Secure Online Transactions with Dual OTP Authentication

A project report submitted in partial fulfillment

of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering with Specialization in AI and Robotics

by

M R MADHAVAN (21BRS1433)
ADARSH S (21BRS1301)
ADARSH K M (21BRS1158)

School Of Electronics Engineering ,
School Of Computer Science and Engineering,
Vellore Institute of Technology Chennai,
Vandalur-Kelambakkam Road,
Chennai - 600127, India.

November 2024

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Declaration

I hereby declare that the report titled **"Secure Online Transactions with Dual OTP Authentication"** submitted by me to the School of Electronics Engineering, Vellore Institute of Technology, Chennai in partial fulfillment of the requirements for the award of **Bachelor of Technology** in **Computer Science and Engineering with Specialization in AI and Robotics** is a bona-fide record of the work carried out by me under the supervision of ***Kalaivanan K***.

I further declare that the work reported in this report, has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma of this institute or of any other institute or University.

Sign: _____

Name & Reg. No.: _____

Date: _____

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

Certificate

This is to certify that the project report titled ***Secure Online Transactions with Dual OTP Authentication*** submitted by Adarsh S **(21BRS1301),** M R Madhavan **(21BRS1433),** Adarsh KM **(21BRS1158)** to Vellore Institute of Technology Chennai, in partial fulfillment of the requirement for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering with Specialization in AI and Robotics** is a bona-fide work carried out under my supervision. The project report fulfills the requirements as per the regulations of this University and in my opinion meets the necessary standards for submission. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma and the same is certified.

Supervisor

Signature: .....

Name: .....

Date:

Head of the Department

Signature: .....

Name: .....

Date:

Examiner

Signature: .....

Name: .....

Date:

(Seal of the School)

Abstract

The Dual OTP and Fingerprint-Based Two-Step Authentication System provides a robust security solution to the improvement of Internet-based financial transaction safety. Conventional single-factor OTPs or passwords have proven themselves vulnerable to phishing, interception, and improper access. This system introduces a two-layered system, with OTPs complemented by biometric fingerprint authentication for the confirmation of both sender and receiver.

The system generates a unique OTP for each transaction, which is securely sent to the concerned parties. Each digit of an OTP is mapped to specific fingerprints, and users are required to input a digit while simultaneously authenticating themselves through a fingerprint scan. This dual factor ensures that even if OTPs are compromised, transactions cannot proceed without matching biometric inputs, thereby reducing fraud risks to a large extent.

The architecture includes an OTP generator, fingerprint scanner, secure Oracle 11g database, and a user-friendly verification interface. The workflow is initiated by the sender where he receives an OTP and types in each digit beside the corresponding fingerprint. This is echoed by the receiver to carry out two-factor authentication on either side. The ELT (Extract-Load-Transform) pipeline is used to process the data, ensuring real-time verification. SOAP/RESTful APIs are used for safe transmission of data while JPublisher integrates database operations with Java components for seamless functionality.

This authentication system is very flexible and expandable in its applications. It comes into use for high-security online banking, digital payments, and other applications. The merging of OTP with biometrics makes for an advanced security solution for fraud, unauthorized access, and other forms of cybersecurity threats. Its transparency, user friendliness, and strong security measures all build up to creating trust and ensuring reliable transactions-a requirement for modern digital authentication needs

Acknowledgements

We wish to express our sincere thanks and deep sense of gratitude to our project guide, Dr. Kalaivanan K, Associate Professor, School of Electronics Engineering, for his consistent encouragement and valuable guidance offered to us in a pleasant manner throughout the course of the project work.

We are extremely grateful to Dr. Ganesan R, Dean, Dr. Parvathi R, Associate Dean (Academics) & Dr. Geetha S, Associate Dean (Research) of the School of Computer Science & Engineering, VIT Chennai, for extending the facilities of the School towards our project and for his unstinting support.

We express our thanks to our Head of the Department Dr. Harini S for her support throughout the course of this project.

We also take this opportunity to thank all the faculty of the School for their support and their wisdom imparted to us throughout the course.

We thank our parents, family, and friends for bearing with us throughout the course of our project and for the opportunity they provided us in undergoing this course in such a prestigious institution.

Contents

List of Figures

Chapter 1

Introduction

1.1 Project Background

Improved accessibility and convenience, as well as the shift of the economy of the world to cashless, make the rapid growth of electronic transactions a distinct characteristic of modern financial systems. However, this growth has been accompanied by more critical security issues, such as financial fraud, identity theft, as well as unauthorized access to sensitive financial information. Conventional authentication techniques, including single-layer OTP (One-Time Password) systems or those reliant on passwords, although offering a fundamental degree of security, are progressively vulnerable to advanced threats such as phishing, man-in-the-middle attacks, and social engineering tactics.

A major security concern within the electronic payment platform is the lack of protection for the identity of both the sender and receiver involved in a transfer. Most verification technologies focus mainly on ensuring the authenticity of the sender or originator of the transaction but often fail to provide for a high level of validation of the receiver. This failure thus poses a major vulnerability which an attacker can leverage to compromise the identity of the receiver and divert money from the account without the knowledge of the sender. To address these limitations, dual OTP-based two-step authentication offers a more resilient security measure wherein both the sender and receiver are verified separately. This lends the process an additional layer of protection, minimizing the possibility of fraudulent transactions and strengthening online monetary exchanges at large.

1.2 Problem Statement

In the digital financial transactions scenario envisioned for the modern landscape, security indeed paints a nightmare, especially when verifying the identities of parties that might engage in a transaction.

The single-layer techniques being used at present lack the potency required to adequately protect users from unauthorized access, identity theft, and further forms of cyber fraud practices. The problem is mainly that the sender and receiver can be easily manipulated, given that authentication systems currently in place do not have multi-layered verification for both parties. This proposed project aims at mitigating this vulnerability by implementing a dual OTP-based two-step authentication system placed to bolster security in digital transactions by first requiring an additional verification step from both the sender and the receiver.

The underlying issue that this project tries to resolve has been the lack of existing authentications to offer protected features for all the parties attributed to any transaction in situations where required. From this, their authenticity risk of unauthorized access thereby lowers user confidence in electronic transactions security and raises financial fraud occurrences.

The installation of a two-factor OTP system in this project aims to offer an answer that would thereby increase security, minimize risks, and thus boost the reliability of transaction.

1.3 Objectives of the Study

The followings are the aims of the present study:

Secure online monetary transaction two-step authentication system using dual OTPs which verifies the sender and receiver independently End.

The objectives of dual OTP will then be met by evaluating the effectiveness of the OTP system in terms of its ability to prevent unauthorized access and fraud, thereby enhancing security online.

To ensure more reusability of user confidence in online transaction systems by introducing strong authentication protocols that would provide greater assurance of security for both the sender and receiver.

To address and overcome challenges with integration of dual OTP systems, especially when implemented on existing transaction platforms that need seamless integration even at high security standards.

To make the OTP system resilient to ever-increasing security threats and potential attacks, it should work in an adaptable and scalable solution for the burgeoning digital transaction platforms.

1.4 Significance of the Study

In this regard, this research becomes significant in that it can bridge a fundamental security gap in digital financial transactions, where verification of the sender as well as the receiver becomes one of the crucial parameters. The present growing rate of e-commerce transactions demands secure identity confirmation of both the parties and thus develops confidence among digital financial ecosystems. Hence, an endeavor such as double OTP-based verification system in the process of transaction further strengthens it and reduces fraud cases to a greater extent.

Dual OTP implementation has some benefits as given below:

More Fraud Protection A dual OTP gives greater protection against attackers since it verifies both parties: the receiver and the sender. It safeguards unauthorized access, minimizes phishing risk for a certain transaction, and limits malicious interceptions of transactions.

Enhanced Confidence in Online Transactions: With more confidence in the security protocols that would protect their transactions, people are more likely to adopt and commit themselves to online transaction systems. The initiative has the capabilities to add enhanced security features that will increase the engagement of the users and increase confidence in digital payment systems.

Dual OTP can be agile to other new security threats; hence, in regard to new vectors attacking security, it could be or extended by the system. This makes its value in the battle for ongoing cybercrime.

In conclusion, the importance of this research goes beyond individual users' security. Responding to a much broader requirement in society, it promotes trustworthy and secure digital financial infrastructures, thereby fostering the sustainable development of online financial services and reducing possible hazards.

1.5 Scope of the Project

This project involves designing, implementing, and evaluating the dual OTP-based two-step authentication system that supplements security of digital financial transactions. The key components of the project are:

Design and develop a secure and efficient OTP generation and verification system of both sender and receiver with mechanisms to independently generate OTP and validate it at the end with minimal overlap and high reliability in the OTP authentication process. Integration and usability testing-the dual OTP system is to be integrated with web- or mobile-based transaction systems while maintaining usability testing to determine whether the system is still user-friendly without compromising security. Security Assessment It basically assesses the effectiveness of a system in safeguarding against unauthorized access, fraud, and identity theft through security testing and threat modeling. Testing for various attack scenarios will be simulated to verify how safe the dual OTP process is. User Experience Evaluation: Assessing the user's opinion regarding the convenience of transactions, level of confidence in, and perception of security towards a two-factor OTP system. The findings will be used to enhance the system for improved usability and trust building. Scalability Analysis: Whether the two-factor OTP system can be scaled up to handle more significant users, thus checking its applicability on various transaction platforms and diverse regional regulations. The project will not get into designing any other authentication mechanisms of any kinds such as biometric or hardware-based authentication since the

project will be focused on the dual OTP-based two-step mechanism of authentications. Also, an independent transaction platform shall not be within the scope of the project as it seeks to seamlessly supplement the existing digital transaction systems with security attributes.

Chapter 2

Literature Review

2.1 Introduction

Advance in the digital economy, electronic banking has become a very integral part of financially conducted global negotiations and produces unmatched ease and accessibility for consumers. However, this convenience brings with it an increase in cyber threats such as identity theft, financial fraud, and unauthorized access, which pose considerable risks for both consumers and financial institutions. After conventional transaction authentication mechanisms, like passwords and one-time password mechanisms, have proven to be inadequate in the face of advanced cyber threats, new strategies emerge among cyber robbers targeting online banking infrastructure. Thus, it is imperative that advanced security architecture should be in place to stop online transactions.

For these problems, researchers have brought forward several advanced security protocols, including MFA, multi-layered encryption, and enhanced OTP systems. One of the research project's major concerns was to investigate how a dual OTP-based two-step authentication method developed for authenticating both the sender and the receiver for any online transaction was functional. In this respect, verification goes independently through two different OTP processes, making it safer and with reduced possibilities for access by somebody else. The principal aim is to create a framework that guarantees safe and smooth online transactions, striking a balance between user ease and strong defenses against cyber threats.

2.2 Multilevel Security and Dual OTP System for Online Transactions Against Attacks

The article "Multilevel Security and Dual OTP System for Online Transaction Against Attacks" provides an elaborate description of the current security issues related to online transactions. The author does talk about the single layer of authentication currently positioned to require robustness against leading sophisticated cyber attacks. The literature in the field indicates that multi-layered security measures such as traditional security Single OTP have basic protection but vulnerabilities to brute-force attacks and identity theft. This is

why this paper proposes dual OTPs requiring independent verification for both the sender and receiver in strengthening transactional security.

Other scholars, like Gao et al. (2018) as well as Johnson et al. (2018), have pointed out security vulnerabilities presented by mobile payment systems. This threatens to cannibalize the said platform's adoption due to security concerns. Mitigating these factors is exactly what the current research proposes: the use of multi-layered encryption based on Blowfish and AES algorithms in more advanced security against unauthorized access.

A combined encryption framework is presented to address the risks when applied in conjunction with dual OTP verification, which has been found to be more secure than related single OTP-based schemes. Though dual OTP system bears the above-said advantages, it potentially creates complexity issues with possible latency and integration complications across other banking systems. To neutralize these challenges, the authors suggest user-friendly alternatives to the current authentication, includes system optimization from time to time, and carries a secondary backup authentication method. According to the authors' research work, this multi-layered approach combining dual OTP represents a feasible solution to secure online transactions.

2.3 Transaction Authorization from Know Your Customer (KYC) Information in Online Banking

The article "Transaction Authorization from Know Your Customer (KYC) Information in Online Banking" uses KYC to implement a challenge-question-based (CQ) authentication mechanism for transactions, highly usable alternative to common OTP systems. Following the background of increased phishing, pharming, and Man-in-the-Middle (MITM) attacks episodes, authors believe OTP-based authentication has some disadvantages specifically when the security aspect of the device is compromised or when there is a delay in issuance of OTP.

The paper proposes a system that derives challenge questions based on risk-assessed information from KYC for transaction authorizations. The process covers two steps: a password-based login to be later followed by dynamic challenge questions that are customized based on the user's behavior; the more risk-prone transactions, the higher the security risk of the questions prompted. It is shown that KYC-based CQs seem to be more secure than the common OTP, mainly because it minimizes interception likelihood and provides a lower dependence on external devices.

In the simulation results, the CQ-based system performed better than typical OTP frameworks in the aspect of security and adaptability, especially when addressing high-risk situations. The reliance of this system on dynamic, behavior-based CQs strengthens its security, but the authors do admit that the feasibility may involve challenges related to computational complexity and integration with the installed infrastructure of existing banks.

2.4 Secure Electronic Banking Transaction using Double Sanction Security Algorithm in Cyber Security

The "Secure Electronic Banking Transaction using Double Sanction Security Algorithm in Cyber Security" focuses on the weaknesses of single OTP systems toward electronic banking transaction security. With ease of access through e-banking, there are so many liabilities; insecure internet connections may leave a user vulnerable enough to various types of cybercrime. This paper proposes a "Double Sanction Security Algorithm" comprising OTP and layered encryption to endow e-banking transactions with a secure environment.

The Double Sanction Security Algorithm employs a 2048-bit encryption key. The procedure, as achieved, strictly relates to all defined cybersecurity practice standards. Although traditional encryption frameworks like AES are used widely, they have specific limitations; authors of this paper recommend using SSL, which would enhance the encryption process, thereby establishing secure connections. Therefore, it highlights that advanced algorithms pose a minimum risk to unauthorized access.

Along with a technical solution, this paper will also briefly discuss the economic impact, highlight monetary damages that have taken place during the last couple of years due to cyberattacks, and mention the desire for state-of-the-art security solutions. The Double Sanction Security Algorithm offers a relatively cost-effective solution in that it builds upon existing encryption platforms and minimizes the need for substantial modifications to bank infrastructure. However, challenges like latency-with added complexity from double encryption-become an area of further research and development.

2.5 Secure Online Banking With Biometrics

The research paper proposed will be discussing a three-factor authentication in online banking, which would be secured better and free from the vulnerability of traditional methods of username/password, where they validate credentials but do not verify the real owner's identity. This system involves three different authentication elements-the username and password along with familiar random images and then fingerprint biometric data. The first layers are the credibility of the usernames and passwords through which a verification is required. The second one is based on already known pseudo-random images, to which the user has assigned at the time of enrollment. This has a natural advantage of depending upon the human visual memory, where the chance of replicating or guessing such images is much more difficult for an intruder. The third one is a fingerprint biometric, for unique physical identity verification, which offers another layer of protection against an access attempt made in an unlawful way.

For ensuring that the biometric data is private and that the binding is secure, the author suggests the technique of Match on Card. In this method, the database of fingerprints is kept on a credit card itself and doesn't go out of the card; rather, matching is performed on the card itself also, hence, biometric data is not breached even in case of security breach. Result of this research showed that the three-factor authentication system gave high security to online banking accounts, thereby it was not easy for intruders to bypass all the three-layer authentication. The proposed approach reduces the risk of cybercrime as the result of merging several factors of security. Consequently, user security confidence will increase regarding online banking transactions.

2.6 Gaps In Literature

While each of these papers brings valuable contributions to online transaction security, much needs to be done in filling research gaps. Of particular interest is the area of usability issues related to system complexity for both dual OTP systems and multi-layered encryption methods. Advanced security measures come at a usability cost in that they entail some increase in time and resource requirements. Future research should aim at method developments that optimize this balance in such a manner that the overall system is both secure and user-friendly.

Another issue is scalability; with high-frequency transaction on bank platforms, latency occurs when doubled encryptions or dual OTP processes take place, and this appears more serious during peak times. It may be resolved if the computational efficiency is increased using lightweight encryption or hardware acceleration. Further research should then take place into other cryptographic methods, such as quantum-resistant algorithms, to prepare the transaction for potential threats posed by the future existence of quantum computing.

Finally, even though two-factor systems of OTP and CQ enhance security, reliance on the security or availability of the access device might be a weakness when users cannot access their devices. Future work can be integrated with methods of biometric-based authentication or adaptive techniques that can reduce one's dependency on one device. A flexible, multi-channel authentication framework improves robustness towards any limitations caused by having multiple devices in place. Under different access scenarios, transactions are reliable and secured. It is very important to fill these gaps for further improvement in security against cyber threats in online banking transactions and will be able to protect users from emerging cyber threats.

Chapter 3
Methodology

3.1 Dual OTP and Fingerprint-Based Two-Step Authentication System

This is specifically a dually OTP and fingerprint-based two-step authentication system that has been designed as a safety framework to improve the safety and security surrounding online financial transactions. It differs from conventional authentication methods using only usernames/passwords or simple OTPs; it has instead introduced a multi-factor approach aimed at verification of both sender and receiver. In such a system, each user will be authenticated with the aid of OTP along with fingerprint data to set up a dual verification process for either side of the transaction. This system ensures that the security vulnerability of online banking is addressed to the parties involved on a transaction being authentic and legitimate thereby denying entry or transaction by unauthorized persons.

3.1.1 Authentication System Architecture

The architecture is multilayer, with layers constructed on the basis of increasing security measures designed for both reliability in the authentication process and providing data safety, respectively. It therefore encompasses a number of associated components working together toward ensuring safe step-by-step multi-step verification of both initiators of transactions (senders) and receivers of such transactions.

Core Components and Their Functions:

1) OTP Generation and Distribution

An OTP generating module is there on the authentication server, which generates one-time, transaction-specific OTP. This OTP is sent through the secure communication channel such as SMS or email both to the sender as well as receiver.

Every OTP is a single, alterable code that has the time factor added to it, which in turn defends against multiple uses of OTP and hampers interceptions.

2) Fingerprint Matching Mechanism

This module provides an interface to capture and verify user fingers through a biometric fingerprint scanner against the pre-registered data maintained in the server database. Each digit of the OTP is related to a particular print position (thumb or finger), this keeps an additional layer of security in case the unauthorized access.

3) Dual Verification Process

Both the sender and the receiver have to do a cycle wherein they need to input the OTP digits while simultaneously furnishing corresponding fingerprint inputs so that even if the OTP is accessed, the transaction will be safe since a fingerprint input is also required.

3.2 Process Workflow

The process workflow is a step sequence from OTP generation to the final confirmation of the transaction. Here, both the users have to follow each one of these for ensuring a secure successful transaction.

Steps in Process Workflow:

Transaction Initiated by Sender

The sender initiates a transaction by triggering a client interface that requests the server to generate an OTP.

Distribution and Verification of OTP

The server generates an OTP and securely sends it over to both the sender and receiver. The OTP sequence both parties need to go through to make sure each digit is used with its matching fingerprint so it is presented.

Fingerprint-OTP Matching

Every digit of the OTP sequence corresponds to a specific fingerprint. For example, if the OTP is "6015," the following sequence will request the sender and receiver to input the digits while using their thumb/finger according to the mapping.

Final Verification

Only both parties can consummate the deal after having successfully authenticated through each of their OTP and fingerprint sequences.

3.2.1 Fingerprint and OTP Mapping Mechanism

Mapping OTP digits to specific fingerprints creates a unique layer of security, as the user must match both the OTP and fingerprint accurately. This mechanism prevents brute-force attacks and adds complexity that secures the transaction.

Example Mapping System:

Digits 0-9 are mapped to specific fingers:

0: Left Thumb

1: Left Index Finger

2: Left Middle Finger

3: Left Ring Finger

4: Left Pinky Finger
5: Right Thumb
6: Right Index Finger
7: Right Middle Finger
8: Left Ring Finger
9: Left Pinky Finger
This mapping requires both sender and receiver to input each digit of the OTP while confirming their identity through fingerprint verification.

3.2.2 Verification Page Mechanism

The verification page acts as a user interface in the case of the sender and receiver, instructing them on the input process for the OTP as well as fingerprint.
Features of the Verification Page:
OTP Display : OTP prompt is being displayed on the screen to the user.
Fingerprint Guidance: This is a list of prompts that indicate how to use which finger for each digit of OTP.
Confirmation Messages: It confirms each input, either as valid or as invalid, such that if verification is not proper then the transaction cannot be processed.
With such a sequence, the verification page reduces the chances of bypassing or overriding the security sequence.

3.3 ELT Process in the Authentication System

The ELT procedure stands for the process of extraction, loading, and transformation. It has to be put in place for the proper management and verification of data inside the authentication system. Every step involved has a specific function toward accuracy and efficiency in the transaction.
Steps in the ELT Process:
Extraction
Extractor receives data from both the sender and the receiver, which consists of fingerprint and OTP inputs.
Such raw data is recovered using secure web services, wherein accuracy and completeness are ensured.
Loading
Data extracted from the above step is stored on the server's secure database temporarily.
The server processes the data, authenticating the validity of both OTP and fingerprint entries.
Transformation
The server authenticates the data with pre-registered patterns by verification of algorithms through fingerprints and OTPs.
The server sends the validated transaction to be processed if all of these checks are

successful.

3.4 Data Connectors

Data connectors are specialized drivers or middleware components that transmit data between modules and manage interfaces. They are pretty important during attempts to protect as well as transfer data from the OTP generator and the fingerprint scanner to the backend server.

Key Functions of Data Connectors:

Data Pulling: Retrieves OTPs and fingerprints as needed for verification.

Data Conversion: Converts data to be rendered in formats consumable by both the database and client interfaces.

Error Handling: It captures the error that occurs during data transfer and monitors it in order to ensure the system relies well.

3.5 Technologies Used

This system is founded on several technologies that allow safe management of data and communication.

Database Management Oracle 11g

Handles OTP, fingerprint mappings and transaction logs.

Encryption and access are provided for safe-keeping of data.

Web Services SOAP/REST APIs

It allows for real-time dissemination of OTP and collecting of fingerprint data.

It utilizes the throught way of encrypted communications in the conveyance of data safely

Fingerprint Scanner API

It serves as an interface to the hardware of fingerprint capturing and its verification.

The collection process of fingerprint input is performed based on OTP-digit mapping for solid verification.

3.6 JPublisher

JPublisher will act like a middleware whereby classes of Java connect the Oracle database objects. This middleware therefore guarantees that verification will come safely with efficient data handling.

Features of JPublisher

SQL to Java mapping: Using JPublisher, database structures from SQL are converted into Java classes for easy manipulation of the data.

It integrates OTP with web service calls for fingerprint data retrieval.

Database Optimization: Data handling becomes more efficient with fast authentication.

3.7 Sample Workflow Code for Dual Authentication

Below is an expanded Java code snippet that demonstrates the authentication process. This code cross-references each OTP digit with a specific fingerprint position, ensuring that both sender and receiver follow the security sequence.

```
public class DualAuthTransaction {
   private String[] getRequiredFingerprints(String otp) {
      String[] fingerprintMapping = {"left_thumb", "right_thumb", "left_index", "right_index", "left_middle", "right_middle", "left_ring", "right_ring", "left_little", "right_little"};
      String[] requiredPrints = new String[otp.length()];
      for (int i = 0; i < otp.length(); i++) {
         int digit = Character.getNumericValue(otp.charAt(i));
         requiredPrints[i] = fingerprintMapping[digit];
      }
      return requiredPrints;
   }
   public boolean authenticateUser(String userType, String otp, String[] fingerprints) {
      String[] requiredPrints = getRequiredFingerprints(otp);
      for (int i = 0; i < otp.length(); i++) {
         if (!fingerprints[i].equals(requiredPrints[i])) {
            return false;
         }
      }
      return true;
   }

   public static void main(String[] args) {
      DualAuthTransaction transaction = new DualAuthTransaction();
      String otp = "6015";
      String[] senderFingerprints = {"left_thumb", "left_little", "right_thumb", "left_ring"};
      if(transaction.authenticateUser("sender", otp, senderFingerprints)) {
         System.out.println("Sender authenticated successfully.");
      } else {
         System.out.println("Sender authentication failed.");
      }
   }
}
```

In this workflow, each digit of the OTP is matched with the corresponding fingerprint. The code checks each step, rejecting the transaction if any sequence fails to match. This approach provides both sender and receiver authentication, achieving a secure transaction environment.

Chapter 4

System Design and Implementation

4.1 Overall System Architecture

Figure 1: Abstract System architecture

This project's overall system architecture is built on two main modules that are designed to work together to provide a safe and effective online banking transaction user experience. The fingerprint sensor and microcontroller, which are in charge of gathering and sending fingerprint data, make up the first module. In particular, a user's fingerprint is captured and converted into a digital representation using an optical fingerprint sensor, such the AS608. The microcontroller in this module, an Arduino UNO, serves as a middleman by reading, processing, and securely sending the fingerprint data to the server for real-time verification. Standard protocols like UART facilitate communication between the sensor and microcontroller, and peripheral parts like power supply circuits guarantee smooth operation. Encryption mechanisms protect the transmission of fingerprint data, providing an additional line of defence against data intrusions.

The bank's web server, which is the second module, is in charge of handling the data that the microcontroller sends it and carrying out transactions after authentication. A strong framework, like Node.js, was used in the server's construction. It can manage several client connections and serve as a reliable interface between the database and the front end. Fingerprint templates along with relevant user information are stored in a secure database such as Firebase, which guarantees quick retrieval and comparison for authentication. After receiving the fingerprint data, the server verifies the user's identification by comparing it against templates that have been saved. The server adds a dual-layer security check by asking the user for an OTP input if the fingerprint is

verified. The OTP verification module compares the code that is saved on the server with the one that is supplied by the user. The server approves the user's requested banking transactions after a successful verification. Furthermore, entering OTPs and viewing transaction results are made easy with a front-end user interface.
Secure channels, usually HTTPS or secure WebSockets, are used for communication between the microcontroller and the server. TLS/SSL encryption is used to guard against unwanted interception. This guarantees the preservation of data confidentiality and integrity during the transaction process. OTP verification and fingerprint matching combine to create a dual-layer authentication system that greatly improves security. To stop replay attacks and illegal access, the architecture also incorporates security best practices including session management and OTP expiration.

4.2 System Components and modules

The project's system modules and components, which include an optical fingerprint sensor and an Arduino UNO board, have been carefully designed to provide a reliable and secure method of user transaction authentication. Each of the two primary modules that make up this system is essential to the project's overall security and functionality.

4.2.1 Fingerprint Sensor and Microcontroller module

This module is in charge of collecting and transmitting biometric information, which is essential for the first stage of user verification. This module’s main elements are as follows:

Optical Fingerprint Sensor (AS608): The AS608 optical fingerprint sensor takes pictures of fingerprints and creates digital templates from them. It works by using an optical lens to scan the user's fingerprint, producing sharp digital images that can be processed for matching. Algorithms for fingerprint feature extraction are integrated within the AS608 sensor, guaranteeing secure and accurate data transmission.
Microcontroller (Arduino UNO): This module’s main processing unit is the Arduino UNO. It uses a UART (Universal Asynchronous Receiver-Transmitter) communication protocol to interact with the fingerprint sensor, enabling effective data transfer. The programming required to initiate fingerprint scanning, receive data from the sensor, and transmit it to the server for validation is built into the microcontroller, which is written using the Arduino IDE. Additionally, the microcontroller has software libraries that improve the system’s processing power and enable communication. Power Supply: For the Arduino UNO and fingerprint sensor to work properly, this module needs a reliable power source. To guarantee continuous functioning, this could involve a rechargeable battery unit or a controlled DC power source.

4.2.2 Web server and backend processing module

The second module of the system is focused on handling authentication requests and facilitating transactions post-verification. The main components include:
Web Server (Node.js): Because of its high scalability and non-blocking I/O capabilities, Node.js was used in the development of the server. It serves as a link between the central repository and the fingerprint sensor module. The microcontroller sends fingerprint data to the server, which processes it and connects to the database to compare the fingerprint to templates that have been recorded. Additionally, the server must safely handle client requests and manage session data.
OTP Generation and Verification System: This subsystem offers a dual-layer authentication mechanism and is integrated into the server module. The user's registered device receives the generated OTP (One-Time Password), usually by SMS. To guard against replay attacks and guarantee timely input, this OTP is kept in the database with a restricted validity duration. Before allowing access to transactions, the server verifies authentication by processing and comparing the user's OTP with the stored OTP.

4.2.3 User Notification System

The system includes a notification feature that lets users know when an OTP has been created and transmitted in an effort to improve the user experience. To guarantee dependable delivery, this notification system is integrated with Twilio, a third-party SMS/email provider. Push alerts can also be added to mobile apps that are connected to the banking system.

4.3 Detailed Data Flow

This project's data flow is made to guarantee a safe and effective transaction authentication procedure. The process is first started by the user by touching the fingerprint sensor with their fingers. The mapping figure E (e.g., thumb as 0 and index finger as 1) is used by the optical fingerprint sensor (AS608) to collect and scan the fingerprint image. After being transformed into a digital template and processed by the Arduino UNO microcontroller, the fingerprint data is safely sent to the bank's web server.

A fingerprint-numeric input system is used to enter the OTP. The user taps their fingers in the order that corresponds to the numeric values assigned to each finger (thumb for 0, index finger for 1). This sequence is read by the microcontroller, which decodes it into the numeric OTP and relays the information to the bank's web server. The entered OTP is compared to the previously generated saved OTP by the server. The server verifies successful authentication and starts the requested transaction if they match and fall within the allotted time frame. However, the server notifies the user of the unsuccessful verification if the OTP is wrong or the time window has passed. This allows for additional security measures, such as account lockout after several unsuccessful attempts.

4.4 System Workflow

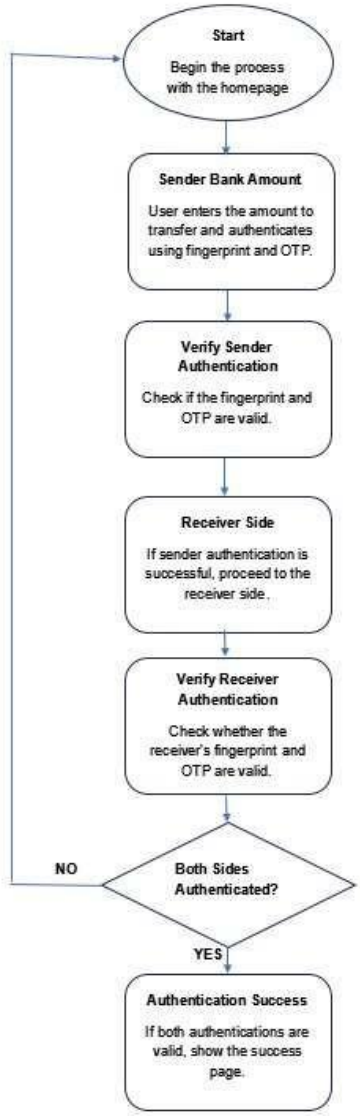

Figure 2: Complete system workflow

The process flow for the complete system including the sender and the recipient during

an online transaction is shown in the system workflow illustrated in figure 2. By ensuring that all parties are safely verified prior to a transaction being approved, this workflow improves the process's safety and dependability. Each stage is explained in full below:

The user starts the procedure by starting the transaction on the homepage. This is where the transaction and authentication processes begin. The sender enters the amount they want to transmit in the first stage. Using a two-layer process that includes fingerprint-numeric OTP (One-Time Password), the sender must now authenticate themselves. While the OTP is generated and verified for accuracy, the fingerprint sensor reads the fingerprint and sends it to the system for validation.

The system proceeds to the Sender authentication phase when the sender has input their credentials. This entails verifying the sender's fingerprint and OTP are valid. The sender's authentication is considered successful if the fingerprint and OTP match those kept in the secure database and the time limits are met. The procedure stops and the sender is informed of the unsuccessful authentication if this verification is unsuccessful.

The workflow moves on to the "Receiver Side" stage, where the system gets ready to authenticate the recipient, if the sender's authentication is successful. To verify their identity and give permission for the transaction to be received, the recipient must also go through a similar authentication procedure. The receiver enters their OTP and fingerprint information, which the system processes and verifies.

Next comes the "Verify Receiver Authentication" stage, in which the system compares the stored records with the recipient's fingerprint and OTP. This guarantees the legitimacy and authorization of the individual receiving the transaction. The transaction is not finalized and the recipient is notified if this step is unsuccessful.

At last, the procedure arrives at the "Both Sides Authenticated?" decision point. In this case, the system checks to see if the sender and recipient have completed their individual authentication processes. The transaction is authorized and the system notifies the participants with a success page if both parties have successfully authenticated. The procedure ends and a notification or error message indicating the transaction's failure is shown if either side fails the authentication tests.

This methodical process makes sure that the sender and recipient are fully validated using dual-factor authentication, which combines biometric information and one-time passwords, thereby strengthening the security of online transactions. A strong system like this reduces the possibility of fraud and illegal access, giving users in delicate financial transactions an extra degree of security.

4.5 Technology Stack

a. Hardware:

- Arduino UNO
- Optical Fingerprint Sensor (AS608)

b. Software:

- Arduino IDE
- Embedded C/C++, Python

c. Web Server:

- Node.js
- Express.js

d. Front-End:

- HTML/CSS
- JavaScript
- Bootstrap

e. Communication and Integration:

- WebSockets
- Serial Communication

f. Security:

- Encryption Protocols
- OTP Generation Algorithm

g. Development and Testing:

- Postman
- Git/GitHub

h. Operating System:

- Windows/Linux

Chapter 5

Result and Discussion

The components were put together successfully. The Arduino Uno has been configured correctly to serve as the circuit's central processing unit, allowing for effective communication between the device and the optical fingerprint sensor. In order to authenticate the user during OTP verification, the fingerprint data is read and stored by the optical fingerprint sensor. The Arduino UNO quickly alerts the PC if there is a match between the stored data and the scanned fingerprint data during the verification procedure. This feature makes the system more secure and guarantees that sensitive data can only be accessed by authorized users.

The banking system establishes a secure link with the user's account details when the user opens the bank's webpage, and Figure 3(a) shows the system's initial webpage and Figure 3(b) displays the system's hardware configuration. The website gives the user the ability to complete a number of transactions, including such as transferring money, checking account balances, withdrawing or depositing money, and more. The page's layout is simple and easy to use, with unambiguous directions and buttons that are simple to understand for smooth navigation. The system uses strong security protocols to guarantee the safeguarding of users' financial and personal information during the course of the transaction.

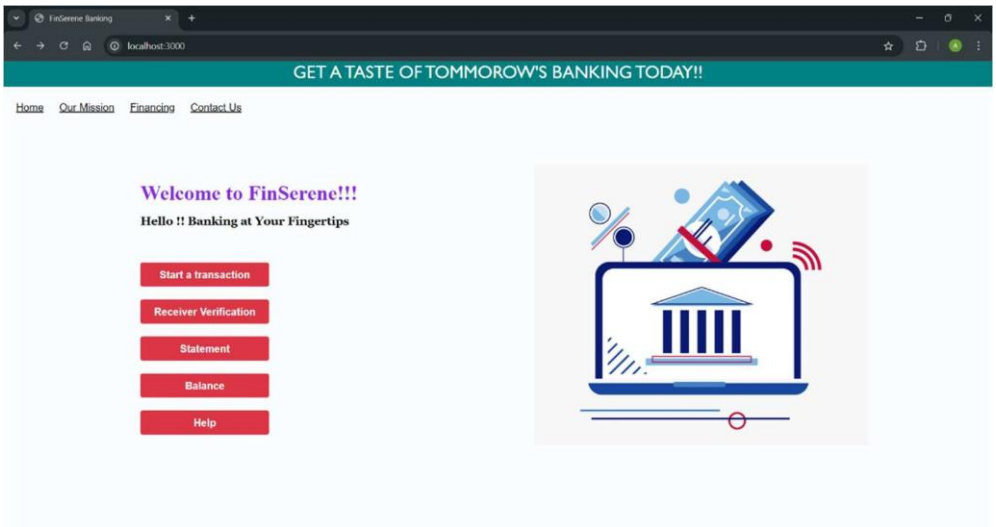

Figure 3(a)

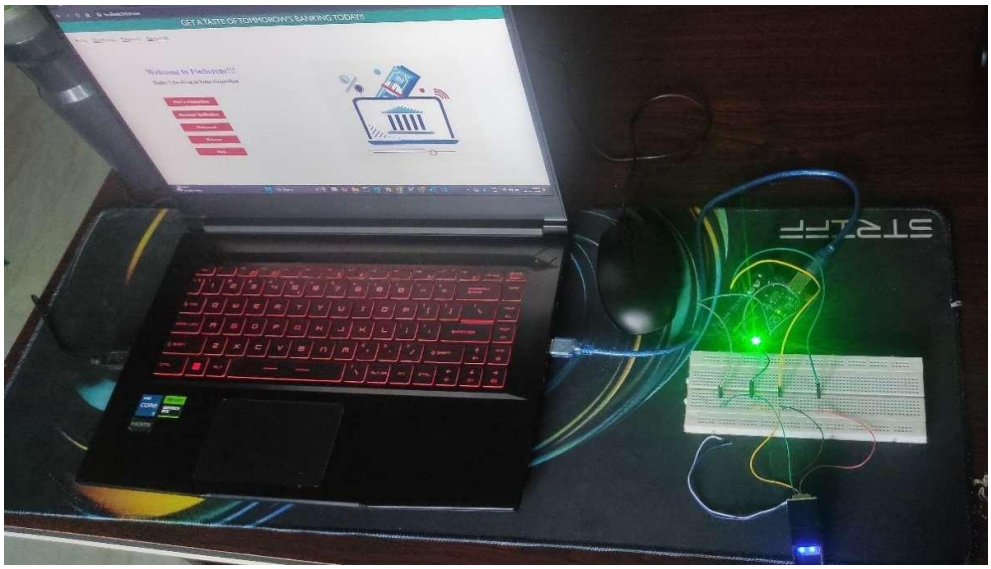

Figure 3(b)

The user is redirected to the next page after choosing the 'Start a transaction' option on the first webpage of the banking system, where they are required to enter the OTP that was sent to their registered mobile number, as shown in Figure 4. Clear instructions on which digits should be manually typed using the keyboard and which should be checked with fingerprints are provided on the homepage. As seen in Figure 5, the letter 'F' stands for a digit that has to be confirmed by the fingerprint scanner, and the letter 'N' for a digit that needs to be manually entered. The user is guaranteed a smooth and safe transaction process thanks to this intuitive UI

.

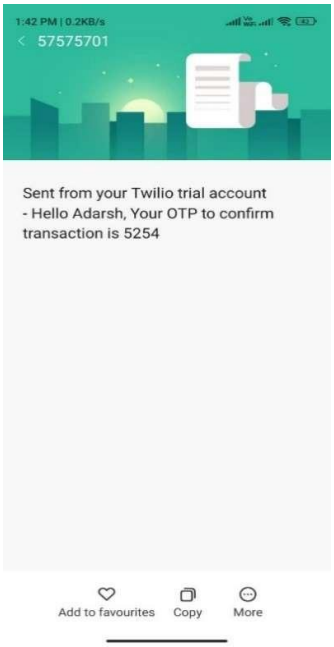

Figure 4

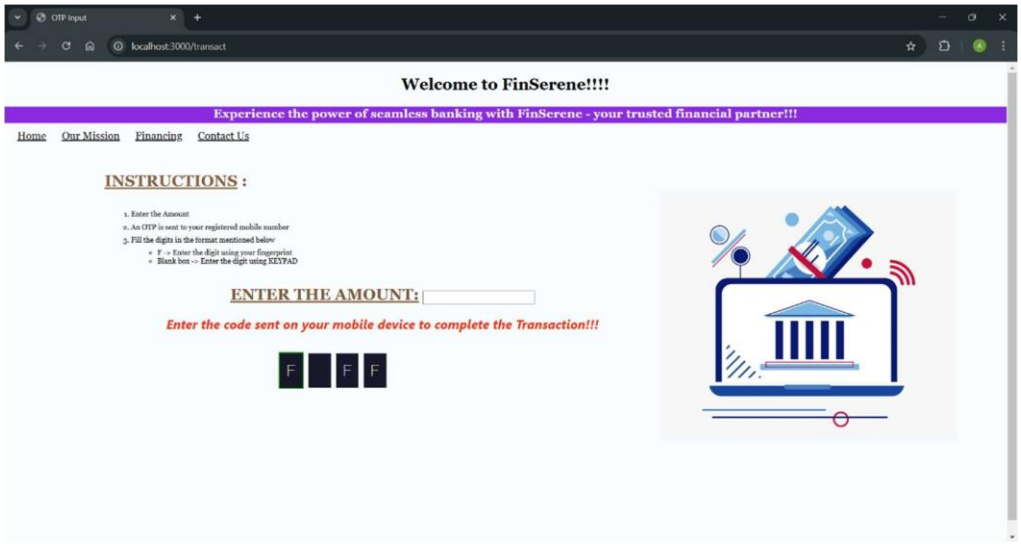

Figure 5

After that, the user enters the OTP in the appropriate field. This step gives the system an extra degree of security by guaranteeing that only the authorized user can access the transaction.

The banking system displays a pop-up notification confirming whether or not the user entered the OTP correctly after they have done so. This guards against unwanted access and guarantees the security of the user's account. In order to better understand user behaviour and enhance the user experience, the system also keeps track of how long it takes the user to input the OTP.

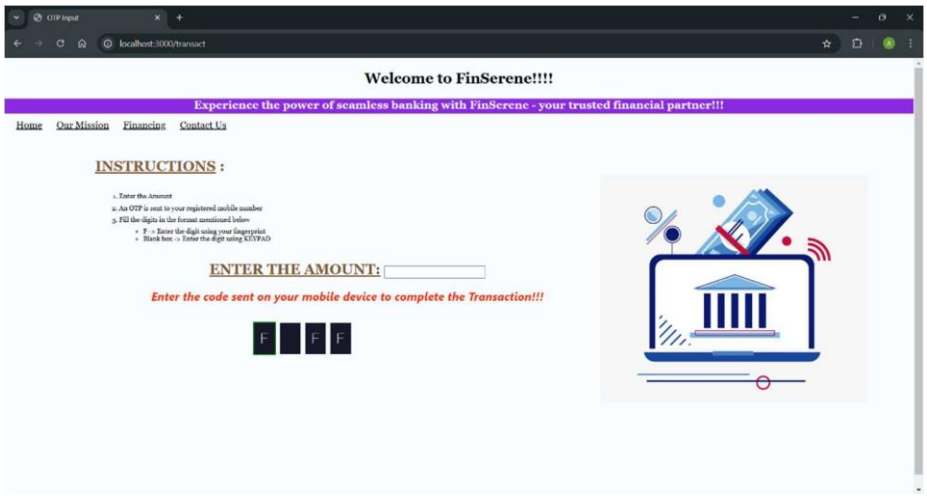

Figure 6(a): Sender side Authentication Page

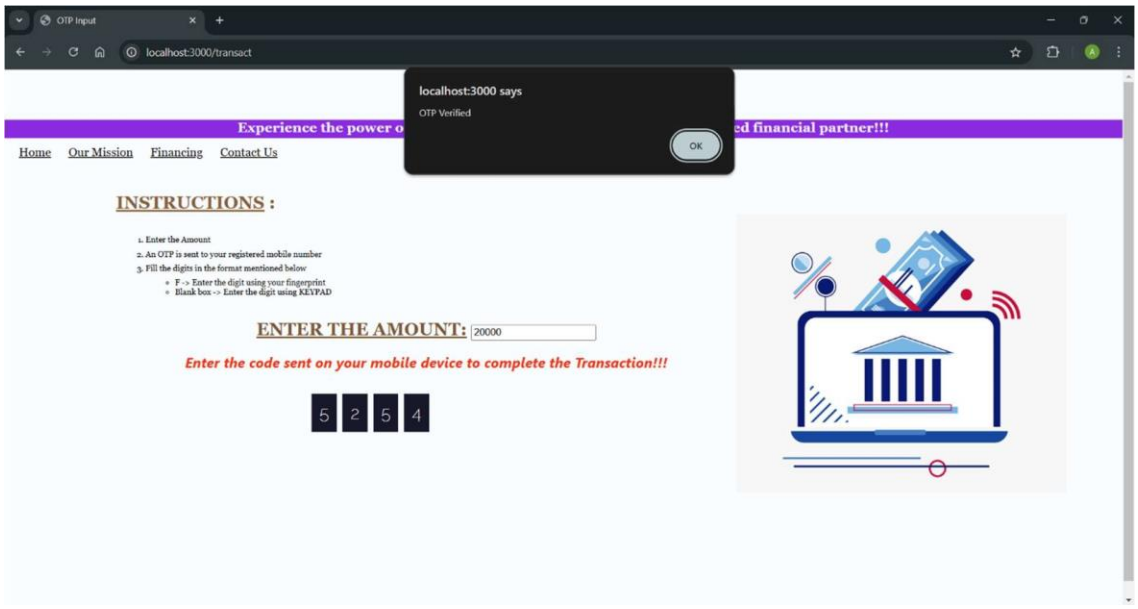

Figure 6(b): Sender side after Successful authentication

The user will be taken to the success page following the sender's successful authentication, where they will see a notice stating that the money will only be taken out of their account following the recipient's successful authentication. This procedure guarantees that the money sent by the sender is only being received by the designated user.

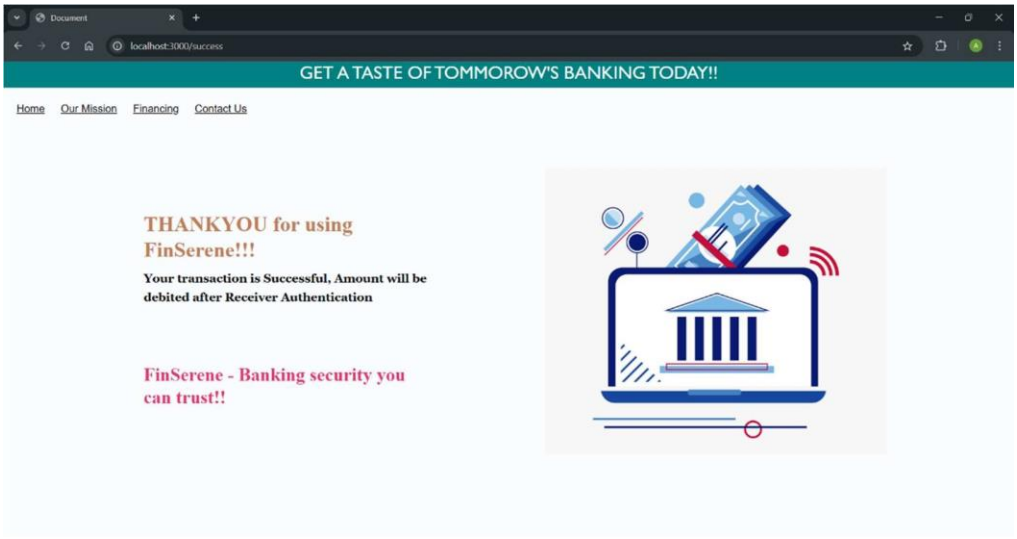

Figure 7: Sender side Success page

Additionally, the recipient will receive an OTP, which they must enter into the gateway in order to verify their identity. The authentication page on the recipient side is displayed in Figure 8(a). The recipient will be taken to the success page when the OTP has been validated, as illustrated in Figure 8(b), where they can observe that the money has been credited to their account and that a confirmation message will be issued to the sender shortly.

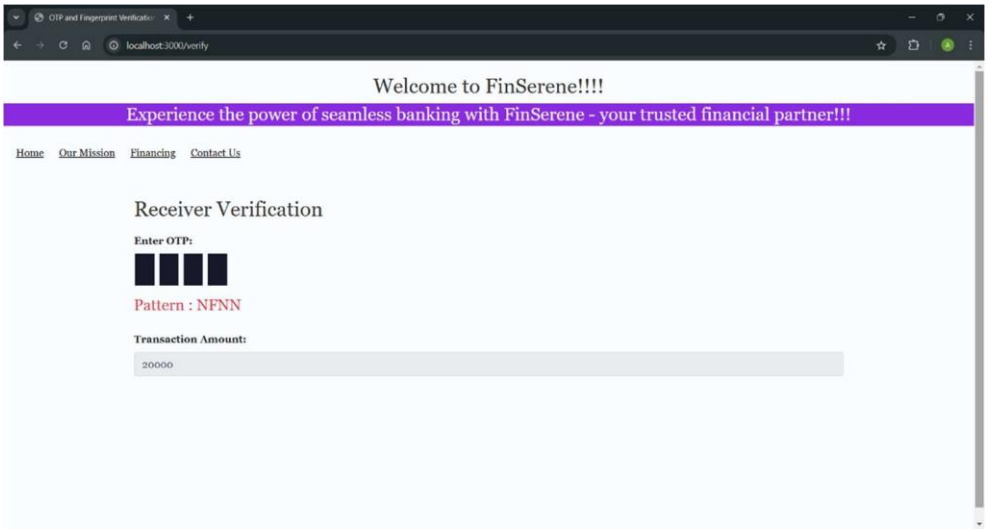

Figure 8(a): Receiver side before authentication

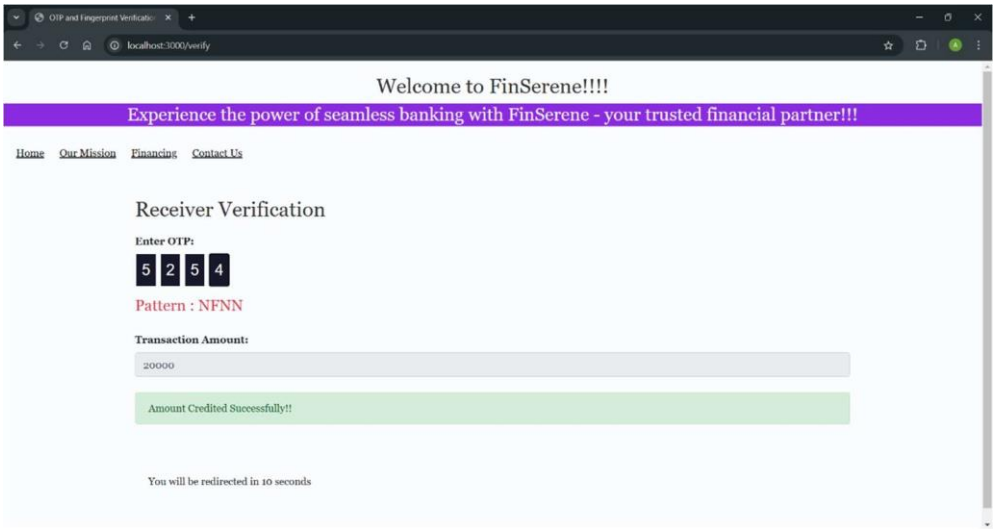

Figure 8(b): Receiver side after authentication

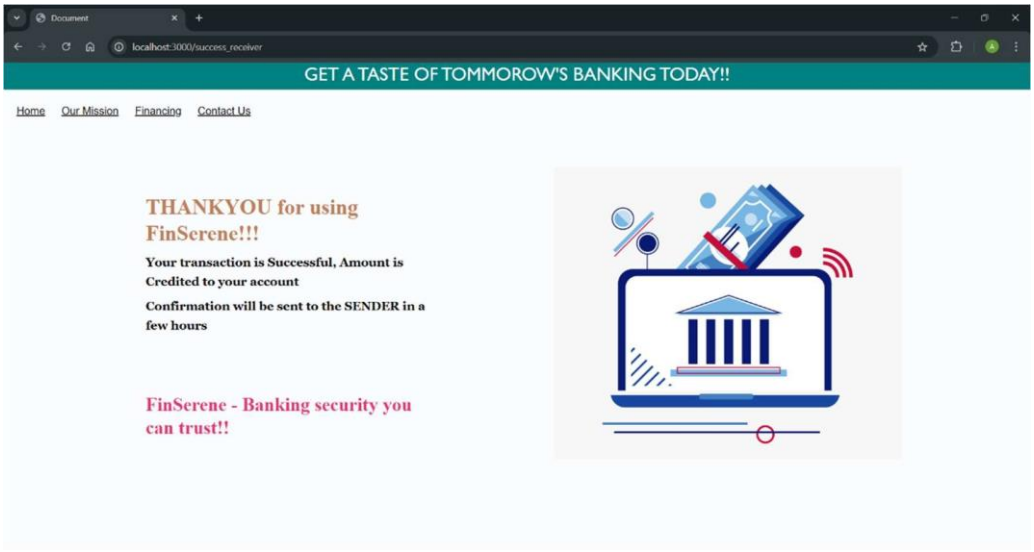

Figure 9: Receiver side Success page

Chapter 6

Conclusion

This project integrates an Arduino UNO board with an optical fingerprint sensor to demonstrate a robust and effective way of verifying OTPs to keep great security in accessing a user account. The successful completion and testing of this project confirm that the system is able to consistently recognize and validate users' fingerprints in such a way that only authorized people will be allowed to continue their transactions.

The most obvious advantage is the capturing of high-resolution images, definitely an enhancement to the accuracy of biometric authentication. This layer of protection dilutes the risks that normally come along with traditional OTP approaches, which are secure but vulnerable to phishing attacks or SIM-swapping frauds. Adding the biometric verification procedure brings a highly important second level of security to the project, making it much more difficult for unauthorized users to gain access that is legal.

The web-based interface developed as part of this contribution of improvement in user experience about the transaction process because it is intuitive and straightforward. It ensures a faultless interaction of users with the system from any place they could access the internet, which simplifies identification verification while performing sensitive activities on the Internet. Biometric and OTP integration in one easy-to-use platform manages both convenience and security concerns that can be useful in one all-inclusive solution for end-users.

This is from a technical standpoint, a proof of concept to show the possibility and efficiency of building a microcontroller-based system, similar to the Arduino UNO, to further support biometric verification. That this project has been developed using open-source hardware and software and opens up possibilities for scalability and customization means that similar approaches can be brought about with regard to other critical applications, such as secure facility access, financial services, or e-commerce transactions.

Therefore, this project points out the practical advantages of integrating biometric technology with traditional authentication methods. Multi-factor security will improve the safety of the system besides being in sync with the current trends in cybersecurity, such as the implementation of multiple layers of defence. Systems like this are offered as the best response at a time when cyber threats are constantly changing by introducing a fusion of something known (OTP) and something one is (biometric data).

In a manner of speaking, the outcome of the present study has much to offer in informing future work in taking robust and secure models of online banking systems where protection of user data and prevention of unauthorized access becomes a prime necessity. This study can be found to also act as a key step and springboard for further enlarging the scope of elaborating how further development using biometric advancement such as facial recognition or voice authentication can be integrated, potentially opening newer fields where such security measures can be enacted.

This project tests how a microcontroller-based system harmoniously integrates with biometric verification-a step further ahead in security that goes along with online transactions. This project, incorporating an optical fingerprint sensor and interfacing this sensor with an Arduino UNO and OTP verification, not only gives life to the feasibility of the approach but also sets a trend for future research and development in this arena: safe online banking and similar applications. In principle, the proposed system has shown the potential to safely contribute to digital environments while eliminating risks of fraud and ensuring for users a trustworthy method for personal and financial information protection.

Appendix A: Code Listings

A.1 Python Code for Fingerprint Integration

```
from serial import Serial
import random
import time
ser = Serial(
    port='COM3',
    baudrate=9600
)
ser.isOpen()
def writeToFile(msg):
    f = open("output.txt", "a")
    f.write(str(msg))
out = ""
ser.readline()
while(True):
    out = ser.readline().strip().decode("utf-8")
    if "Found ID " in out:
        break
# out = int(out.split(" ")[2])%10
try:
    out_value = out.split(" ")[2]
    out = int(out_value.strip("#")) % 10  # Strip the `#` and convert to integer
except ValueError:
    print(f"Error: Could not convert '{out_value}' to an integer")
    # Handle the error (e.g., set a default value or skip this iteration)
    out = None

writeToFile(out)
```

A.2 NodeJS code for integrating OTP service with web server

```
var express = require('express')
var app = express.Router()
app.use(express.urlencoded({ extended: false }));
const path = require('path')

app.use(express.json());
var fs = require("fs");

app.use(express.static(path.join(__dirname)))

function readFileSync(file)
{
   return new Promise((s,r)=>{
      fs.readFile(file, (err, data) => {
         s(data.toString())
       })
   })
}

app.get('/transact',async(req,res)=>{

   var pin = ""
   var order = ""

   await readFileSync('./pin.txt').then(async(data)=>{
      pin=data
      await readFileSync('./order.txt').then((res)=>{
         order=res
      })
   })
    console.log("yep",pin,order)

   res.render('home.ejs',{pin:pin,order:order})
})
```

```
app.post('/generate',(req,res)=>{

    let pin = req.body.pin
    let order = req.body.order
     console.log(order,pin)

    fs.writeFileSync('pin.txt', pin.toString(), function(err) {
        if (err) {
          return console.error(err);
        }
    })

    fs.writeFileSync('order.txt', order, function(err) {
        if (err) {
          return console.error(err);
        }
    })

    res.send("ok")
    var pstring = pin.toString()
    var twilio = require('twilio');
    var client = new twilio('AC42c125b39304c68b3c0dd0f87035ed85',
              'e722286b9ccbb4da919633e2fadf966f');
    client.messages.create({
    to: '+918714583425',
    from: '+13153815047',
    body: `Hello Adarsh, Your OTP to confirm transaction is ${pstring}`
    });

})


app.get('/success',(req,res)=>{
    res.render('success.ejs')
})

app.get('/success_receiver',(req,res)=>{
    res.render('success_receiver.ejs')
```

```
})

app.post('/getfingerprint',(req,res)=>{


const { spawn } = require('child_process');
const child = spawn('python', ['test.py'], {shell: true});

child.on('close',(code)=>{
    readFileSync('./output.txt').then(async(data)=>{
        val = data.toString()
        console.log(val=="")
        if(val!="")
        {
            finger_sensor_data=val
            res.send(val)
            fs.writeFileSync('output.txt', "", function(err) {
                if (err) {
                  return console.error(err);
                }
            })
        }
        else
        {
            finger_sensor_data='N'
            res.send('N')
        }
    })
})

})

module.exports = app
```

Bibliography

[1] Gao, et al. ”Multilevel Security and Dual OTP System for Online Transactions,”IEEE, 2018.

[2] Mondal, P. C., et al. ”Transaction Authorization from KYC Information,” IEEE,2023.

[3] Viswesh, G. & Vinothiyalakshmi, P., ”Secure Electronic Banking Transaction usingDouble Sanction Security Algorithm,” IEEE, 2023.

[4] D. Datta, S. Sarkar, and P. Bhowmick, "Design and Implementation of Online Banking System with Two Factor Authentication," International Journal of Computer Applications, vol. 107, no. 10, pp. 29-34, Dec. 2014.

[5] S. Singh and S. Sharma, "Design and Implementation of Online Banking System with Fingerprint Authentication," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 10, pp. 275-280, Oct. 2016.

[6] Mishra, A., Yadav, D., Yadav, N., & Tiwari, N. (2019). ATM security system using biometric identification technique. In 2019 International Conference on Advanced Computing and Intelligent Engineering (ICACIE) (pp. 136-140). IEEE.

[7] Nasir, A. A., Usman, M., Ullah, A., Hassan, M., & Riaz, M. N. (2018). Design and development of fingerprint authentication and verification system for ATM security. In 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST) (pp. 494-498). IEEE.

[8] Gohil, P., & Patel, A. (2019). Fingerprint authentication and verification system for ATM security. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 63-68). IEEE.