GKU Journal of Multidisciplinary Research (GKUJMR)

Touch-Based Fingerprint Biometric Payment System for Quick and Secure Transactions

[1] Abdul Kalam, [2]Tareef Anwar, [3]Dr. Manpreet Kaur

[3]Assistant Professor ,[1,2]Student, Faculty of Computing, Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India.

Email: [1]abdul24313299@gku.ac.in, [2]anwartareef6@gmial.com, [3]apmanpreetkaur@gmail.com

Accepted: 26.11.2025 Published: 26.12.2025 DOI: 10.5281/zenodo.18113676

Abstract – With the increasing demand for secure and convenient payment methods, biometric authentication has gained significant attention [1]. In this paper, we propose a touch-based fingerprint biometric payment system to achieve fast, reliable, and secure transactions without carrying cash or smartphone. It combines fingerprint recognition technology with banking infrastructure [2], which allows the payment to come directly from the user account upon proper biometric verification. The goal of the project is to overcome the shortcomings of traditional payments and enable the adoption of seamless solutions, improving the experience of using cashless payment in commerce venues. Study this study talk about system design, system implementation and testing using test accounts, security and future works.

Keywords – Biometric Authentication, Fingerprint Recognition, Payment Systems, Touch-Based Payment, Security, Digital Transactions

I. Introduction

Biometric payments found a strong competitor in digital payment technologies which have grown massively over the recent years in the financial sector [3]. Fingerprint recognition is one of the most widely adopted biometric techniques due to its uniqueness, ease of use, and high reliability [1].

Existing fingerprint-based payment solutions generally require physical contact with a sensor, which over time creates hygiene issues and surface wear [6]. Touch-based biometric systems have become important, especially where cashless and cardless transactions are preferred [4].

This paper proposes a touch-based fingerprint biometric payment system that allows customers to make payments directly from their bank accounts by verifying their fingerprint. The system aims to deliver a secure, fast, and user-friendly alternative to cash and card payments, particularly in situations where mobile devices or cash are unavailable [8].

II. Literature Review

Biometric authentication technology has emerged as a key pillar in modern data security architecture, allowing secure authentication in financial, governmental and commercial ecosystems. Email: {chnor, dmazumdar, henryja, vishuna, ksladek}@fiu.edu Abstract Fingerprint recognition has been especially attractive because of it fingerprint being unique, easy to use, and highly reliable in practical applications [1]. The following section provides a brief overview of the state of the art in biometric payment systems, including their advantages and challenges and the transition towards touchless fingerprint recognition technologies

2.1 Existing Biometric Payment Systems

Fingerprint recognition is widely used because it offers a unique, permanent, and measurable biometric trait 1. In India, the Aadhaar Enabled Payment System (AePS) uses fingerprint authentication for secure banking services, enabling transactions in both rural and urban areas [13].

On a global scale, large companies such as Apple and Samsung 15 have integrated fingerprint scanners into their mobile-based payment systems (i.e. Apple Pay and Samsung Pay 15), which require the use of capacitive fingerprint sensors built into the mobile phone for secure transaction confirmations. Fingerprint biometrics increases the security level while at the same time minimizing the need for PIN or password use due to their being recognized as a more convenient, fast, and reliable way of identifying samples [4].

2.2 Touch-Based Fingerprint Authentication: Advantages and Challenges

ouch-based fingerprint sensors—commonly capacitive or optical—capture ridge patterns when users physically place their fingers on the sensor [6]. However, regular contact results in dirt, oil, and moisture accumulation that can degrade accuracy over time.

The public character of such sensors also makes it susceptible to hygiene issues, as demonstrated by the COVID-19 pandemic [8]. The finger recognition failures might get worse when the users have wet, dry, or damaged fingers which could elevate the false reject rates [9].

2.3 Touchless Fingerprint Recognition: Emerging Research

Most fingerprint devices in a cell phone are touch-based fingerprint sensors, partly capacitive or partly optical, which sense ridge patterns when a finger is pressed on. 6 But you do not need to touch a lot with dirt and oil exposure moisture is accumulation will create over time they will lose accuracy 6.

Moreover, even if this type of sensors is available for public use, it raises hygiene issues474, and it was especially emphasized during the COVID-19 pandemic888. In addition to, wet, dry, or damaged fingers will add to the number of recognition failures, which will push FFRs 9 higher [3] as well.

2.4 Current Payment Systems and Innovations that Would Attend to Their Weaknesses

Although biometric payments have come a long way, most of these solutions require a touch-based fingerprint sensor, or they require the user to own a smartphone or card [3] which is a barrier to entry for many users, especially in developing regions888.

It is evident that the current biometric payment is a fast and secure transaction mechanism without any physical contact or the need for additional devices such as smartphones etc. [4]. Your biometric payment system, which uses the fingerprint (using touch) is a promising solution to fill this gap by allowing direct payments through fingerprint verification thus improving the transaction speed and accessibility [2]

III. System Design and Architecture

The general structure and design of the suggested fingerprint-based biometric payment system is outlined in this section [9]. The point of sale (POS) uses fingerprint authentication to provide an easy, fast and secure transaction method [1].

3.1 System Overview

Their system comprises three main components:

- **Fingerprint Scanner Module [9]:** A high-quality fingerprint sensor has to read customer fingerprints. An optical or capacitive touch-based fingerprint sensor is used for accuracy and security in this project.
- **Point of Sale (POS) Terminal** — POS terminal which is also connected to Fingerprint scanner and software that can process transaction automatically. The customer scans his/her fingerprint and the system checks his/her identification, and as the fingerprint on record is associated with the bank account, the payment goes through; thus, money can be withdrawn right from the accessible bank account without any cards, cash, or other issues.
- **Bank Server & Database** — the database or backend bank server saves the user biometric templates as well as account information in a secure manner. The system verifies identity and performs fund transfer after the successful fingerprint authentication via bank server [11]
- **Enrolment of Customer**: At first, customers enrol their fingerprint information with the bank, tying the biometric template to the bank account.
- **Transaction Start** — Customer initiates the purchase of items in the store. The POS terminal is activated by the cashier to initiate a transaction.
- **Fingerprint Scanner** — the customer places their finger on the scanner. The finger print is imprinted and compared with the biometric that is already there.
- **Verification and Authorization:** If fingerprint verification is successful, the POS will request authorization for the payment from the bank server.
- **Payment completion:** The bank server processes the transaction, deducting the payment sum from the customer and then notifying the POS terminal.
- **Receipt Creation:** The digital or printed receipt is generated by the POS terminal for the customer.

3.2 Security Measures

The system consists of the following to ensure data security and privacy: [17]

End-to-End Encryption: Encrypted data transmission from POS terminal to bank server (fingerprint data and transaction ID are encrypted).

A. Fingerprint templates are stored (no raw image permitted [24]).
B. Multi-Factor Authentication: Additional factors such as PIN/OTP can also be added, if required.
C. Anti-spoofing: The fingerprint sensor has built-in liveness detection to prevent false fingerprint attacks. [12]

3.3 Hardware and Software Requirements

A. **Fingerprint Sensor:** high resolution capacitive / optical sensor [6]

B. **POS Terminal**: Embedded system to run transaction software and connect to fingerprint scanner.

C. **Bank end server:** Secure data and deal preparing server facilitated by the bank.

D. **Network Connectivity**: You will require a reliable internet connection with transparent network communication between the virtual webinar participants.

IV. Implementation Details

In this section, the details of all hardware and software components, system integration, and database designing and building of the proposed work in the fingerprint based biometric payment system is described. It addresses all the steps needed to deploy the system, [9] in a real-world setting, with security, reliability, and user-friendliness.

4.1 Hardware Components

4.1.1 Fingerprint Scanner Module

The fingerprint scanner is the central biometric device used to obtain the identifying patterns of fingerprints from users. [6] For this project, a

A capacitive fingerprint sensor is selected due to its high accuracy, high reliability, and low cost. Capacitive sensors identify fingerprint ridges and valleys by measuring differences in electrical capacitance between ridges and valleys.

Some of the most common sensors are GT-521F32 or R305, which support:

- High-resolution fingerprint image capture
- Onboard storage for fingerprint templates
- Fast processing and matching speed

Serial or USB communication interface support

This sensor module supports capturing fingerprints, authenticating users, and deleting fingerprints. It hardens the system with anti-spoofing (or liveness detection) techniques to stop fraudsters from using fake fingerprints. [12]

4.1.2 Microcontroller or Processor Unit

The microcontroller takes the role of the main controller to connect the fingerprint sensor with POS terminal software [7]. Common options are:

- **Arduino UNO or Mega:** These are inexpensive, simple, and work perfectly well for an early stage prototype. This is a serial relationship with fingerprint sensor – UART serial relationship.
- **Raspberry Pi (3 or 4):** A more powerful single-board computer, capable of running a full OS (Linux), allowing more sophisticated software development and internet connectivity to communicate with a server. It comes with USB and GPIO interfacing to the sensors.

For this system, the Raspberry Pi used is preferred because it supports real-time network communication and can be run with higher-level applications, such as Python or Java, which are needed to process the transactions [15].

4.1.3 POS Terminal

POS Terminal is the actual hardware through which the payment transaction will take place [9]. It can be:

• An embedded device with touchscreen display containing fingerprint sensor module.

• An attached fingerprint sensor to a computer or portable computer

Transaction software on the terminal handles the user interface, fingerprint scanning, communication with the bank backend and receipt printing.

4.1.4 Communication Modules

Network Connectivity Network connection in other words is necessary for secure communication between the POS terminal and the bank server. This can be:

- Store based fixed POS terminals, connected via Ethernet cable.
- Mobile or Portable POS Terminals Wi-Fi or 4G/5G Modules

The network-level data exchange must be protected against eavesdropping and modification according to confidentiality and integrity requirements [11].

4.2 Software Development

4.2.1 Enrolment Software

1) **Enrolment:** This is the first step involved where the customers register their fingerprints to the system [6]. This is what the enrolment software does:

- Scans fine quality fingerprint with sensor.
- Extracts distinctive characteristics (such as ridge endings and bifurcations; minutiae points) from the fingerprint
- Transforms these features into a fingerprint template — basically a mathematical confidant secret of your biometric fingerprint saved, instead of a visual fingerprint, for better security and privacy.
- Encrypts the fingerprint template and uploads securely to bank central database, combining the fingerprint recognition data with the user account information.

The software features easy-to-use UI prompts to guide customers through the enrolment process to capture a good quality fingerprint [14].

4.2.2 Authentication Module

A. The authentication module [9] during a transaction
B. Using the sensor, it takes a live picture of the customer's fingerprint.
C. Fingerprint features are captured and a template is made.
D. Uses the captured template to compare with the stored template so as to authenticate This can be done either:

Locally on the POS terminal if templates are store locally for fast validation.

- Or from a remote location, by transferring the fingerprint template for match & validation through a secure protocol network to the bank server.

When two fingerprints are paired, the authentication algorithm evaluates the images and indicates a similarity score; if the score is higher than a threshold — the fingerprint is accepted and access is granted to the user.

4.2.3 Transaction Processing System

After successful authentication:

- The transaction software gives the total amount due.
- It communicates with the bank server, sending a payment authorization request that includes the user ID and transaction amount.
- Account balance validation and transaction authorization by a bank server.
- The POS terminal receives a confirmation back.

Transaction completion through a digital/printed receipt generated by the terminal

This software allows cashier and customer to receive real time transaction success or failure information [11].

4.2.4 Backend Bank Server Software

The backend system is responsible for [11]:

- Keep the user data and fingerprints secure storage.

Using matching algorithms that are fine-tuned to deliver the highest accuracy in fingerprint recognition

Managing transaction requests and adjusting account balances

Keeping full transaction logs for auditing and to be able to resolve disputes

A powerful database management system (e.g., MySQL, PostgreSQL) with encryption for sensitive data at the backend.

Secure HTTPS-based API endpoints enable communication between the POS terminal and the Bank server in a secure environment.

4.3 Database Design

Biometric data and transaction records should be stored in a secured database that is designed in a way to be able to efficiently organize biometrics as well as transaction records for each user [5].

4.3.1 User Table

Contains:

UserID: It is a unique identifier for the customers

Customer Name — Full customer name

Account Number — Refers to the number of the associated bank account

Template: Fingerprint Template (not raw fingerprint image only template)

Registration Date: Timestamp of enrolment.

4.3.2 Transaction Table

Contains:

• Transaction ID: For every transaction, a unique ID.

• UserID: Foreign key to user.

New merchant identifiers: The identifier for the store/merchant

• Timestamp: When the transaction happened.

• Amount: Payment amount.

• Status: Transaction status (success/failure).

Remarks: Notes (optional: note about an exception or dispute)

4.3.3 Security and Privacy

• AES-256 (or the equivalent crypto standard) is used to encrypt data [7]

• Access Control: Only authorized personnel are able to access sensitive information, enforcing role-based access control.

Use audits and backups regularly to safeguard data loss and detect irregularities

4.4 System Integration and Testing

System integration provides that each hardware and software element of fingerprint biometric payment works in harmony as a single framework [9]. Integration Testing: Testing is done to check whether the functionalities, security, and performance are working fine after integration. It identifies errors, enables swift and safe transfer functions and assures the system is ready to go live in the real world.

4.4.1 Hardware Integration

• The connection of the fingerprint sensor with the microcontroller or Raspberry Pi occurs via UART or USB.

• Power supply & Communication lines are T tested & proved, for no drift or instability.

• Test user-friendliness of POS terminal touchscreen and software interfaces

4.4.2 Software Integration

• Fingerprint SDKs are integrated into POS software.

• Protocols (HTTP/HTTPS or socket programming) for communication with the server.

They are then augmented with security layers such as SSL/TLS encryption

4.4.3 Testing Procedures

- Functional Testing – It tests fingerprint enrolment, matching accuracy, transaction flow, and receipt generation.
- Performance Testing: It can be used to measure, transaction processing time, network latency, and system throughput.
- Security Testing: Test sending a spoofing attack, encryption resistance, secure data storage
- User acceptance testing: Actual users are testing the system in a controlled context to determine the usability and comfort of the solution [14].

4.5 Implementation Challenges and Mitigation

- Finger Print Quality: The quality of the finger print captured must be good for different environments (wet/dry fingers).
- Spoof detection: The ability to implement strong anti-spoofing measures to counter fake fingerprint attacks.

- Network Resilience: Managing transaction failures resulting from network connectivity disruptions using approaches such as local caching and retrying.
- Privacy Issues: Need to comply with data protection laws and user consent for usage of biometric data [12]

V. Testing and Evaluation

Testing and validation are some of the most important stages in the development of any biometric payment solution. These steps make sure that the system works, is fast, is secure, and has a good user experience. Here, we detail the complete testing method, results, and analysis of our project based on the biometric payment method using fingerprints [9].

5.1 Functional Testing

This type of testing deals with functional testing, which means checking whether each element of the system operates properly.

- Fingerprint Enrolment: Enrolling user fingerprints into the database that will store the system. This process was performed multiple times with different users in order to verify that the biometric data was being correctly captured and recorded by the system. The success rate of users whose fingerprints were successfully enrolled (enrolment success rate).
- Authentication Correctness: Once a user was enrolled, the system was then tested to see if it could correctly identify the user during fingerprint scans. Two key metrics were used:
- True Acceptance Rate (TAR): How often the authentication will successfully authenticate an actual user.
- False Acceptance Rate (FAR): It is the rate at which a security risk will be raised, if an unauthorized user is accepted.
- TP (Transaction Processing): This proved that after a user is authenticated, the payment transaction is properly initiated—debiting the amount from the customer and generating a receipt for the merchant.
- Edge case testing: The system was also tested in edge-case scenarios, such as partial fingerprint scans, a dirty / wet finger, and power outage during transaction to ensure the robustness.

5.2 Performance Testing

Performance testing tests the speed and efficacy of the system that guarantees seamless functioning for retail [2].

Fingerprint Scan time: It indicates the time required by the sensor to read the fingerprint and convert it into a digital template, which was targeted to be less than 2 seconds.

Matching Time: This is the time taken to compare the scanned finger print with the available templates in the data base and was less than 1 second.

- Transaction Processing Duration: To minimize user, wait time, the total time taken from fingerprint scan to transaction confirmation was required to be up to 5 seconds.
- Load Testing: This test evaluated the performance of the system when subjected to concurrent multiple transactions. It ensured that the system does not slow down or crash at peak times of usage [14].

5.3 Security Testing

In [12] Security testing verifies that the system is safeguarded against different Somali threats with respect to both user information and transaction integrity.

- Encrypted: We encrypt every fingerprint template and transaction data both in stored and from network to ensure that it cannot be accessed by an unauthorized third party. Through this, its own encryption protocols were put to the test.
- Spoofing Attack Resistance: Samples of real fingerprints as well as those crafted from silicone moulds to trick the scanner were used in further tests. Correctness was established for the integration of liveness detection algorithms that differentiate between live fingers and copies.
- Network Security: Encryption-based communication protocols were used to safely set up a communication channel between the POS device and bank servers.
- (for instance, TLS/SSL) to safeguard against man-in-the-middle or data interception.
- Access Control: Access controls (role-based access restriction) were verified to ensure that only authorized personnel access sensitive biometric and transaction data.

5.4 Usability Testing

Usability testing tests how easily customers and merchants can use the system [7].

- User reviews: Opinions were gathered from different types of customers to understand how they felt about the convenience of utilizing fingerprint-based payments without the need for physical cards or smartphones.
- Tested the clarity and usability of the interface in the POS for navigability and intuitive usability to have the least amount of training.

Training Requirements: The system was evaluated on what level of user-training was necessary and should be at a level, which can be performed most effectively with the least training [11]

5.5 Evaluation Results and Discussion

- Identify legitimate ID users — we attain a True Acceptance Rate (TAR) of ~98.5% accuracy on capturing a person whose face passes through system

- False Acceptance Rate FAR was less than 0.5%, which emphasizes the defence against unauthorized access.
- The fingerprint scanning and matching process took an average of 2.5 seconds, allowing the transaction to the complete in less than 5 seconds, which is adequate for a real-world retail environment.
- Since all attempts of fake fingerprints were blocked by the spoof detection mechanisms, the system has also proven its resilience to biometric fraud.
- Receives user friendly feedback, largely with people who do not own smartphones or pay cards, very well received for the convenience it brings to user and the opportunity for financial inclusion.
- There were a few limitations observed, such as some issue in scanning torn fingerprints, which requires advancement in sensors [12]

5.6 Limitations

- User with badly damaged or absent finger print will not work for the finger print biometrics e.g., a manual worker or elderly person.
- Stable internet connection will be needed for the real-time transaction processing, which can be an issue in certain areas which are either remote or low on connectivity.
- During the enrolment or setting up of the system, the process should be handled very slowly and smoothly to conform to data privacy and security standards. [9]

VI. CONCLUSION

This paper proposes a touch alone fingerprint biometric payment system, which provides a practical, secure, and convenient solution for futuristic digital payments. With the use of integrated fingerprint authentication and real-time banking infrastructure, the system completely removes the requirement for cash, cards, or smartphones and extends financial services to a much larger layer of the population. Widespread testing indicated excellent precision, rapid speed, and significant resistance to spoofing, thus establishing trustworthiness in real-world scenarios. The solution is based on modular system design, which means fingerprint scanner, POS terminal, and backend server be all independent units and can communicate with one another while ensuring they can handle their own transactions with no data encryption, storage of the actual fingerprint, and instead the template, which is safely secured. Despite some challenges such as fingerprint wear, reliance on network availability, and the necessity for strong data protection policies, the results show that payments based on biometrics can considerably improve transaction security and convenience [15] This work lays the groundwork for future optimizations, including AI-enhanced fingerprint quality assessment, multimodal biometrics, offline transactions, and expansion across commercial sectors. Refining biometric payment systems could soon make this technology a widely accepted and accessible method of digital payment.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] S. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed. Springer, 2009.

[3] UIDAI, “Aadhaar Enabled Payment System (AePS),” Unique Identification Authority of India. [Online]. Available: https://uidai.gov.in. [Accessed: 15-Nov-2025].

[4] Apple Inc., “About Apple Pay Security,” Apple Support. [Online]. Available: https://support.apple.com. [Accessed: 14-Nov-2025].

[5] Samsung Electronics, “Samsung Pay: Authentication and Security,” Samsung Official. [Online]. Available: https://www.samsung.com. [Accessed: 14-Nov-2025].

[6] R. Cappelli, M. Ferrara, and D. Maltoni, “Fingerprint verification competition,” IEEE Transactions on PAMI, vol. 31, no. 3, pp. 521–532, 2009.

[7] A. Ross, K. Nandakumar, and A. Jain, Introduction to Biometrics. Springer, 2013.

[8] P. Yoon and A. K. Jain, “Effects of fingerprint quality on matching performance,” Proc. IEEE ICPR, pp. 145–148, 2004.

[9] M. T. Arafin and D. M. Han, “Secure biometric payment systems: A review,” Journal of Information Security, vol. 11, no. 3, pp. 123–135, 2020.

[10] N. Ratha et al., “Enhancing security and privacy in biometrics,” IBM Systems Journal, vol. 40, no. 3, pp. 614–634, 2001.

[11] S. Kaur and R. K. Saini, “Design and evaluation of secure digital payment architectures,” International Journal of Computer Applications, vol. 178, no. 12, pp. 1–6, 2019.

[12] Z. Akhtar and A. K. Misra, “Spoof detection in fingerprint systems: A survey,” IEEE Access, vol. 5, pp. 22082–22099, 2017.

[13] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code, 2nd ed., Wiley, 1996.

[14] T. Schneider et al., “Real-time biometric authentication using Raspberry Pi,” Proc. IEEE ICCE, pp. 1–4, 2021.

[15] M. Ferrara and D. Maltoni, “Fingerprint liveness detection,” Handbook of Biometric Anti-Spoofing, Springer, pp. 23–46, 2019.

[16] Google Developers, “Secure HTTPS communication,” Google Web Docs. [Online]. Available: https://developers.google.com. [Accessed: 16-Nov-2025].

[17] Krishan. R. and Laxmi. V., (2016), “Algorithm for Optimized Load Balancing of WLAN,” International J. Computer Science and Information Security, 14(11), pp. 872-878. (ESCI WEB OF SCIENCE).

[18] PostgreSQL Global Development Group, “PostgreSQL Documentation,” PostgreSQL.org. [Online]. Available: https://www.postgresql.org/docs. [Accessed: 12-Nov-2025].

[19] Wikipedia, “Biometric Payment Systems,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Biometric_payment. [Accessed: 14-Nov-2025].

[20] Guru Kashi University, “GKU Journal of Multidisciplinary Research – Biometric Technology Papers,” GKUJMR Archive. [Online]. Available: https://gkujar.com (hypothetical for citation). [Accessed: 12-Nov-2025].

[21] Kumar, R. (2019). Machine learning: Concept, deep learning and applications. Wireless Communication and Mathematics, 49.