INTRODUCTION

1. INTRODUCTION

1.1 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 hand written signature.

1.2 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 with data optimization.

1.3 SCOPE OF THE PROJECT

- E-Authentication system revolutionizes web site login and authentication. It eliminates many problems inherent in traditional login techniques.
- It is more secure as it involves AES encryption technique and it is easy to use, also gives freedom from remembering so many username and password for different websites.
- The simple and straight forward E-Authentication system yields a surprising array offeatures and benefits and can be used in various applications like e-commerce, e-retail, e-booking, e-learning and many more.
- The internet has made electronic authentication an almost effortless task.

1.4 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 schemes 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 schemes 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 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.

LITERATURE SURVEY

2.LITERATURE SURVEY

2.1 LITERATURE SURVEY

The literature on e-authentication systems employing QR codes and OTPs explores their integration, security, usability, and effectiveness across various domains. QR codes, known for their efficiency in encoding data and ease of use, are utilized in authentication processes to enable secure login and transaction verification. Studies address security challenges such as QR code spoofing and interception through cryptographic techniques like encryption and digital signatures, ensuring data integrity and user trust. Usability research focuses on user acceptance and accessibility, highlighting improvements in user experience and system accessibility for diverse user groups.

On the other hand, OTPs are crucial in providing dynamic and time-sensitive passwords, often delivered via SMS or dedicated mobile applications. They serve as a second factor in multi-factor authentication systems, enhancing security by requiring users to authenticate with a temporary password alongside their regular credentials. Research underscores OTP security standards compliance and the effectiveness of OTPs in mitigating risks associated with static passwords. Integration studies explore hybrid approaches that combine QR codes for initial authentication with OTPs for transaction verification, offering robust security synergies. Overall, while these systems offer significant advancements in e-authentication, ongoing research addresses challenges and explores innovative solutions to enhance their reliability, security, and user acceptance in diverse application contexts.

2.2 OVERVIEW OF E-AUTHENTICATION SYSTEM

An e-authentication system utilizing QR codes and OTP (One-Time Passwords) combines convenience with security, catering to modern digital interactions. QR codes serve as a user-friendly entry point, often generated by the service provider and scanned by the user's device equipped with a camera. This method eliminates manual entry errors and streamlines the authentication process. Once scanned, the system prompts for an OTP, typically sent via SMS, email, or generated by an authenticator app. OTPs ensure a second layer of security by providing a temporary code that expires shortly after issuance, thwarting unauthorized access attempts. Together, QR codes and OTPs create a robust authentication framework suitable for various applications, from online transactions to accessing secure systems, balancing usability with stringent security protocols in the digital landscape.

2.3 QR CODE BASED AUTHENTICATION

QR code-based authentication systems have become increasingly popular in e-authentication due to their convenience and security features. These systems typically utilize a combination of OTP (One-Time Password) and QR code technology to verify user identity. In such systems, a user initiates the authentication process by requesting access to a service or platform. They are then prompted to enter their credentials along with an OTP generated either by an authenticator app or sent via SMS. Simultaneously, a QR code containing encrypted authentication details is generated and displayed on the screen.The user scans this QR code using a mobile device equipped with a QR code reader. The scanned data, including the OTP, is decrypted and verified against the server's records. If the OTP matches and the credentials are valid, access is granted securely.This method offers several advantages. Firstly, it enhances security by requiring both something the user knows (credentials) and something they have (mobile device with QR code scanner). Secondly, it simplifies the authentication process for users, reducing the likelihood of human error in entering complex passwords. Additionally, QR codes can be time-sensitive, further enhancing security by limiting the validity period of the authentication session.Overall, QR code-based authentication with OTP integration provides a robust and user-friendly approach to secure e-authentication, making it a preferred choice for various online services and platforms.

2.4 OTP BASED AUTHENTICATION

In an OTP-based e-authentication system that incorporates QR code technology, users undergo a streamlined yet secure authentication process. Initially, users request access to a platform or service and are prompted to enter their credentials. Simultaneously, an OTP is generated either through an authenticator app or delivered via SMS to the registered mobile number. Alongside this OTP generation, a QR code containing encrypted authentication details is dynamically generated and displayed.To complete the authentication, users scan the QR code using a mobile device equipped with a QR code reader. The scanned data, including the OTP, is decrypted and validated against the server's records.

If the OTP matches and the credentials are verified, access is granted securely.This method offers significant advantages in terms of security and usability. It combines the strengths of OTPs, which provide a time-sensitive second factor of authentication, with the

ease and efficiency of QR code scanning. Users benefit from enhanced security due to the dual-factor authentication approach (something they know – the OTP, and something they have – access to the QR code on their mobile device). Moreover, the process minimizes the risk of credential theft and unauthorized access, ensuring robust protection for online services and platforms.Overall, OTP-based e-authentication systems utilizing QR codes represent a sophisticated yet user-friendly approach to securing access, meeting the evolving demands of digital security.

SYSTEM ANALYSIS

3.SYSTEM ANALYSIS

3.1 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.

3.2 EXISTING SYSTEM

In "A Secure Mobile Payment System using QR Code" paper, the authors proposed a state of affairs for mobile payment that tackles each considerations of the method, namely: speed of group action and security, while not complicating the method or creating it undesirable to users.

In the paper "QR-TAN: Secure Mobile Transaction Authentication, the authors contributed with the QR-TAN authentication technique. QR-tans area unit a dealing authentication technique supported two-dimensional bar codes. Compared to different established techniques, QR-tans show 3 advantages: initial, QR-tans enable the user to directly validate The content of a dealing among a sure device. Second,validation is secure notwithstanding associate offender manages to achieve full management over a user‟s laptop. Finally, QR-tans together with sensible cards may also be utilized for offline transactions that don't need any server

In the system "Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q-R Code", the authors explained implementation details of on-line banking authentication system. Security is associate vital issue for on-line banking application which might be enforced by varied web technologies. Whereas implementing on-line banking system, secure information transfer want is consummated by exploitation https information transfer and info encryption techniques for secure storage of sensitive info. To eliminate threat of phishing and to substantiate user identity we have a tendency to ar aiming to use conception of QR-code with robot application. QR-code which might be scanned by

user mobile device that overcome the weakness of ancient countersign based mostly system. We have a tendency to improve more security by exploitation only once countersign (OTP) that hides within QR- code.

3.2.1 LIMITATIONS OF EXISTING SYSTEM

- The most drawbacks is that data on the web may be haphazardly changed by malicious code.
- Easily hacked by Intruders/hackers.
- Very traditional method of using passwords or using complex passwords makes to store the data somewhere so it is mostly leakable to some other easily.
- Need to change the password in regular interval of time.

3.3 PROPOSED SYSTEM

In the proposed scheme, the user can easily and efficiently login into the system. 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 schemes 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 and OTP (One Time Password).

Once the user selects the authentication type, the use needs to upload the QR code and enter the OTP which is received in the email. If the user passes the authentication, then system will redirect to the main page and attendance is marked. The OTP is randomly generated by the system at every time of login.

3.4 FEASIBILITY STUDY

A feasibility study of an e-authentication system utilizing OTP (One-Time Password) and QR code technologies would assess various critical aspects to determine its practicality and viability. Firstly, the technical feasibility involves evaluating the capabilities of existing infrastructure and systems to integrate OTP generation, QR code processing, and secure transmission channels. This includes assessing compatibility with different platforms (e.g., mobile, web) and devices (smartphones, tablets, desktops) to ensure seamless functionality across diverse user environments.

Secondly, financial feasibility examines the costs associated with implementing and maintaining the system. This includes expenses related to hardware (e.g., QR code scanners, OTP generators), software (authentication servers, encryption mechanisms), and operational costs (maintenance, support). Cost-effectiveness analysis would weigh these expenditures against potential benefits such as reduced security risks, improved user experience, and compliance with regulatory standards.

Thirdly, operational feasibility evaluates the practical aspects of deploying and managing the system within organizational workflows. It involves assessing the system's scalability to accommodate growing user bases and increasing authentication demands. Additionally, considerations for training requirements and support infrastructure are crucial to ensure that administrators and end-users can effectively utilize and troubleshoot the authentication system.

Fourthly, legal and regulatory feasibility examines compliance with relevant laws (e.g., GDPR, HIPAA) and industry standards (e.g., PCI-DSS) governing data protection and privacy. Ensuring adherence to these regulations is essential to mitigate legal risks and potential liabilities associated with handling sensitive user information and authentication data.

SYSTEM REQUIREMENTS SPECIFICATION

4.SYSTEM REQUIREMENTS SPECIFICATION

4.1 SRS

A Software Requirement specification (SRS) is a complete description of the behavior of the system to be developed. It includes a set of use case that describes all the interaction the user will have with the software. Use cases are also known as functional requirements. In addition to use cases, the SRS also contains non-functional requirements. Non-functional requirements are requirements which impose constraint on the design or implementation (such as performance requirement, quality standard or design constraints).Goals of SRS are: -

➢It provides feedback to the customer. An SRS is the customer's assurance that the development organizations understand the issues or problems to be solved and the software behavior necessary to address those problems.

➢It decomposes the problem into component parts. The simple act of writing down software requirements in a well design format organizes information, places borders around the problem, solidifies ideas, and help break down the problem into its component part in an orderly fashion.

➢It serves as an input to the design specification. Therefore, the SRS must contain sufficient detail in the functional system requirement so that the design solution can be devised.

4.2 REQUIRMENT ANALYSIS:

Requirement analysis in system engineering and software engineering encompasses those tasks that go into determining the need or conditions to meet for a new or altered product,taking account of the possibly conflicting requirements of the various stack holders, such as beneficiaries or users.Requirement analysis is critical to the success of a development project. Requirement must be documented, actionable, measurable, testable related to identified business need or opportunity, and define to a level of detail sufficient for system design.Requirements are a description of how a system should behave or a description of system properties or attributes. It can alternatively be a statement of what an application is expected to do. The software requirement analysis process covers the complex task of eliciting and documenting the requirement of all these users, modeling and analyzing these requirement sand documenting them as a basis for system design.

4.3 NON FUNCTIONAL REQUIREMENTS:

It consists of following parameters: -

Reliability : The system will consistently perform its intended function.

For e.g. The important information must be validated.

Efficiency : Unnecessary data will not be transmitted on the network and database server will be properly connected.

Re-usability : The system can be reused in any organization or site of the same group,by defining the organization master definition under software license agreement.

Integrity : Only System Administrator has rights to access the database, not every user can access all the information. Each user will be having rights to access the modules.

4.4 SOFTWARE REQUIREMENTS :

- Operating system:windows 10
- Coding language : java
- Tool : Net-beans 8.2
- Database : MYSQL

4.5 HARDWARE REQUIREMENTS :

- System : Pentium i3 Processor
- Hard Disk : 500 GB
- Monitor : 15” LED
- Input Device : Keyboard,Mouse
- RAM : 2GB

SYSTEM DESIGN

5.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 designer 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.

5.1 SYSTEM MODULES

An e-authentication system that incorporates OTP (One-Time Password) and QR code functionalities typically consists of several key modules to ensure secure and efficient operation:

1.User Management Module :

- Responsible for managing user accounts, including registration, authentication settings, and user profile management.
- Stores user credentials securely, including passwords and associated OTP secret keys.
- Provides interfaces for users to update their authentication preferences and manage trusted devices.

2. OTP Generation and Delivery Module :

- Generates OTPs using algorithms like TOTP (Time-based One-Time Password) or HOTP (HMAC-based One-Time Password).
- Integrates with messaging services (SMS, email) to deliver OTPs securely to registered users.
- Implements mechanisms to handle OTP expiration and re-sending in case of delivery failures.

3. QR Code Generation and Decoding Module :

- Generates QR codes containing authentication information such as URLs or encrypted data.

- Provides APIs or interfaces for decoding QR codes scanned by users' devices.
- Ensures QR codes are securely generated and decoded to prevent tampering or interception.

4.Authentication Verification Module :

- Receives authentication requests from users along with OTPs or QR code data.
- Validates OTPs against stored secrets using secure cryptographic algorithms.
- Decrypts and verifies QR code data to authenticate users based on encoded information.

5.Logging and Audit Module :

- Logs authentication attempts, including successful and failed attempts.
- Monitors system performance and security metrics related to authentication processes.
- Supports auditing requirements for compliance with security standards and regulations.

6. Security and Encryption Module :

- Implements strong encryption mechanisms to protect sensitive user data, including OTP secrets and authentication tokens.
- Ensures secure transmission of OTPs and QR code data over the network.
- Implements measures to prevent brute-force attacks and other security threats.

7. Integration and APIs Module :

- Provides APIs for integration with applications and services that require authentication.
- Supports standards such as Oath, Open ID Connect, and SAML for federated authentication scenarios.
- Enables seamless integration of OTP and QR code authentication into existing systems and applications.

8.User Interface Module:

- Provides user-friendly interfaces for OTP input during authentication.
- Integrates QR code scanning capabilities into mobile apps or web applications.
- Ensures accessibility and usability across different devices and platforms.

By organizing the e-authentication system into these modular components, organizations can build a robust and flexible authentication solution that enhances security while maintaining usability for end-users. Each module plays a critical role in ensuring the integrity, reliability, and security of the authentication process using OTP and QR code technologies.

5.2 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 processor 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.

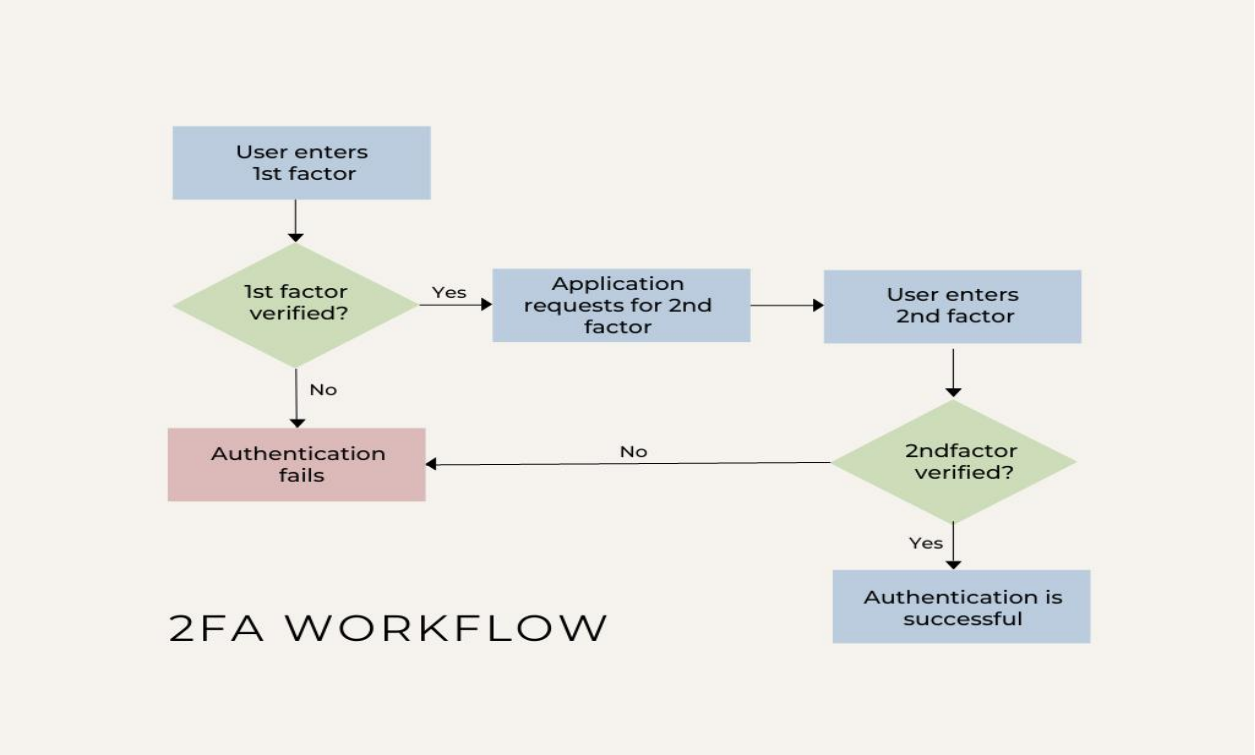


Fig:5.2.1-Flow chart

https://mojoauth.com/blog/multi-factor-authentication-best-practices/mfa-2fa-flowchart.png

5.3 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.

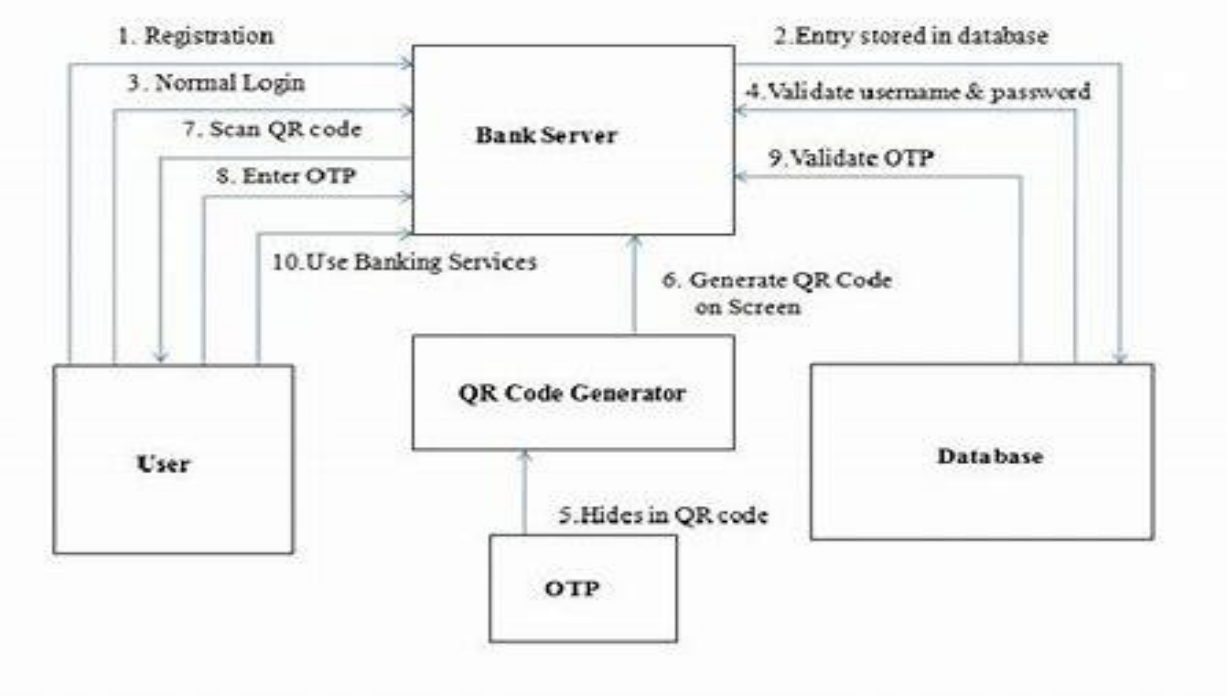


Fig:5.3.1-Data Flow Diagram

https://www.bing.com/images/search?view=detailV2&ccid=2p0Jpf

5.4 ACTIVITY DIAGRAM:

Activity diagrams are a loosely defined diagram technique for showing workflows ofstepwise activities and actions, with support for choice, iteration and concurrency. In theUnified Modeling Language, activity diagrams can be used to describe the business andoperational step-by-step workflows of components in a system. An activity diagram showsthe 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.

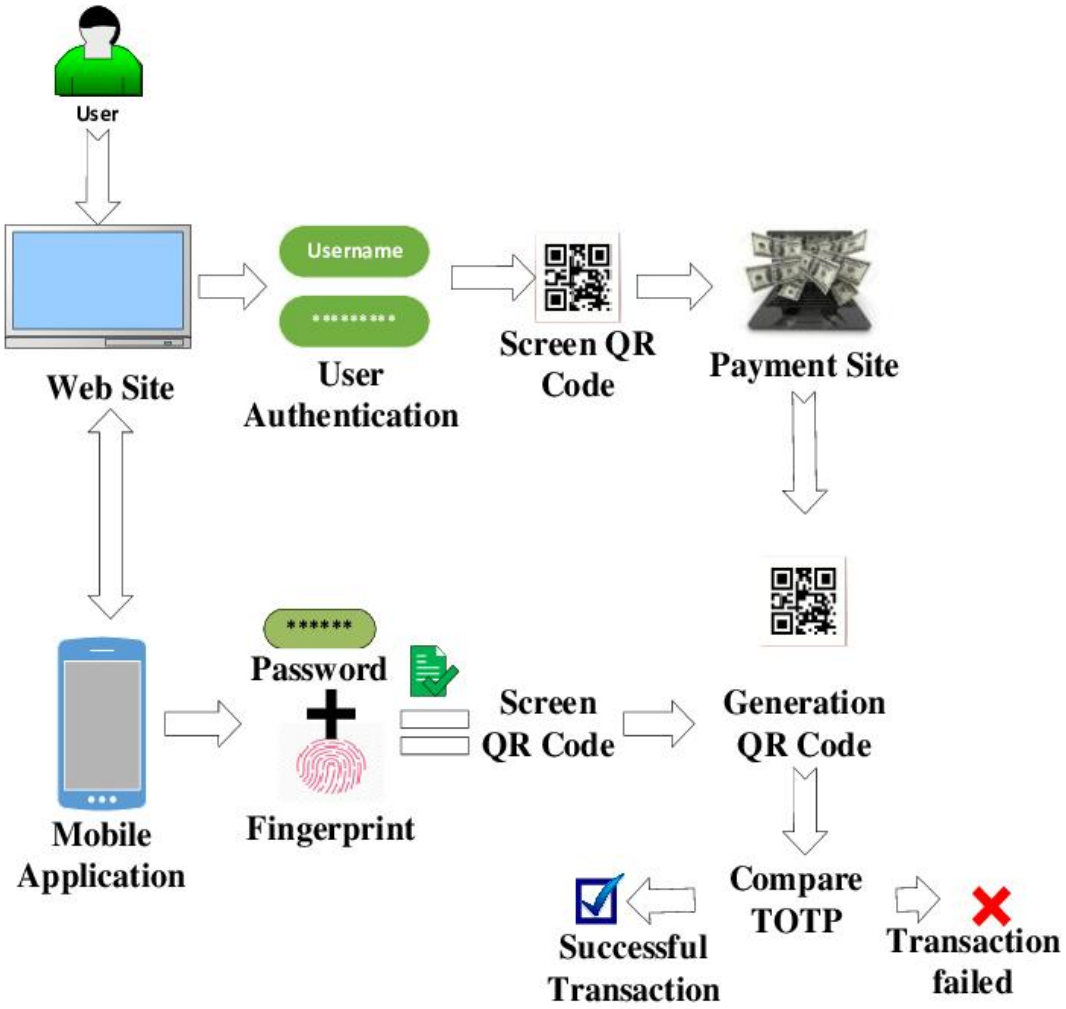


Fig:5.4.1-Activity Diagram

5.5 SYSTEM ARCHITECTURE :

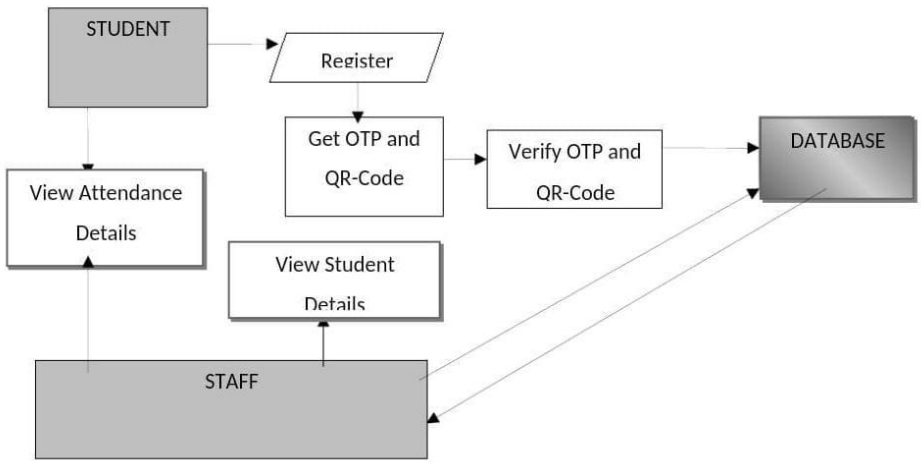


FIG:5.5.1:Architecture

IMPLEMENTATION

6.IMPLEMENTION

6.1 IMPLEMENTATION:

Designing an e-authentication system using OTP (One-Time Password) and QR code involves several components including generating OTPs, creating and scanning QR codes, and verifying user input. Below is an outline of the algorithm along with simplified Java code snippets for each part.

Implementing user registration for an e-authentication system using OTP and QR code involves several steps, including generating a secret key for OTP generation, storing user details securely, and potentially associating QR code functionality. Below is a simplified Java example outlining the process:

1.User Registration:

- User provides necessary details (username, password, etc.).
- Server generates a secret key for OTP generation and stores it securely.
- Server associates the secret key with the user account.

User.java

java

```
public class User {
    private String username;
    private String password;
    private String otpSecretKey; // Secret key for OTP generation

    public User(String username, String password, String otpSecretKey) {
        this.username = username;
```

```
    this.password = password;
    this.otpSecretKey = otpSecretKey;
}

// Getters and setters
public String getUsername() {
    return username;
}

public void setUsername(String username) {
    this.username = username;
}

public String getPassword() {
    return password;
}

public void setPassword(String password) {
    this.password = password;
}
```

```
    public String getOtpSecretKey() {
        return otpSecretKey;
    }

    public void setOtpSecretKey(String otpSecretKey) {
        this.otpSecretKey = otpSecretKey;
    }
}
```

2. Login Process:

- User enters username and password.
- Server verifies credentials.
- If valid, server generates an OTP and creates a QR code containing this OTP.

2.1. OTP Verification:

- User enters the OTP displayed by the scanning app.
- Client sends the OTP to the server for verification.
- Server verifies the OTP against the stored secret key associated with the user account.
- If OTP matches, authentication is successful.

OTP Generation:

```
java

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;
```

```
import javax.crypto.spec.SecretKeySpec;

import java.util.Base64;


public class OTPGenerator {


    public static String generateSecretKey() throws Exception {

        KeyGenerator keyGen = KeyGenerator.getInstance("AES");

        keyGen.init(256); // AES key size

        SecretKey secretKey = keyGen.generateKey();

        return Base64.getEncoder().encodeToString(secretKey.getEncoded());

    }


    public static String generateOTP(String secretKey) throws Exception {

        // Implement OTP generation using HMAC-SHA1 or TOTP

        // Example using TOTP (Time-based OTP) with a library like Google Authenticator
TOTP

        // Here we use a placeholder method for demonstration purposes

        return "123456"; // Replace with actual OTP generation logic

    }

}
```

2.2. QR Code Generation:

- Server generates a QR code using a library like ZXing (Zebra Crossing).
- The QR code contains the OTP which is encrypted or encoded.

QR Code Display:

- Server sends the QR code image to the client (e.g., as a download link or embedded in a web page).

QR Code Generation:

java

```
import com.google.zxing.BarcodeFormat;

import com.google.zxing.EncodeHintType;

import com.google.zxing.WriterException;

import com.google.zxing.client.j2se.MatrixToImageWriter;

import com.google.zxing.common.BitMatrix;

import com.google.zxing.qrcode.QRCodeWriter;


import java.io.ByteArrayOutputStream;

import java.util.HashMap;

import java.util.Map;


public class QRCodeGenerator {
```

```
    public static byte[] generateQRCodeImage(String text, int width, int height) throws
WriterException {

        QRCodeWriter qrCodeWriter = new QRCodeWriter();

        Map<EncodeHintType, Object> hints = new HashMap<>();

        hints.put(EncodeHintType.MARGIN, 1);

        BitMatrix bitMatrix = qrCodeWriter.encode(text, BarcodeFormat.QR_CODE, width,
height, hints);

        ByteArrayOutputStream pngOutputStream = new ByteArrayOutputStream();

        try {

            MatrixToImageWriter.writeToStream(bitMatrix, "PNG", pngOutputStream);

        } catch (Exception e) {

            e.printStackTrace();

        }

        return pngOutputStream.toByteArray();

    }

}
```

3. Authentication:

- User scans the QR code using a dedicated app or device.
- App decrypts or decodes the OTP and displays it to the user.
- Firstly, you need to generate a time-based OTP. For this, you can use the TOTP (Time-Based One-Time Password) algorithm from a library like Google Authenticator. Here's how you can do it using the java-otp-generator library:

```java

import com.eatthepath.otp.TimeBasedOneTimePasswordGenerator;

import javax.crypto.KeyGenerator;

import java.security.InvalidKeyException;

import java.security.Key;

import java.security.NoSuchAlgorithmException;

import java.time.Duration;

import java.time.Instant;

import java.util.Base64;

import java.util.Random;

import com.google.common.io.BaseEncoding;
```

6.2 Main Registration Logic:

```
java

import java.util.HashMap;

import java.util.Map;



public class UserRegistration {



    private Map<String, User> usersDatabase = new HashMap<>();
```

```
    public void registerUser(String username, String password) {
        try {
            // Generate OTP secret key
            String otpSecretKey = OTPGenerator.generateSecretKey();

            // Create User object
            User newUser = new User(username, password, otpSecretKey);

            // Store user details in database
            usersDatabase.put(username, newUser);

            // Optionally, generate QR code and associate with user
            // Example:
            // byte[] qrCodeImage =
QRCodeGenerator.generateQRCodeImage("otpauth://totp/YourAppName:" + username +
"?secret=" + otpSecretKey, 200, 200);
            // Store qrCodeImage or link in user's profile for future authentication

            System.out.println("User registered successfully: " + username);
        } catch (Exception e) {
            System.err.println("Error registering user: " + e.getMessage());
```

```
        }
    }

    public static void main(String[] args) {
        UserRegistration registration = new UserRegistration();
        registration.registerUser("user123", "password123");
    }
}
```

TESTING

7.TESTING

7.1 TESTING METHODS

Testing an e-authentication system that uses OTP (One-Time Password) and QR code involves validating various aspects of the system's functionality and security. Here are key aspects and strategies to consider when testing such a system:

1. Unit Testing

OTP Generation and Validation:

- Test OTP Generation: Verify that OTPs are generated correctly based on the secret key and current time.
- Test OTP Validation: Ensure OTPs are validated correctly against the expected values.

QR Code Generation:

- Test QR Code Generation:Validate that QR codes are generated correctly for enrollment.
- Test QR Code Decoding:Verify that QR codes can be scanned and decoded to retrieve the correct secret key.

2. Integration Testing

End-to-End Workflow:

- Enrollment Process:Test the entire process of enrolling a new user, including generating a QR code, scanning it with an authenticator app, and storing the secret securely.
- Login Process:Validate the end-to-end login process, including entering the OTP from the authenticator app and verifying its correctness.

3. Security Testing

Data Security:

- Encryption:Ensure that sensitive data such as secret keys and OTPs are transmitted securely over HTTPS.
- Storage:Verify that secret keys and OTPs are stored securely and are not exposed to unauthorized access.

Authentication Bypass:

- Testing for OTP Reuse:Attempt to reuse OTPs for authentication and ensure that each OTP can only be used once within its validity period.
- Testing for Time Drift:Validate that OTP validation takes into account time synchronization issues (clock drift) between the server and the user's device.

4. Performance Testing

Load Testing:

- Simulate Concurrent Users:Test how the system handles multiple concurrent users trying to enroll or authenticate simultaneously.
- Response Time:Measure the time taken to generate OTPs, validate OTPs, and generate QR codes to ensure they meet performance expectations.

5. Usability Testing

User Experience:

QR Code Scanning:Test the ease of QR code scanning and enrollment process from various authenticator apps.

Error Handling:Validate how the system handles incorrect OTP entries, expired OTPs, or QR codes that fail to scan.

7.2 TEST CASES

Here are some example test cases you might consider:

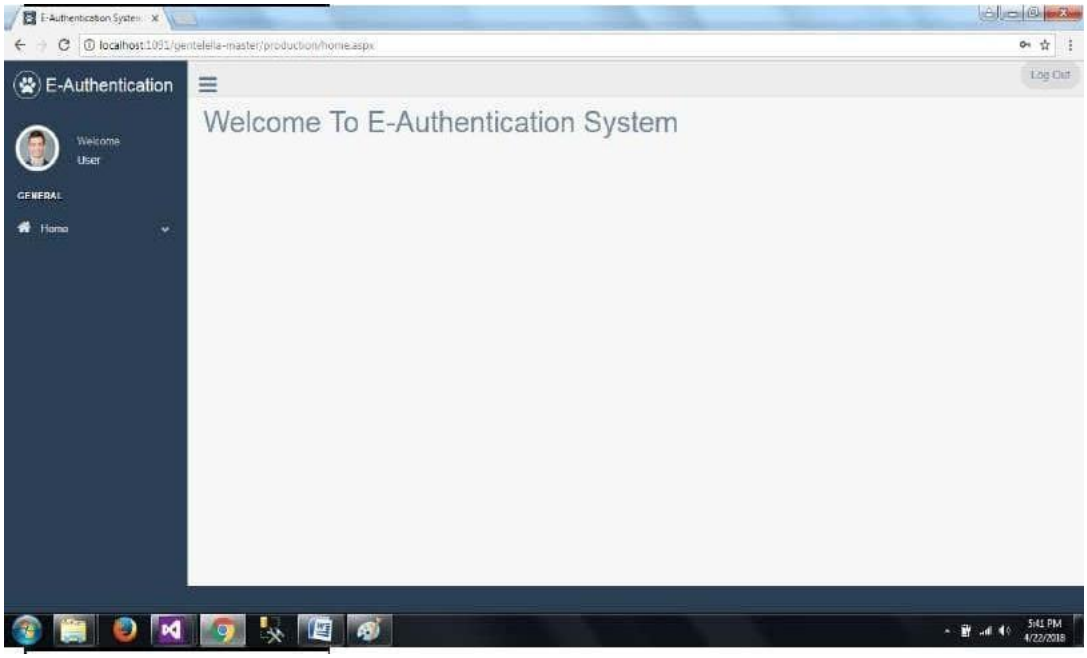
- TC01: OTP Generation:Verify that OTPs are generated correctly for a given secret key

- TC02: OTP Validation:Ensure OTPs are validated correctly against expected values.
- TC03: QR Code Generation:Validate that QR codes are generated correctly for enrollment.
- TC04: QR Code Decoding:Test that QR codes can be scanned and decoded to retrieve the correct secret key.
- TC05: Time Synchronization:Check how the system handles OTPs when there is a slight time difference (clock drift) between the server and client devices.
- TC06:Security:Attempt to intercept or manipulate OTPs or secret keys during transmission or storage to ensure data security measures are effective.
- TC07: Performance:Measure the system's performance under load by simulating a large number of users enrolling and authenticating simultaneously.

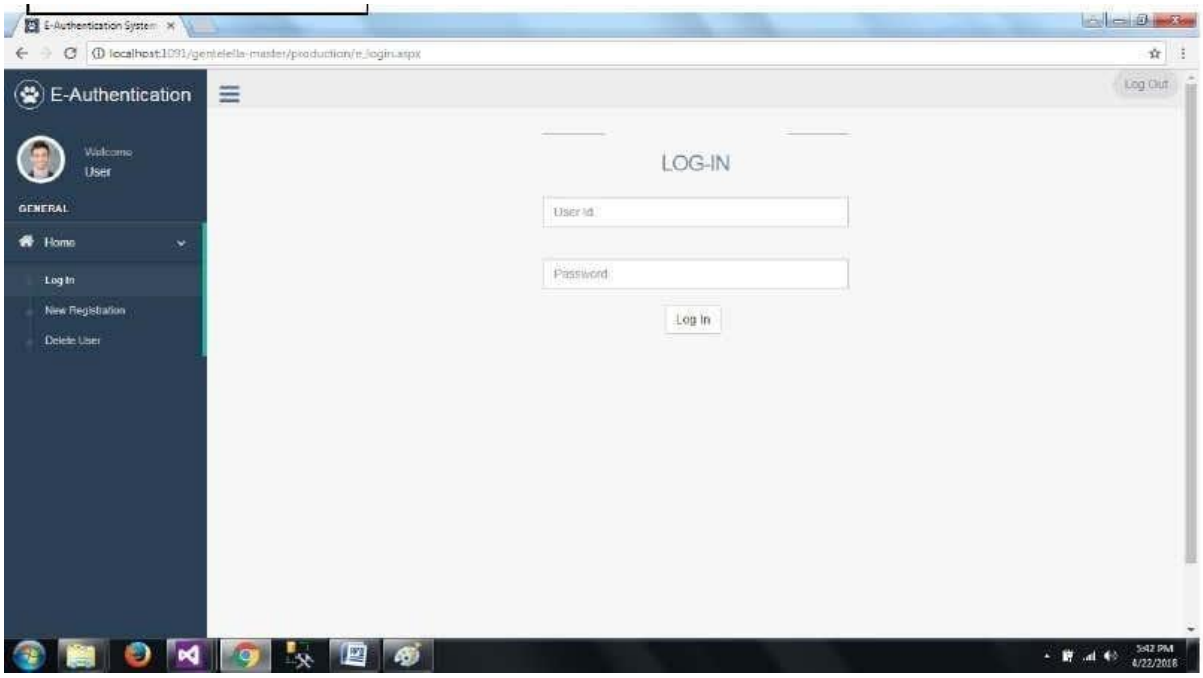
RESULTS

8. RESULTS

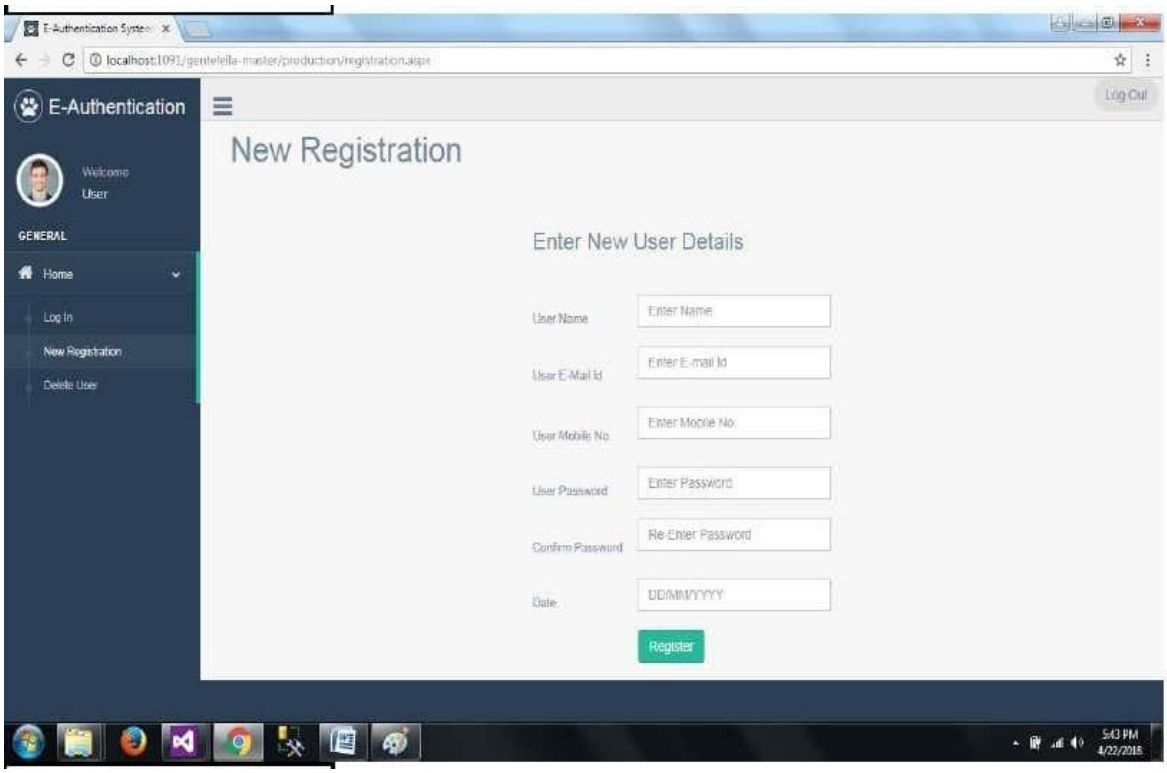
8.1 HOME PAGE:



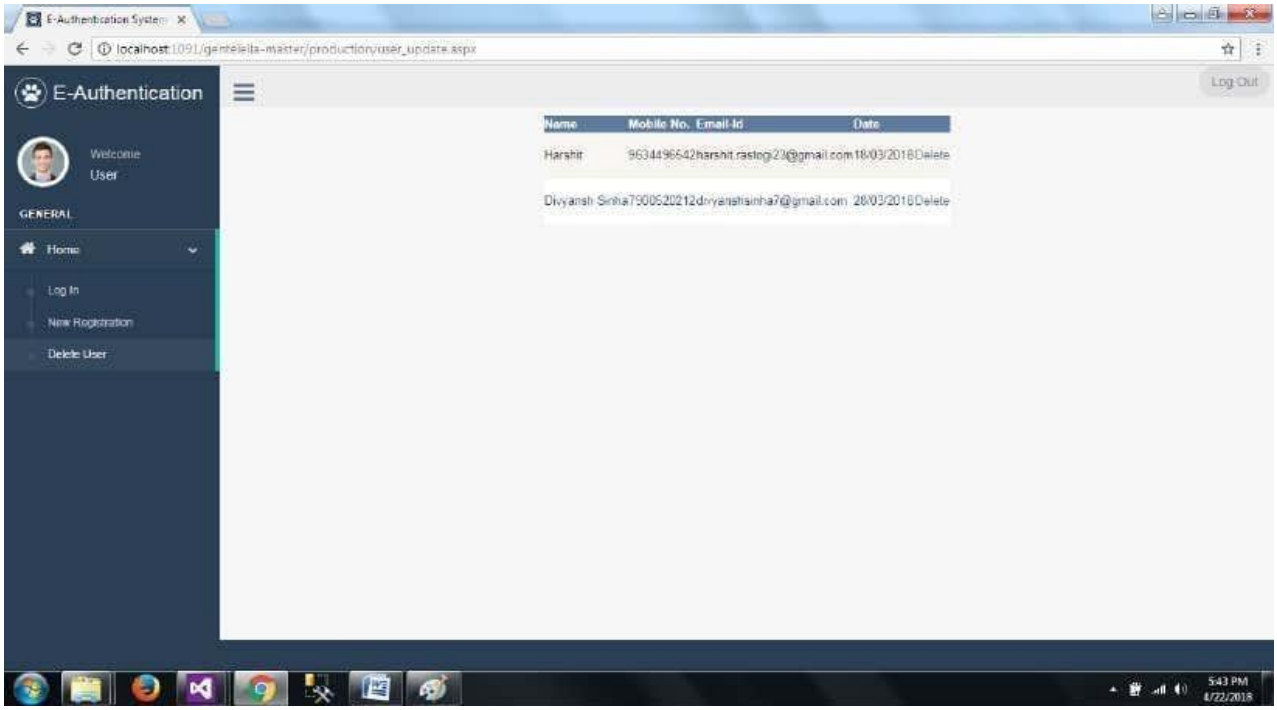
8.2 LOGIN PAGE:



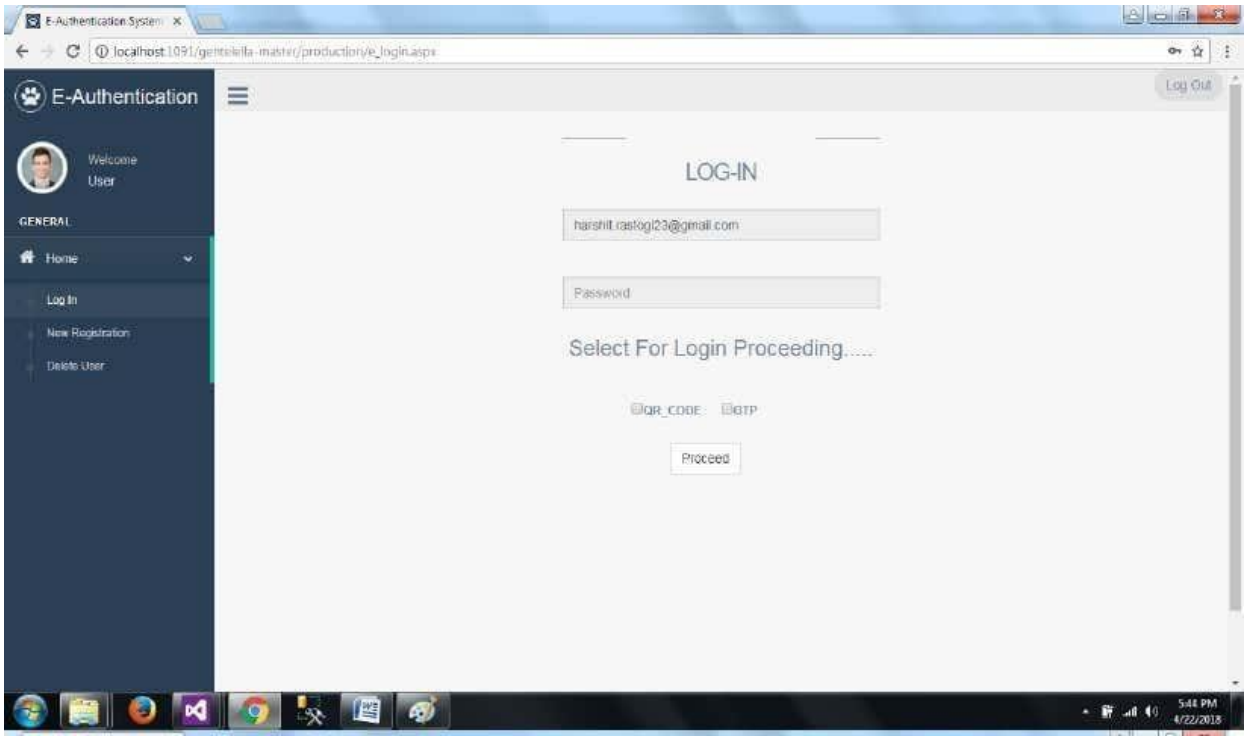
8.3 NEW REGISTRATION:



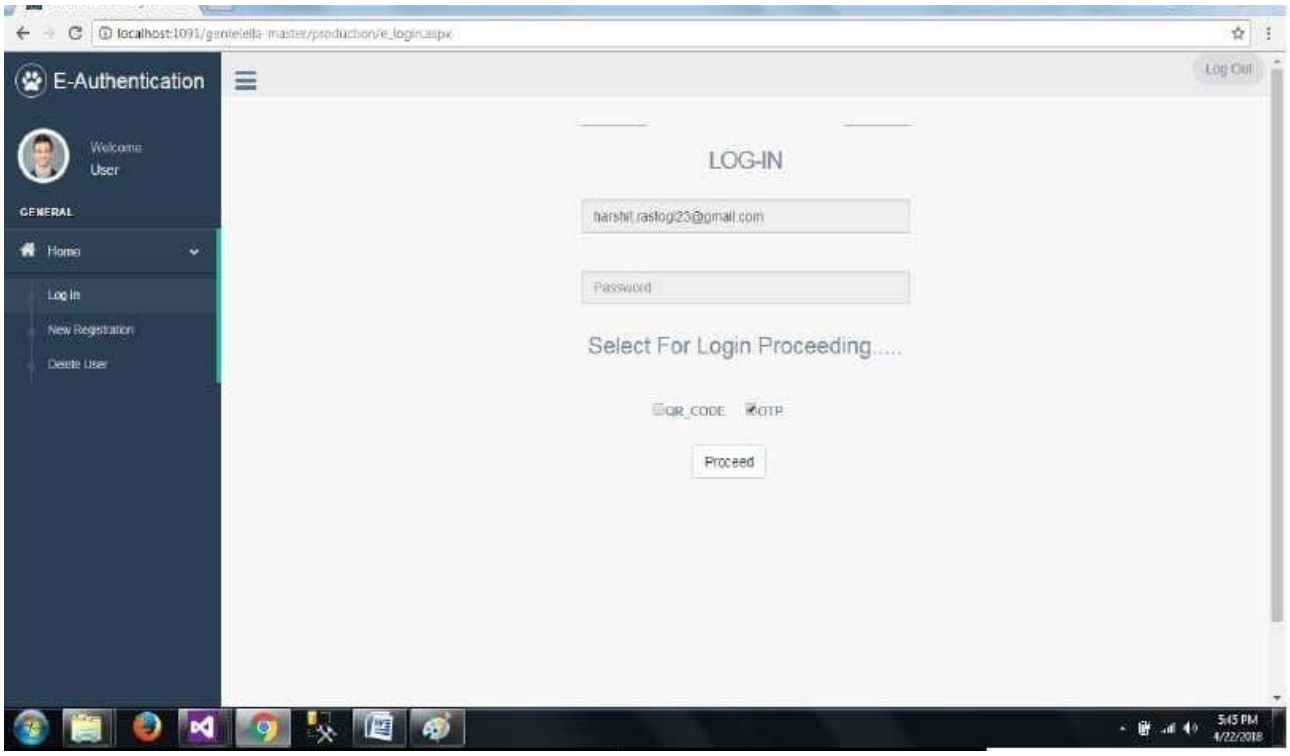
8.4 UPDATE USER:



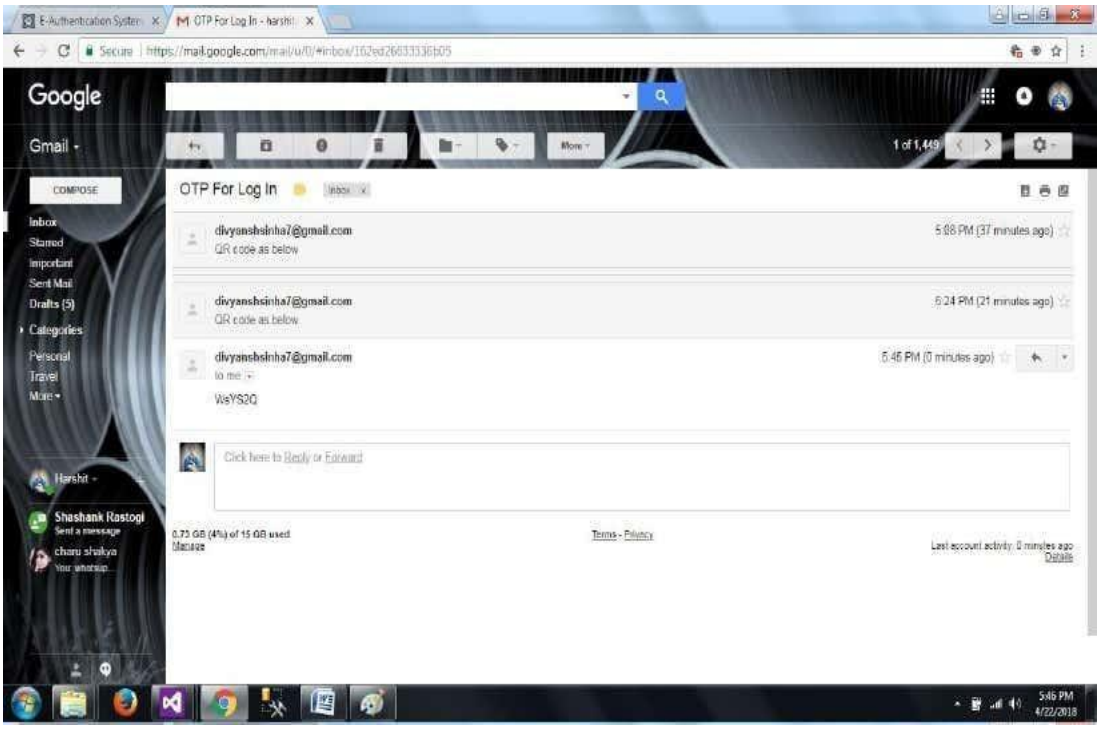
8.5 LOGIN VIA OTP AND QR CODE:



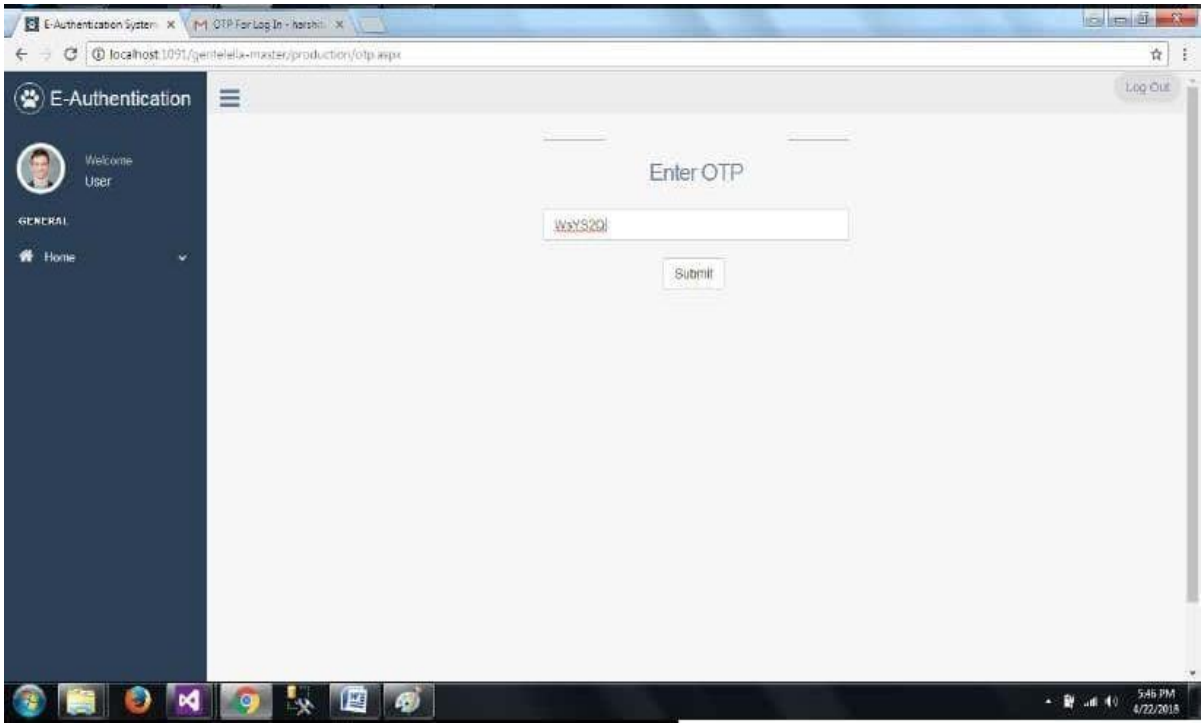
8.6 LOGIN VIA OTP:



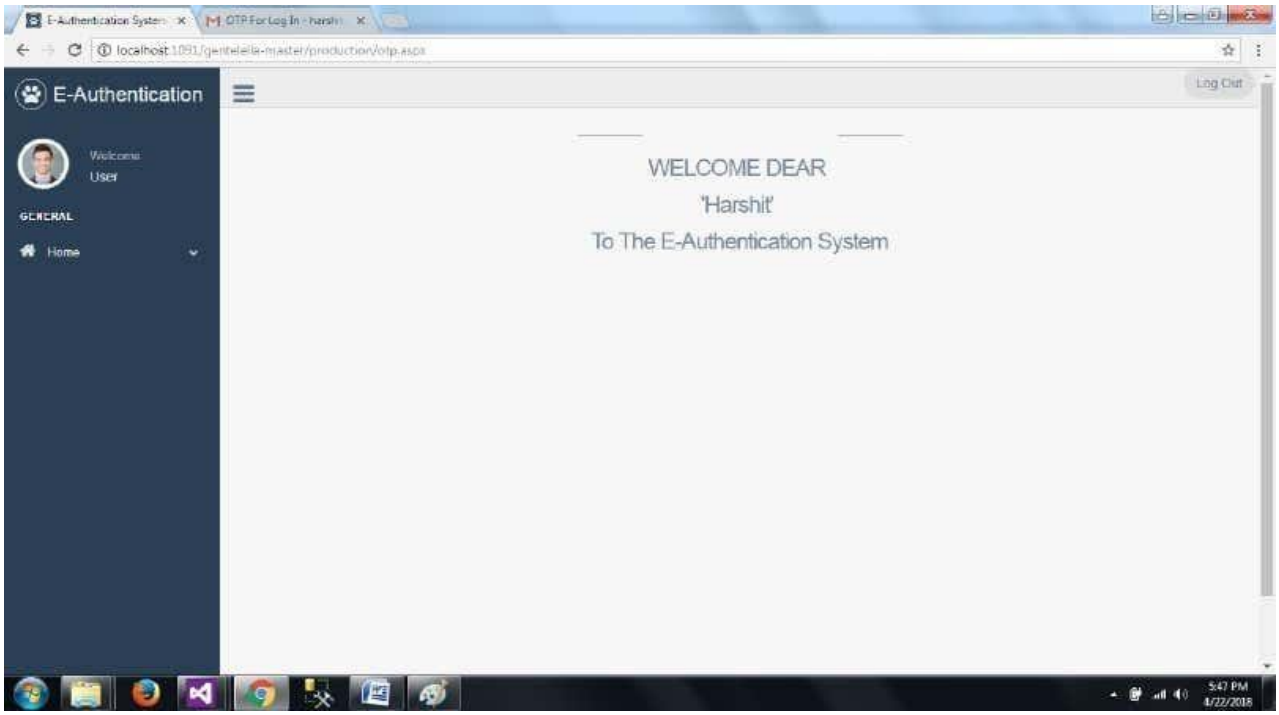
8.7 OTP ON MAIL:



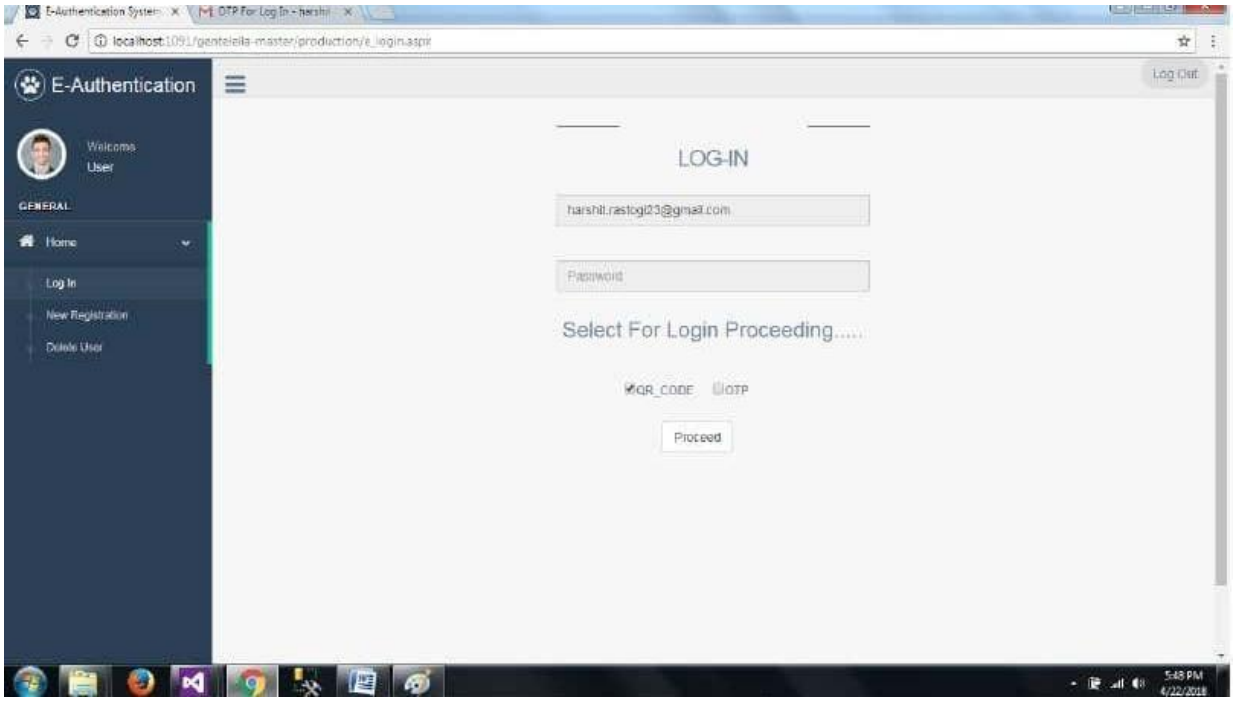
8.8 OTP VERIFICATION:



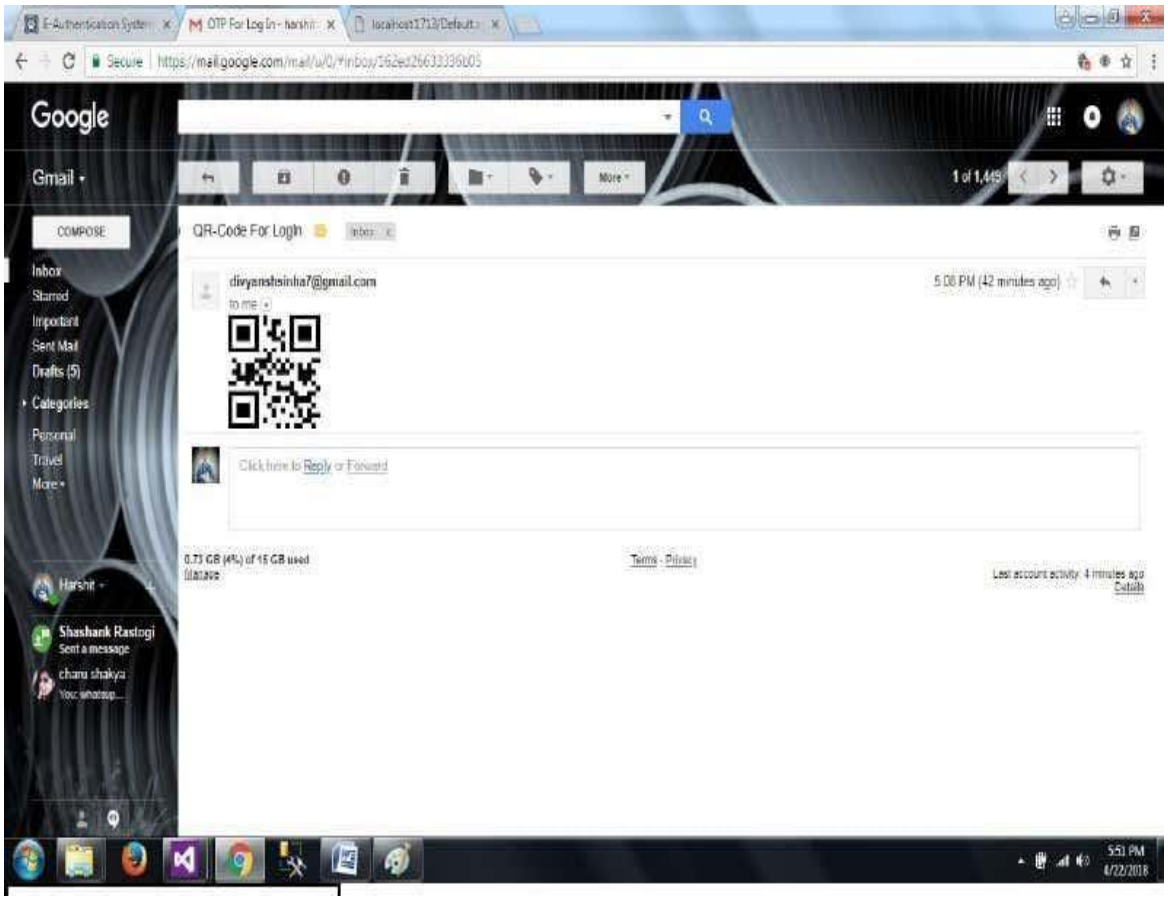
8.9 WELCOME TO USER:



8.10 LOGIN VIA QR CODE:



8.11 QR CODE ON MAIL:



CONCLUSION

9.CONCLUSION

In conclusion, an e-authentication system using OTP and QR code is a secure and efficient way of authenticating users for online services. The system offers an easy-to-use and accessible way for users to log in securely and reduce the risk of unauthorized access.The system's use of OTP and QR code technologies ensures that the user's identity is verified in a timely and secure manner. The system's design allows for flexibility, scalability, and ease of integration with other systems.The system also has potential applications in various sectors, including banking, e-commerce, and healthcare, where secure authentication is of utmost importance.

Furthermore, the system can be customized to meet the specific needs of various organizations, making it a versatile solution for online authentication.Overall, the e-authentication system using OTP and QR code is a reliable and secure solution that has the potential to transform online authentication and provide users with a seamless and secure login experience.The e-authentication system using QR codes and OTPs offers a robust and secure method for verifying user identities in digital platforms. By integrating these two technologies, the system leverages the unique benefits of both QR codes and OTPs, ensuring multi-factor authentication that enhances security.

9.1 KEY BENEFITS:

- **Enhanced Security**: Combining QR codes and OTPs ensures that two independent factors are required for authentication, making it much harder for unauthorized users to gain access.
- **User Convenience:** QR codes streamline the login process by reducing the need for manual input, while OTPs provide a dynamic and time-sensitive second layer of security.
- **Scalability**: The system can be easily scaled to accommodate a large number of users and integrated with various platforms and services.
- **Cost-Effective**: Implementing QR codes and OTPs is relatively cost-effective compared to more complex biometric systems, yet it offers a high level of security.

- **Implementation Outcomes**: Increased Adoption: Users are likely to adopt the system due to its ease of use and the familiarity of QR codes and OTPs.

- **Reduced Fraud:** The system's robust authentication mechanism helps in significantly reducing instances of fraud and unauthorized access.

- **Improved User Trust:** Users gain confidence in the security measures protecting their information, leading to greater trust in the platform.

9.2 FUTURE SCOPE:

The e-authentication system can be further enhanced by integrating with biometric verification for even higher security, utilizing machine learning for detecting fraudulent patterns, and expanding its use cases to include secure transactions and access control in physical spaces.

Overall, this e-authentication system serves as a reliable, secure, and user-friendly solution for modern authentication needs, striking a balance between security and convenience.

BIBLIOGRAPHY

10.BIBLIOGRAPHY

- Ali, M. S., & Raza, M. (2020). A Comprehensive Review on QR Code Technology. Journal of Information Technology Research, 13(2), 34.50 https://doi.org/10.4018/JITR.2020040103.

- Bahga, A., & Madisetti, V. (2013). Internet of Things: A Hands-On Approach. VPT.

- Bhardwaj, R., & Kumar, M. (2017). A Study on QR Code Technology. International Journal of Computer Science and Mobile Computing, 6(5), 5-11.

- Das, A., Borisov, N., & Caesar, M. (2014). Do You Hear What I Hear? Fingerprinting Smart Devices Through Embedded Acoustic Components. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 441-452). ACM. https://doi.org/10.1145/2660267.2660355.

- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4(5), 1125-1142. https://doi.org/10.1109/JIOT.2017.2683200.

- Luo, W., & Zeng, D. (2017). QR Code Based Secure Mobile Payment System. Journal of Information Security, 8(2), 111-122. https://doi.org/10.4236/jis.2017.82009

- Mani, S., & Pooja, M. (2015). Enhanced Authentication System Using QR Code. International Journal of Computer Applications, 119(19), 33-37. https://doi.org/10.5120/21102-4006

- Saxena, N., Ekberg, J. E., Kostiainen, K., & Asokan, N. (2015). Secure Device Pairing Based on a Visual Channel. IEEE Transactions on Mobile Computing, 14(4), 884-896. https://doi.org/10.1109/TMC.2014.2333014

- Sheng, Y., & Jiang, Y. (2016). Two-Factor Authentication Based on QR Code. Advances in Computer Science and Engineering, 16(2), 75-81.

- Wheeler, D. J. (2019). OTP Security: An In-Depth Look at One-Time Password Systems. Tech Publishing.-21, 2007.