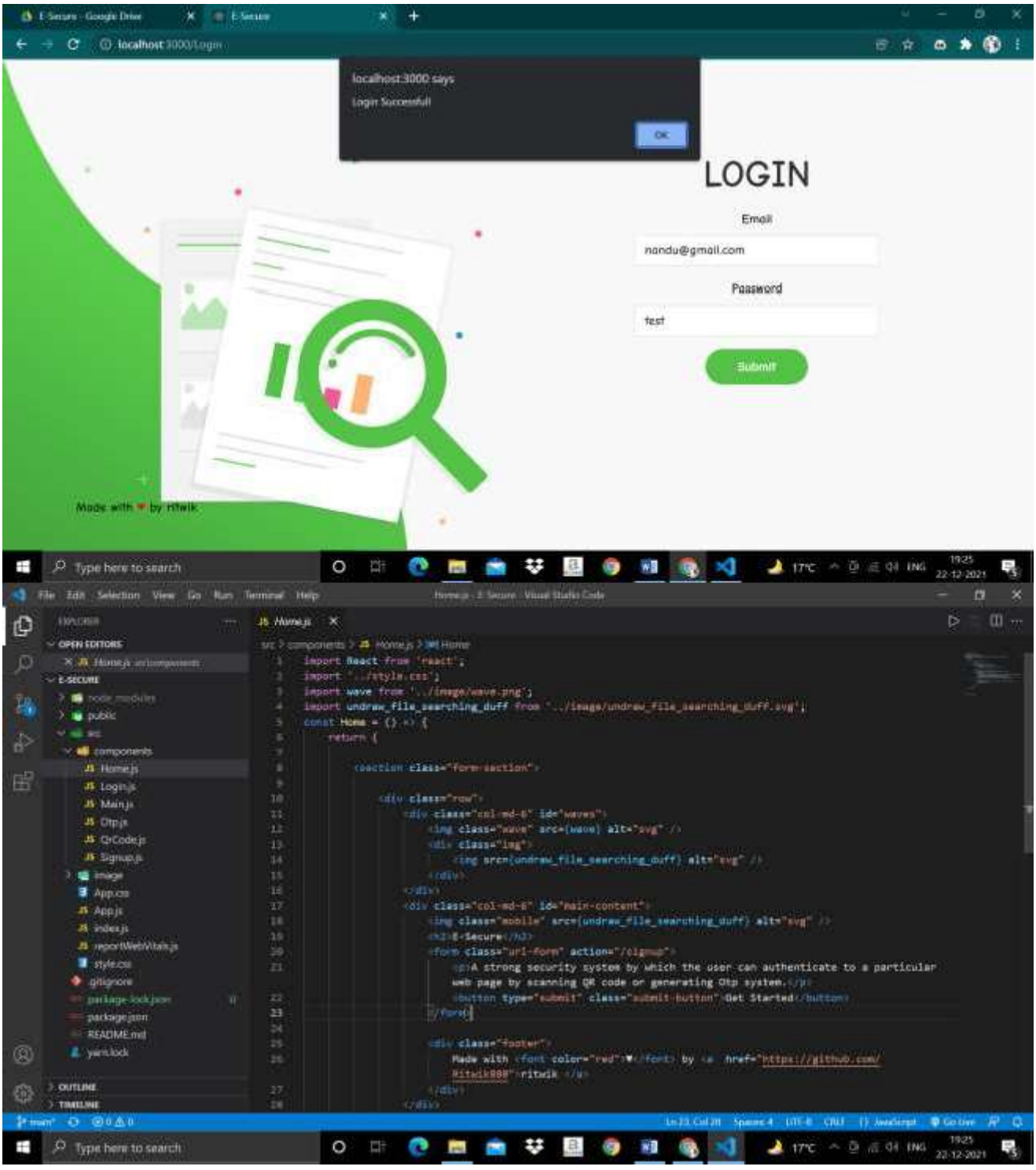
<h1>E-Secure</h1>
<form class="url-form" action="/signup">
A strong security system by which the user can authenticate to a particular
web page by scanning QR code or generating Otp system.
<button type="submit" class="submit-button">Get Started</button>
</form>

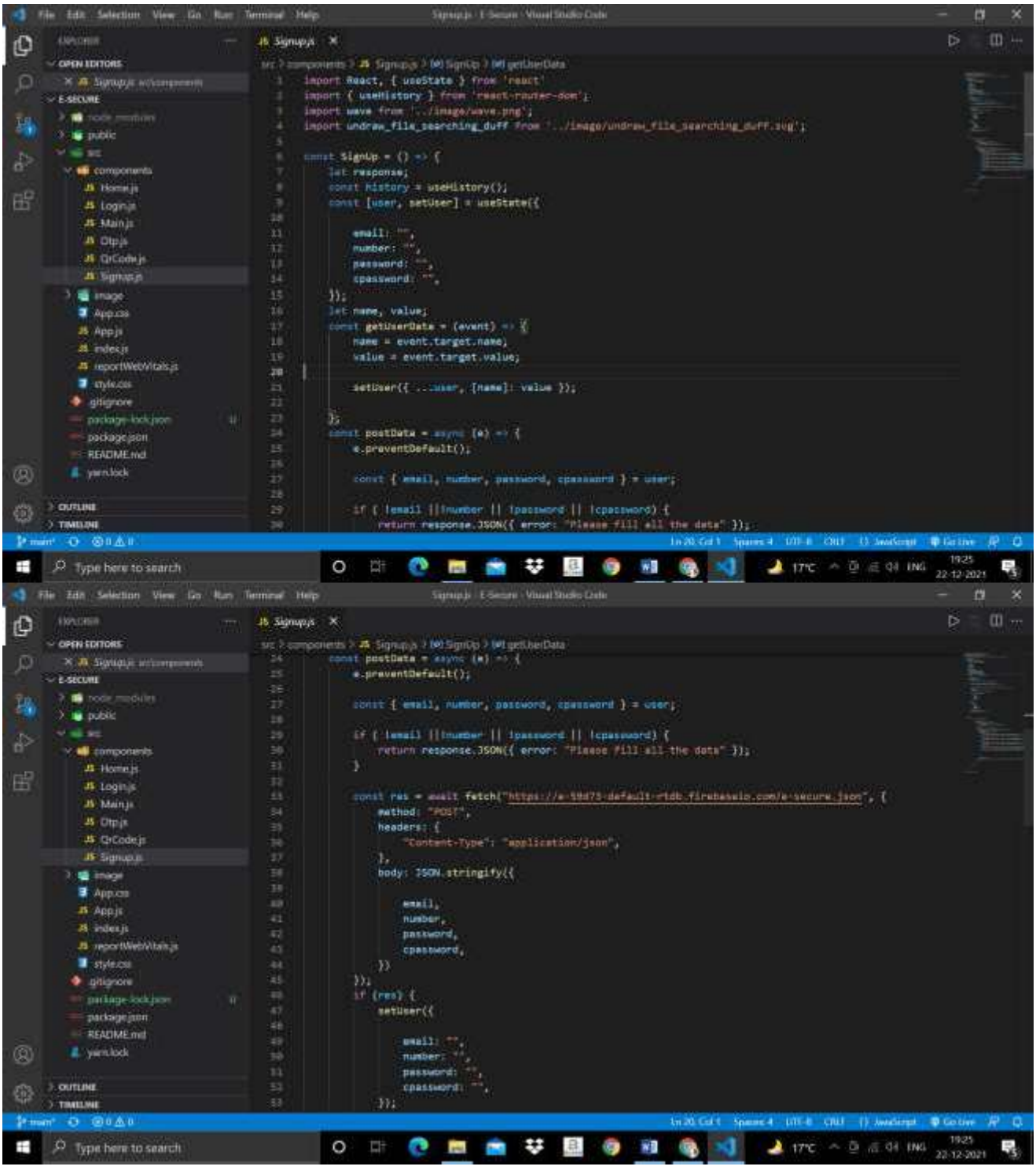
Made with ♥ by <a href="https://github.com/
Ritwik888">ritwik

Type here to search
17°C
ENG
19:25
22-12-2021

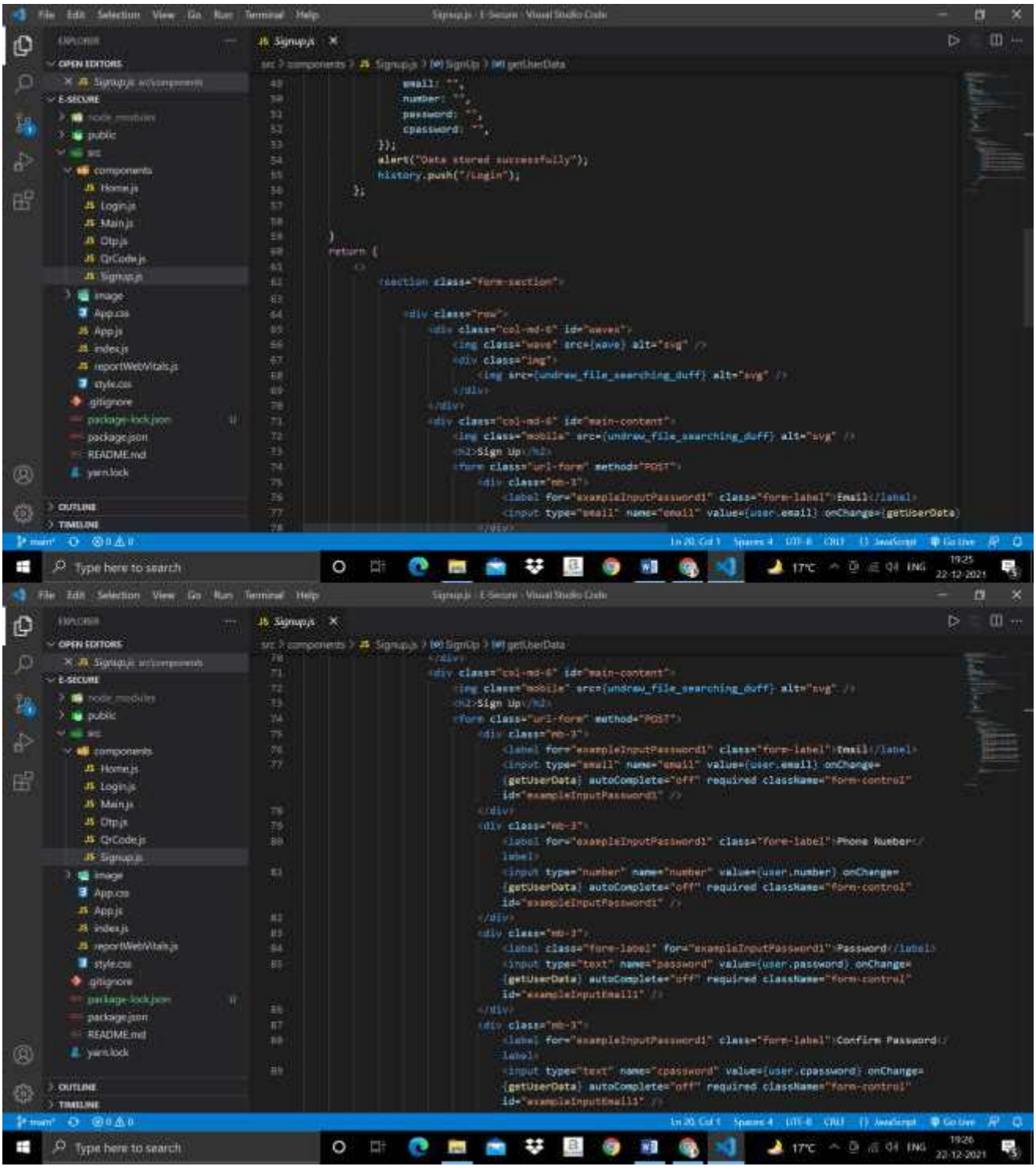

E-Secure - Google Drive
E-Secure
localhost:3000
E-SECURE
A strong security system by which the user can authenticate to a particular web page by scanning QR code or generating Otp system.
Get Started
Made with ♥ by ritwik
Type here to search
17°C
ENG
19:24
22-12-2021

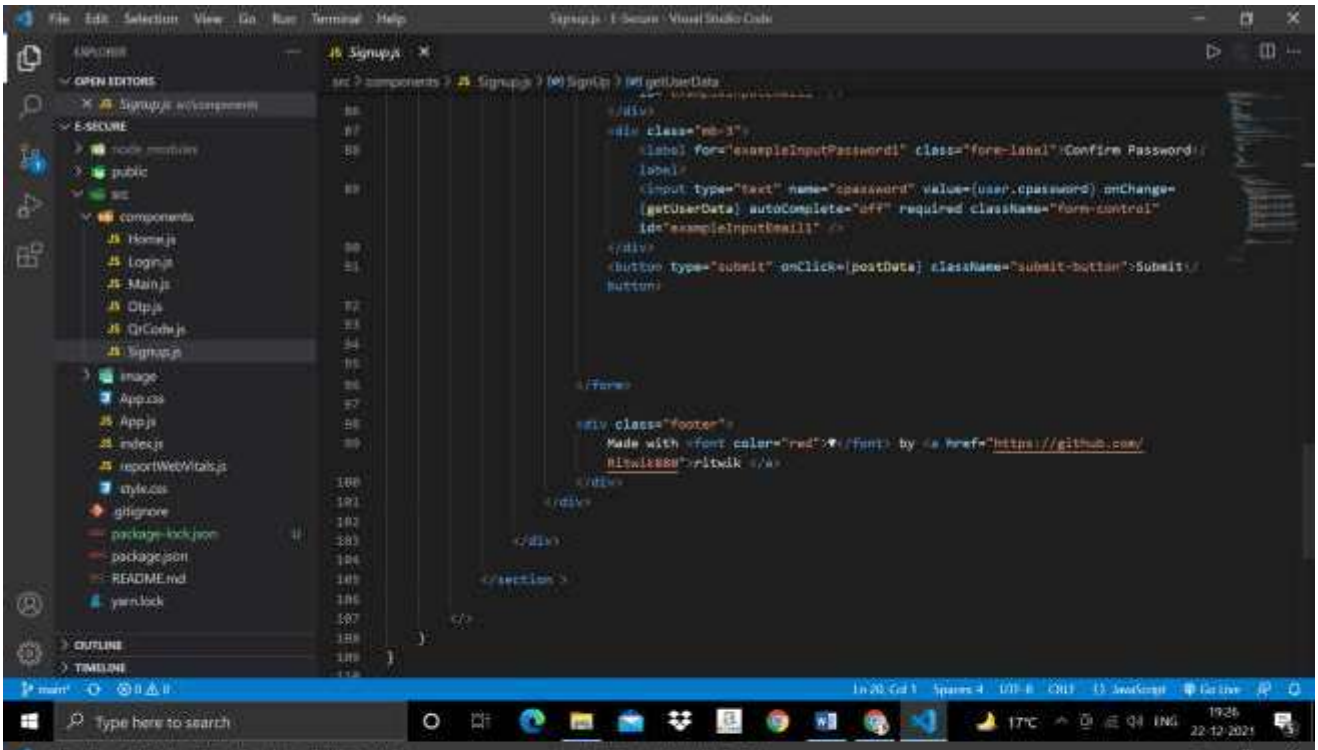

E-Secure - Google Drive
E-Secure
localhost:3000/signup?
SIGN UP
Email
Phone Number
Password
Confirm Password
Submit
Made with ♥ by ritwik
Type here to search
17°C
ENG
19:24
22-12-2021
localhost:3000 says
Data stored successfully
OK
SIGN UP
Email
nandu@gmail.com
Phone Number
8809711912
Password
test
Confirm Password
test
Submit
Made with ♥ by ritwik
Type here to search
17°C
ENG
19:24
22-12-2021

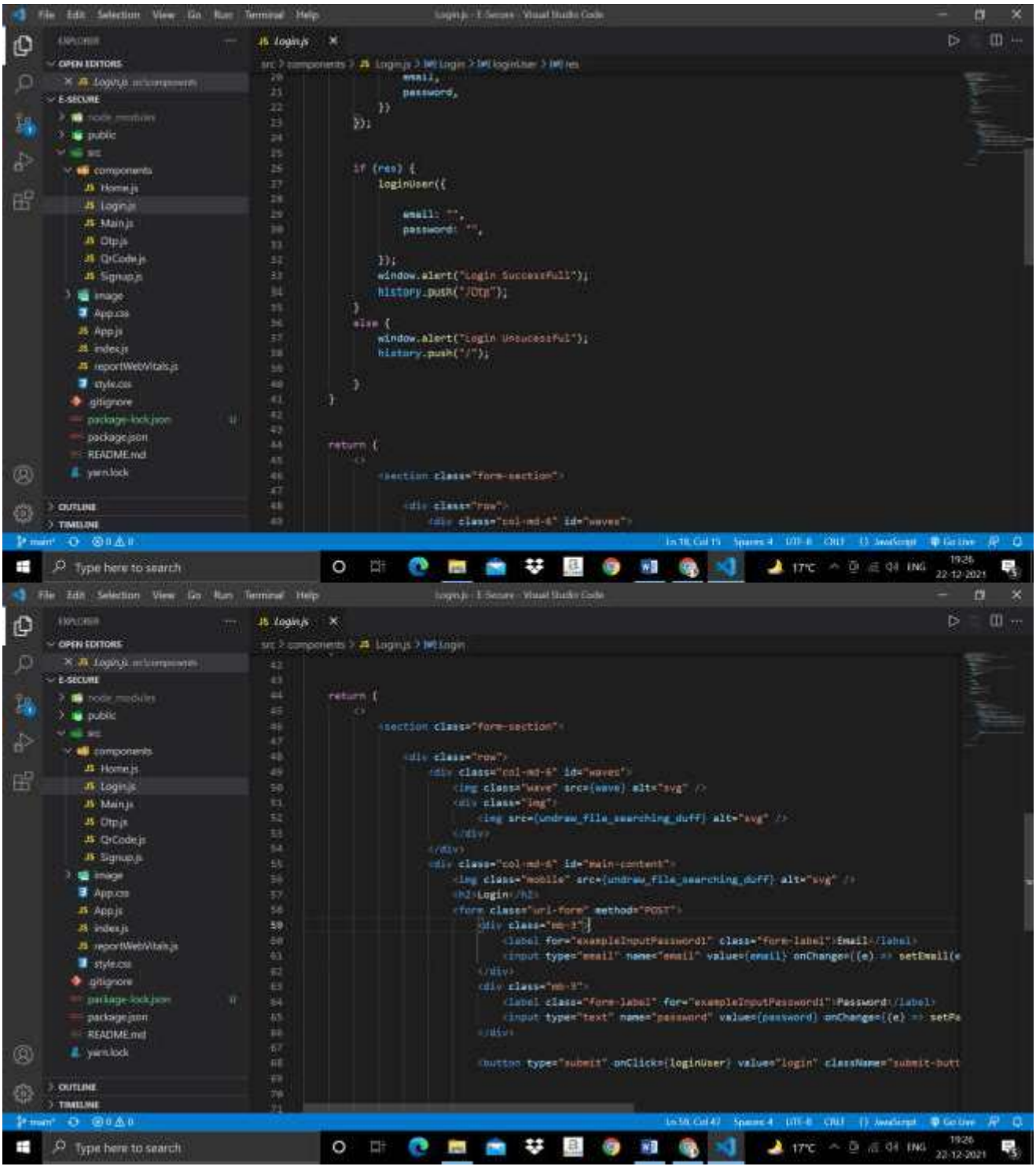

localhost:3000 says
Login Successfull
OK
LOGIN
Email
nandu@gmail.com
Password
test
Submit
Made with ♥ by ritwik


Signup.js - E-Secure - Visual Studio Code
Signup.js
src > components > Signup.js > getUserData
import React, { useState } from 'react'
import { useHistory } from 'react-router-dom';
import wave from '../image/wave.png';
import undraw_file_searching_duff from '../image/undraw_file_searching_duff.svg';
const SignUp = () => {
let response;
const history = useHistory();
const [user, setUser] = useState({
email: "",
number: "",
password: "",
cpassword: "",
});
let name, value;
const getUserData = (event) => {
name = event.target.name;
value = event.target.value;
setUser({ ...user, [name]: value });
};
const postData = async (e) => {
e.preventDefault();
const { email, number, password, cpassword } = user;
if (!email ||!number || !password || !cpassword) {
return response.JSON({ error: "Please fill all the data" });
Type here to search
17°C
ENG
19:25
22-12-2021

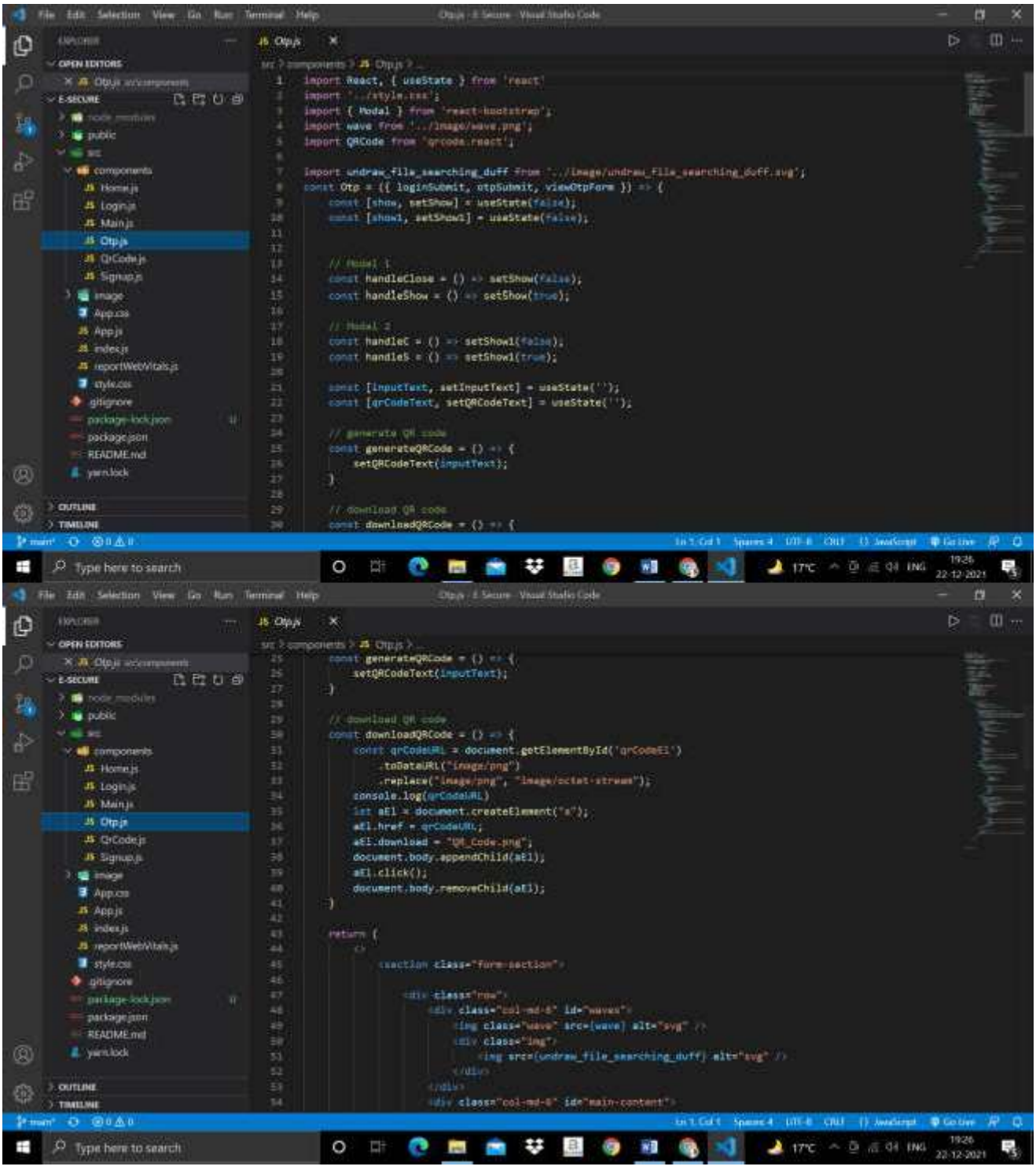
Signup.js - E-Secure - Visual Studio Code
Signup.js
src > components > Signup.js > getUserData
const postData = async (e) => {
e.preventDefault();
const { email, number, password, cpassword } = user;
if (!email ||!number || !password || !cpassword) {
return response.JSON({ error: "Please fill all the data" });
}
const res = await fetch("https://e-59d75-default-rtdb.firebaseio.com/e-secure.json", {
method: "POST",
headers: {
"Content-Type": "application/json",
},
body: JSON.stringify({
email,
number,
password,
cpassword,
})
});
if (res) {
setUser({
email: "",
number: "",
password: "",
cpassword: "",
});
Type here to search
17°C
ENG
19:25
22-12-2021



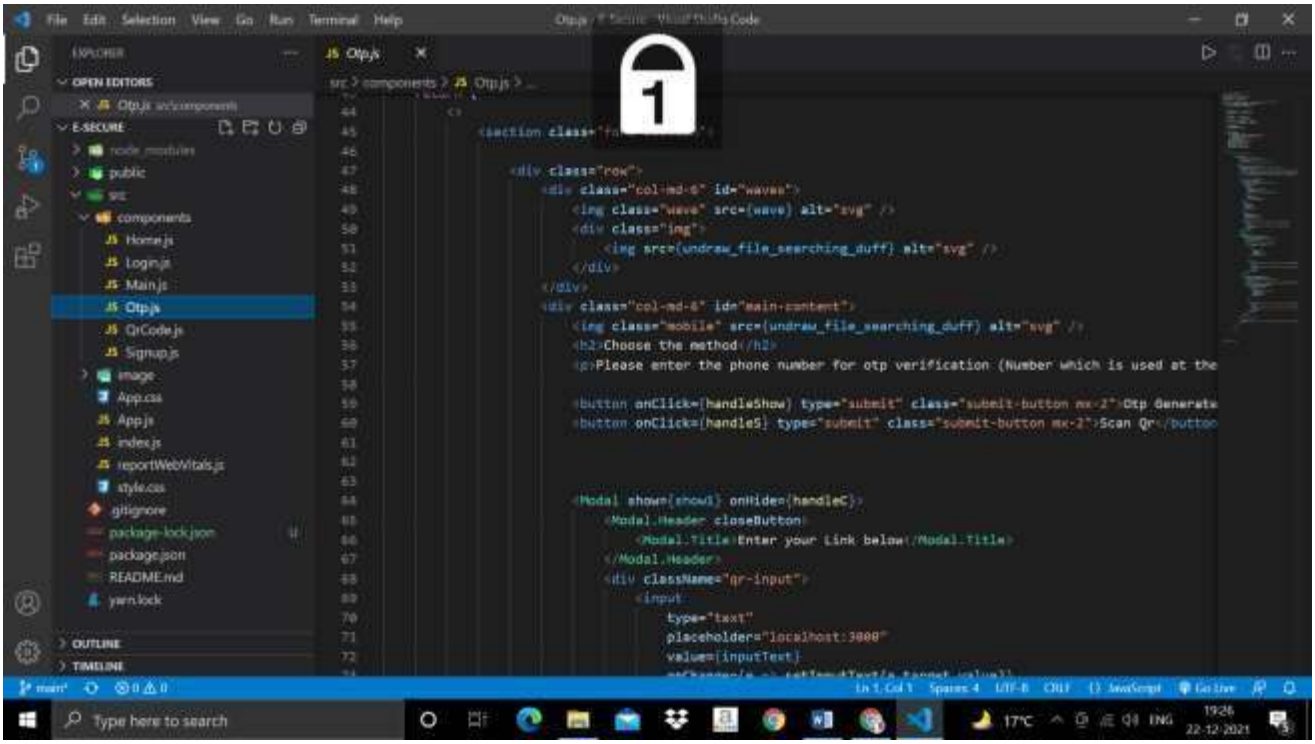

Signup.js
Login.js
Type here to search


Login.js
E-SECURE
OPEN EDITORS
components
Home.js
Login.js
Main.js
Otp.js
QrCode.js
Signup.js
image
App.css
App.js
index.js
reportWebVitals.js
style.css
.gitignore
package-lock.json
package.json
README.md
yarn.lock
OUTLINE
TIMELINE
email,
password,
});
if (res) {
loginUser({
email: "",
password: "",
});
window.alert("Login SuccessFull");
history.push("/Otp");
}
else {
window.alert("Login Unsucessful");
history.push("/");
}
}
return (
<section class="form-section">

<h2>Login</h2>
<form class="url-form" method="POST">
<label for="exampleInputPassword1" class="form-label">Email</label>
<label class="form-label" for="exampleInputPassword1">Password</label>
<input type="text" name="password" value={password} onChange={(e) => setPa
<button type="submit" onClick={loginUser} value="login" class="submit-butt
Type here to search
17°C
ENG
19:26
22-12-2021


Otp.js
import React, { useState } from 'react'
import '../style.css';
import { Modal } from 'react-bootstrap';
import wave from '../image/wave.png';
import QRCode from 'qrcode.react';
import undraw_file_searching_duff from '../image/undraw_file_searching_duff.svg';
const Otp = ({ loginSubmit, otpSubmit, viewOtpForm }) => {
const [show, setShow] = useState(false);
const [show1, setShow1] = useState(false);
// Modal 1
const handleClose = () => setShow(false);
const handleShow = () => setShow(true);
// Modal 2
const handleC = () => setShow1(false);
const handleS = () => setShow1(true);
const [inputText, setInputText] = useState('');
const [qrCodeText, setQRCodeText] = useState('');
// generate QR code
const generateQRCode = () => {
setQRCodeText(inputText);
}
// download QR code
const downloadQRCode = () => {
const qrCodeURL = document.getElementById('qrCodeEl')
.toDataURL("image/png")
.replace("image/png", "image/octet-stream");
console.log(qrCodeURL)
let aEl = document.createElement("a");
aEl.href = qrCodeURL;
aEl.download = "QR_Code.png";
document.body.appendChild(aEl);
aEl.click();
document.body.removeChild(aEl);
}
return (
<>
<section class="form-section">

Type here to search
17°C
ENG
19:26
22-12-2021


File Edit Selection View Go Run Terminal Help
Otp.js - E-SECURE - Visual Studio Code
EXPLORER
OPEN EDITORS
Otp.js src\components
E-SECURE
node_modules
public
src
components
Home.js
Login.js
Main.js
Otp.js
QrCode.js
Signup.js
image
App.css
App.js
index.js
reportWebVitals.js
style.css
.gitignore
package-lock.json
package.json
README.md
yarn.lock
OUTLINE
TIMELINE
Otp.js
src > components > Otp.js > ...
<section class="

<h2>Choose the method</h2>
<p>Please enter the phone number for otp verification (Number which is used at the
<button onClick={handleShow} type="submit" class="submit-button mx-2">Otp Generate
<button onClick={handleS} type="submit" class="submit-button mx-2">Scan Qr</buttoo
<Modal shown={show1} onHide={handleC}>
<Modal.Header closeButton>
<Modal.Title>Enter your Link below</Modal.Title>
</Modal.Header>

<input
type="text"
placeholder="localhost:3000"
value={inputText}
Ln 1, Col 1 Spaces: 4 UTF-8 CRLF {} JavaScript Go Live
Type here to search
17°C ENG 19:26 22-12-2021