World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Biometric based payment system

Banumathi KL [1], Shreyas P [2,*], S Suhas [2], Vyshnavi HK [2] and Chitra A [2]

[1] *Assistant Professor, Department of Electronics and Communication Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India.*

[2] *Department of Electronics and Communication Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 1880–1892

Publication history: Received on 01 June 2024; revised on 15 July 2024; accepted on 18 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2120

Abstract

The increasing need for secure and convenient payment methods has fueled the exploration of biometric authentication systems. This paper presents a Biometric Based Payment System designed to streamline transactions while prioritizing security. The system employs a fingerprint sensor (R307) to ensure robust user identification, complemented by a 4x4 keypad for versatile input and an I2C OLED display for clear feedback. At its core, the system leverages an ESP32 microcontroller and robust SHA-256 encryption to protect sensitive information during storage and transmission. Transaction data resides in a centralized MySQL database on an Apache server, and users manage payment history through a web interface. The system emphasizes security and ease of use, with the potential for future exploration of multi-factor authentication, offline capabilities, and blockchain integration to further enhance its robustness

Keywords: Biometric payment system; Biometric authentication; Fingerprint sensor (R307); Security; SHA-256 encryption; MySQL database; HTTP protocol; ESP32; User interface; Web interface

1. Introduction

The current landscape of daily payments is dominated by cash and IC cards, each with its limitations. Cash transactions, while prevalent in offline scenarios, are cumbersome due to the need for change-giving. Similarly, IC cards, though offering convenience for everyday purchases, lack a robust authentication process.

Biometric payment emerges as a promising solution. Leveraging the unique biological characteristics of users for identification significantly enhances security in offline payments. Additionally, eliminating the need to carry cash or cards fosters greater convenience. Biometric payment effectively bridges the gap between security and ease of use.

The widespread adoption of biometric payment has yet to reach its full potential due to cost and technical hurdles. This paper addresses these challenges by proposing a low-cost embedded biometric payment system, making this secure and convenient payment method more accessible.

The Biometric Based Payment System, detailed in this paper, offers a secure and streamlined payment experience. It utilizes biometric authentication for user verification, employing a fingerprint sensor (like the R307) for user identification. Users interact with a versatile 4x4 matrix keypad for functionalities such as payment amount entry, account balance inquiries, and fund deposits. All actions are confirmed on a clear I2C OLED display, providing real-time visual feedback.

[*] Corresponding author: Shreyas P

The ESP32 microcontroller serves as the heart of the system. This powerful unit safeguards sensitive information through robust SHA-256 hashing for on-board data encryption. This encryption protects transaction details during transmission to a centralized MySQL database hosted on an Apache server. The system efficiently communicates between the ESP32 microcontroller and the server using the HTTP protocol. For user convenience, a dedicated web interface allows users to manage their payment history.

2. Literature Review

2.1. The Rise of Biometric Payment Systems

The growing demand for secure and convenient payment methods has fueled significant research and development in biometric payment systems. Traditional cash transactions, while prevalent for a long time, are hampered by the need for change giving, slowing down the payment process. IC cards, while offering a faster alternative, lack robust authentication mechanisms, leaving them vulnerable to fraud if lost or stolen. Biometric payment systems have emerged as a promising solution that addresses these limitations.

Biometric Technologies: Biometric authentication leverages unique biological characteristics, such as fingerprints, facial features, or iris patterns, for user identification. This significantly enhances security in offline payment scenarios compared to cash or IC cards, where the physical possession of the medium grants access. Research in this field has explored various biometric modalities, with fingerprint recognition being the most widely adopted due to its maturity, sensor affordability, and user acceptance [1]. Advancements in facial recognition and iris scanning technologies, however, are continuously improving their accuracy and reducing costs, potentially paving the way for wider adoption in the future [2, 3].

Recent Advancements and Market Exploration: Research efforts are not only focused on improving the accuracy of biometric recognition technologies but also on reducing sensor costs to make biometric payment systems more accessible. A growing number of companies recognize the potential of biometrics in the payment landscape. For instance, retail giants like Walmart have begun piloting fingerprint payment systems in their stores [4]. However, widespread adoption of this technology has yet to materialize, likely due to a combination of cost considerations and technical hurdles that need to be addressed.

2.2. Challenges in Biometric Payments

Despite the promising advancements in biometrics, several challenges hinder the widespread adoption of biometric payment systems:

Cost: High-quality biometric sensors can be expensive, particularly for emerging technologies like iris scanners. This cost can be a significant barrier for businesses considering implementing biometric payment solutions, as it directly impacts the overall system cost [5]. Research into cost-effective sensor development and alternative materials is crucial to making biometric payments more accessible.

Security Concerns: While biometric authentication offers a strong layer of security compared to traditional methods, it's not without vulnerabilities. Spoofing attacks, where unauthorized individuals attempt to bypass the system using replicas of fingerprints or other biometric data, are a potential concern. However, ongoing research in liveness detection techniques and secure key management protocols is continuously improving the robustness of biometric authentication systems [6, 7].

Technical Complexity: Developing reliable embedded platforms for biometric payment systems requires expertise in hardware design, secure system programming, and robust communication protocols. Additionally, secure data storage and transmission of biometric information are crucial aspects that need careful consideration [8].

Privacy Considerations: The collection and storage of biometric data raise public concerns about privacy and potential misuse. Regulatory frameworks, such as the General Data Protection Regulation (GDPR) in Europe, establish guidelines for data protection and user consent. Biometric payment system developers must ensure compliance with relevant regulations and implement transparent data security practices to gain user trust [9].

2.3. The Need for Low-Cost Embedded Solutions

The key to wider adoption of biometric payment systems lies in developing cost-effective solutions that address the challenges mentioned above. While high-end biometric systems exist, their high cost limits their scalability and accessibility for everyday transactions. There is a clear research gap in developing low-cost embedded platforms that integrate secure biometric authentication with efficient payment processing capabilities.

2.4. Transition to Work

The Biometric Based Payment System proposed in this paper aims to bridge this gap by offering a secure and convenient payment solution at a significantly lower cost compared to traditional biometric systems. By leveraging a combination of readily available hardware components and efficient software design, our system achieves robust user authentication using fingerprint recognition while maintaining affordability.

2.5. Comparison

Comparison with Traditional Payment Methods

Table 1 Comparison with Traditional Payment Methods

Feature	**Cash**	**IC Card**	**Biometric Based Payment System**
Security	Low	Medium (requires PIN, but vulnerable to lost/stolen cards)	High (fingerprint authentication eliminates the risk of unauthorized card use and PIN cracking)
Convenience	Cumbersome (change giving slows down transactions)	Faster for small transactions; requires carrying the card	Most convenient; eliminates the need to carry cash or cards and simplifies transactions
Fraud Potential	Moderate (lost or stolen cash can be difficult to recover)	Moderate (lost or stolen cards can be used fraudulently if PIN is compromised)	Reduced (fingerprint verification ensures only the authorized user can make transactions)
Offline Capability	Yes	Limited (may require online verification for certain transactions)	Yes (transactions can be processed and stored locally, with later synchronization to the central database)

Objectives

- Integrate and evaluate sensor modules for fingerprint capture, ensuring compatibility with the ESP32 environment.
- Develop a secure system for users to link their fingerprint data with their payment information.
- Enable secure and fast transactions using fingerprint authentication for payment processing

2.6. System Overview

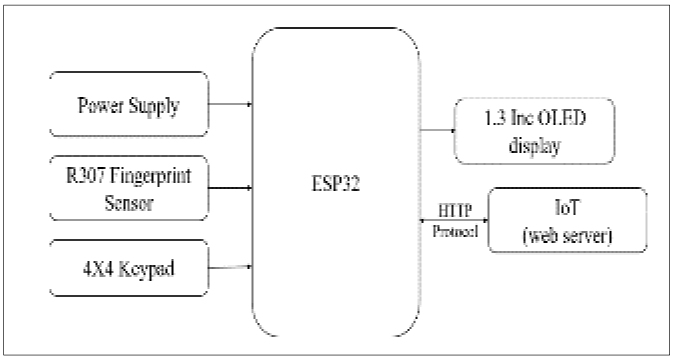

Figure 1 Block diagram of Biometric Based Payment System

At the heart of the system lies the ESP32 microcontroller, a powerful and versatile choice offering processing muscle, communication capabilities, and robust security features. Its dual-core processor efficiently handles fingerprint image processing and secure communication. Built-in Wi-Fi facilitates seamless data transmission to a central server, while

Bluetooth Low Energy (BLE) provides a power-saving alternative for suitable scenarios. The ESP32 boasts ample memory to accommodate program storage, data manipulation, and fingerprint template storage.

The system utilizes a readily available and cost-effective R307 fingerprint sensor for fingerprint image capture during both enrollment and verification. This sensor offers a favorable balance between affordability and image quality, guaranteeing reliable fingerprint acquisition. The R307 fingerprint sensor's integrated DSP (Digital Signal Processor) performs image cleanup (noise reduction), normalization (for consistency), and extraction of key details (minutiae) essential for matching.

I2C OLED display provides a user-friendly interface for visual feedback. I2C stands for Inter-Integrated Circuit, which is a communication protocol used to connect the display to the main controller. OLED stands for Organic Light-Emitting Diode, a type of display technology known for its thin profile and high contrast.

A 4x4 matrix keypad is a grid of buttons arranged in four rows and four columns. It is used to take user input by scanning the button presses. This scanning method determines which button is being pressed.

Security is paramount in our design. The ESP32's hardware-based encryption capabilities are harnessed to encrypt sensitive data, such as fingerprint templates, before transmission. This on-board encryption adds a crucial layer of protection for user information. The system leverages the efficient HTTP protocol for communication with a central server hosted on an Apache web server. This server manages a MySQL database that stores user account information, transaction history, and other relevant data. To ensure secure communication, robust authentication and authorization mechanisms are implemented on the server side. Additionally, the system integrates with a web application, providing users with a convenient platform to track their transaction history and manage their accounts.

3. Methodology

The biometric payment system uses fingerprint identification to allow users to make secure and convenient payment transactions.

It operates in two primary modes:

- Enrollment Mode.
- Payee Mode.

3.1. Enrollment Mode

- The system guides the user to begin the enrollment process (by displaying on OLED).
- The fingerprint sensor captures two images of the same finger.
- The images are processed to create a unique and reliable fingerprint template.
- The generated template is transmitted over a secure network connection to a central server or securely stored in the device's memory (non-volatile, such as EEPROM or Flash) in case of no network and associated with a unique ID.
- The system indicates the success or failure of the enrollment (by displaying it on OLED).

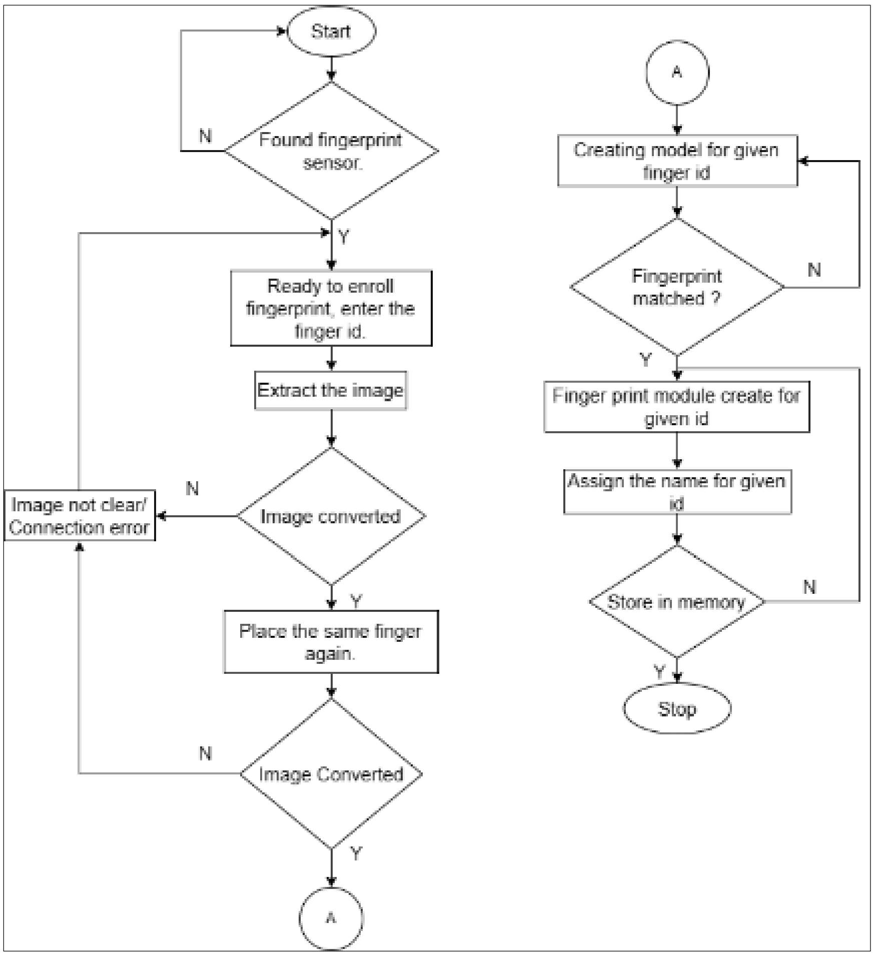
Start
Found fingerprint sensor.
N
Y
Ready to enroll fingerprint, enter the finger id.
Extract the image
Image converted
N
Image not clear/ Connection error
Y
Place the same finger again.
Image Converted
N
Y
A
A
Creating model for given finger id
Fingerprint matched ?
N
Y
Finger print module create for given id
Assign the name for given id
Store in memory
N
Y
Stop

Figure 2 Flowchart of Enrolment Mode

3.2. Payee Mode (Authentication)

- The system requests the user to place their finger on the sensor for authentication.
- The sensor obtains a new fingerprint image.
- The captured image is compared against stored fingerprint templates.
- If a match is found, the system presents the user with choices (Balance, Add Money, Pay) on the OLED display.

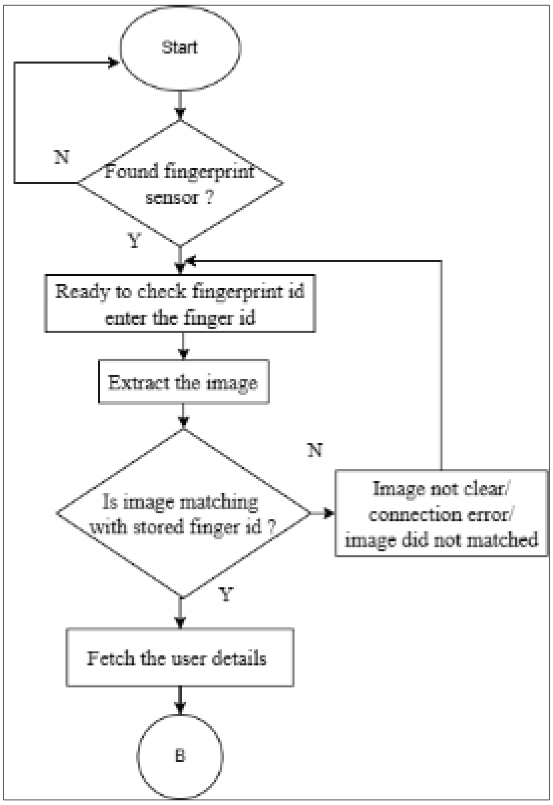
Start
N
Found fingerprint sensor ?
Y
Ready to check fingerprint id enter the finger id
Extract the image
N
Is image matching with stored finger id ?
Image not clear/ connection error/ image did not matched
Y
Fetch the user details
B

Figure 3 Flowchart of Payee Mode Authentication

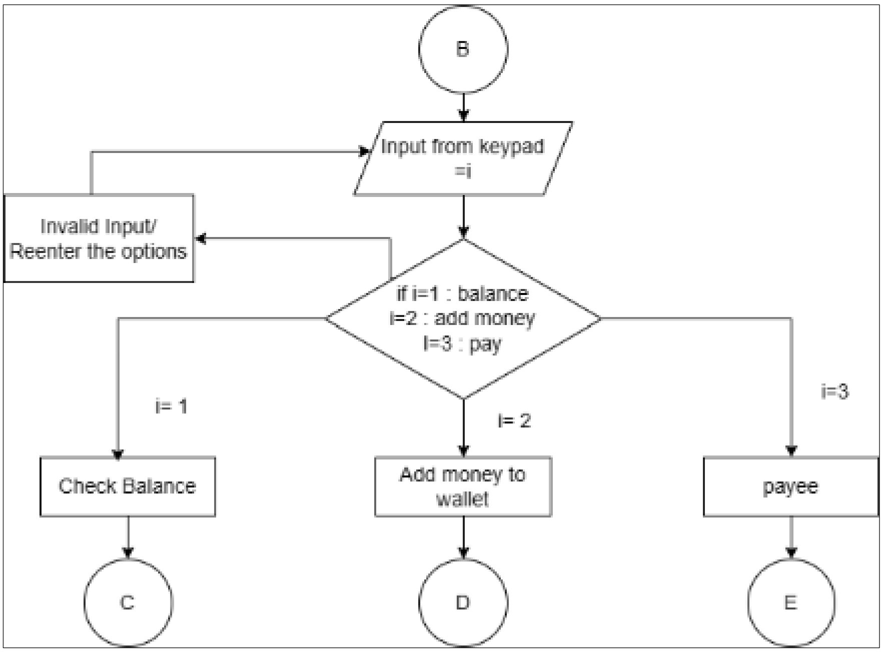

Figure 4 Flowchart of Menu

- The keypad is used to collect the user's selection.
- The system executes the chosen action:
- Balance: Retrieves and displays the current wallet balance.

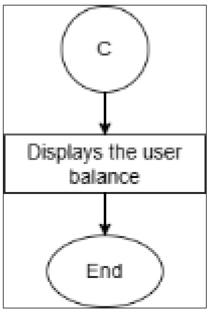

Figure 5 Flowchart of Check balance

- Add Money: Provides an interface to add funds to the wallet.

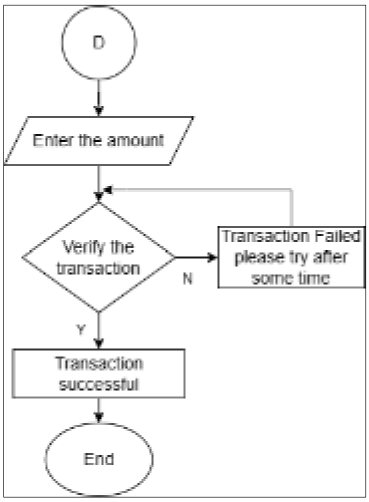

Figure 6 Flowchart of Add money

- Pay: Initiates a secure payment process, contingent on sufficient balance.

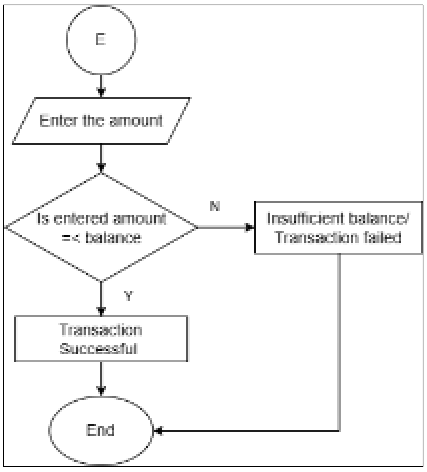
E
Enter the amount
Is entered amount =< balance
N
Insufficient balance/ Transaction failed
Y
Transaction Successful
End

Figure 7 Flowchart of Payment

- The system communicates the payment status to the user (success/failure).
- Transaction data is either transmitted over a secure network connection to a central server or stored locally (e.g., SD card) with appropriate safeguards for enhanced record-keeping and traceability.
- For each completed transaction, essential details are captured, which the user can later access.

3.3. Image Capture

To ensure high-quality fingerprint image capture, the system prompts the user to place their finger on the sensor in a specific orientation. The sensor captures multiple (typically two or three) fingerprint images during enrollment. Image quality is crucial for accurate fingerprint recognition, and the system employs image pre-processing techniques to enhance the captured fingerprint data. These pre-processing steps may involve noise reduction to remove artifacts from the sensor, segmentation to isolate the fingerprint region of interest, and thinning to normalize the thickness of fingerprint ridges.

3.4. Template Generation

Algorithm: The system utilizes a well-established fingerprint minutiae extraction algorithm to create a unique feature representation (template) from the captured fingerprint images. This algorithm identifies distinctive characteristics within the fingerprint, such as minutiae points (ridge endings and bifurcations). The minutiae points are extracted along with their associated features (e.g., type of ending, direction) and their relative locations within the fingerprint image. These features are then mathematically encoded and stored as a compact fingerprint template.

3.5. Template Format

Fingerprint templates within the system are represented using a data structure that efficiently captures the minutiae details extracted from the fingerprint images.

This data structure typically includes:

- Minutiae Type: This field specifies the type of minutiae point (e.g., bifurcation, ending).
- X-Coordinate: This value indicates the horizontal position of the minutiae point within the fingerprint image.
- Y-Coordinate: This value indicates the vertical position of the minutiae point within the fingerprint image.
- Minutiae Angle: This field stores the orientation of the minutiae point, which can be helpful for matching purposes.

3.6. Template Storage

The decision to store the fingerprint template locally on the device or transmit it to a central server depends on factors such as available storage space on the device, system security considerations, and network availability. If the device has sufficient non-volatile memory (e.g., flash memory) and reliable network connectivity is available, the template may be securely stored locally on the device using SHA-256 encryption and secure key management practices. SHA-256 is a robust cryptographic hash function that transforms the fingerprint template into a fixed-size bit string. This hash serves as a unique identifier for the fingerprint, but it does not contain the actual fingerprint data itself. Secure key management ensures that only authorized entities have access to the decryption key needed to reverse the hashing process and potentially recreate the original fingerprint template.

Alternatively, for scenarios where local storage is limited or network connectivity is intermittent, the template can be encrypted using the ESP32's hardware encryption engine and transmitted over a secure channel to the central server for storage within the MySQL database. Additionally, the system can be designed to support optional local storage of the encrypted fingerprint template on an SD card. This approach offers a balance between security and redundancy. The SD card should be formatted with a file system that supports secure erase functionalities to prevent potential data recovery in case of physical theft. Encryption of the template at rest on the SD card using the same SHA-256 approach further enhances security.

3.7. Fingerprint Matching Algorithms

Fingerprint matching algorithms are the heart of fingerprint recognition systems, responsible for accurately comparing a captured fingerprint image with a stored template to verify a user's identity. Several approaches exist, each with its advantages and considerations:

Minutiae-Based Matching: This is the dominant technique in fingerprint recognition. It extracts distinctive features called minutiae points (ridge endings and bifurcations) from both the captured fingerprint image and the stored template. The algorithm then compares the corresponding minutiae points, focusing on their relative positions and orientations. This approach offers a high degree of accuracy and is robust to minor variations in fingerprint placement during capture. Many well-established minutiae-based matching algorithms are available, some even included in open-source libraries, making them a cost-effective choice for embedded systems.

Correlation-Based Matching: These algorithms compare the overall grayscale intensity patterns of fingerprint images. They treat the fingerprint image as a whole and calculate a similarity score between the captured image and the stored template. This method can be less sensitive to minor fingerprint distortions caused by rotation or pressure variations during sensor contact. However, correlation-based algorithms can be computationally expensive, potentially impacting real-time performance, and may be susceptible to noise or artifacts in the fingerprint image.

Hybrid Approaches: The strengths of both minutiae-based and correlation-based techniques. They may extract minutiae points but also incorporate image features or textural analysis to enhance matching accuracy and robustness. This approach can be particularly beneficial in scenarios where fingerprint quality might be less than ideal due to factors like dry or scarred skin.

3.8. UI Interactions

Menu Presentation and Navigation

- Simplicity: Design a simple hierarchical menu system that's intuitive to navigate. Limit the number of options at each level.
- OLED Display Utilization: Use the OLED display to present menu titles (e.g., "Main Menu," "Payment"), individual options (e.g., "1. Balance," "2. Pay"), and prompts (e.g., "Enter Amount").
- Keypad Navigation: Assign keys on the 4x4 keypad to navigate the menu. For example:
  - '1', '2', '3' for option selection
  - '*' for "Back" or moving up a menu level
  - '#' for "Confirm" or entering a submenu

Amount Entry

- Keypad Utilization: Use the number keys to enter the transaction amount.
- Display Feedback: Display the entered digits on the OLED as the user types them in.
- Decimal Support: Incorporate a designated key (e.g., '0') for entering a decimal point.
- Input Validation: Implement simple checks to prevent unrealistic amounts (e.g., limit the number of digits, and reject leading zeroes).

Status Display

- Clear Messages: Use the OLED to display concise payment status messages:
  - "Payment Successful"
  - "Payment Failed"
  - "Insufficient Balance"
- Visual Cues (optional): Consider using symbols or even a small LED for quick visual confirmation of success or failure.

3.9. Secure Payment Handling

Encryption

- SHA-256: SHA-256 hashing for securing sensitive payment data (e.g., account numbers, transaction amounts). Explain where the hashing takes place (on the ESP32 before transmission).
- Hashing vs. Encryption: Clarify that SHA-256 is a one-way cryptographic hash function, not reversible encryption. It allows authentication of data integrity without storing information in a decryptable form.

Communication Protocol

- HTTP: HTTP protocol for ESP32-server communication.
- Authentication: Describe the authentication mechanisms used to ensure that only authorized devices and users can interact with the server.
- Device Authentication: Consider device-specific certificates or pre-shared keys.
- User Authentication: This could involve transmitting the fingerprint template hash along with a user ID, or a separate login system using the keypad.

3.10. Software Flow

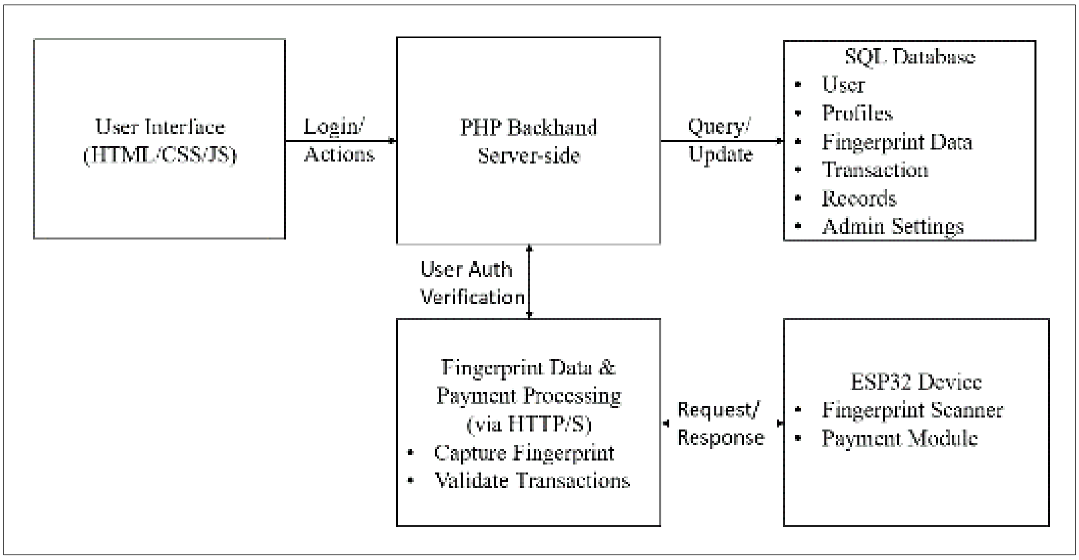

Figure 8 Software Flow

3.11. Data Management

Database Interaction

Database Schema

- Table: Users
- user_id (INT, Primary Key, Auto Increment)
- username (VARCHAR, Unique)
- fingerprint_hash (VARCHAR)
- account_balance (DECIMAL)
- Table: Transactions
- transaction_id (INT, Primary Key, Auto Increment)
- transaction_timestamp (DATETIME)

Explanation

- The 'Users' table stores core user information and a hash of the fingerprint template (using SHA-256).
- Transactions are recorded in the 'Transactions' table, linked to a user via the 'user_id' foreign key.
- Consider adding additional fields as needed (e.g., location, store ID) if the system captures such data.

Data Integrity

Local Transaction Logging

- Implement a local transaction queue on the device (potentially on an SD card for increased capacity).
- Each transaction is logged with relevant data (user, amount, type) and a timestamp when initiated.
- A background process on the ESP32 periodically attempts to synchronize the local queue with the central database.
- Successful transactions are removed from the local queue; failed transactions are kept for re-attempts.

Synchronization Process

- The process uses HTTP requests to transmit local transaction data to the server.
- Server-side scripts update the MySQL database and return success/failure responses.
- Device logic handles clearing the local queue upon success or scheduling retries upon failure.

Offline Payment Handling

- During network outages, the system can temporarily allow payment transactions.
- Validate transactions against the last known account balance (potentially stored locally in secure device memory).
- Log all offline transactions in the local queue with a special "offline" flag.
- Upon network restoration, synchronize offline transactions with the priority to prevent overspending.

Local Storage

- Choose SD card storage for its larger capacity and ease of data recoverability in case of device failure
- Implement file system-level encryption and secure erase features on the SD card.
- Optionally, maintain a limited-size offline transaction log in secure device memory to provide partial functionality during short outages.

4. System Test

A prototype was developed using an ESP32 Dev Kit V1 and an R307 fingerprint sensor for cost-effectiveness and real-world applicability. The system was tested for enrollment, recharge, payment, and user interface functionality, ensuring secure fingerprint storage (SHA-256) and data integrity (HTTPS communication with a central MySQL database).

5. Application

- Point-of-Sale (POS) Terminals: Integrate the system into retail stores, restaurants, or service counters as an alternative to traditional card terminals or cash-based transactions.
- Vending Machines: Retrofit existing vending machines to accept secure, cashless biometric payments, enhancing convenience for customers.
- Public Transportation: Enable biometric-based fare payment systems on buses, trains, or subways, streamlining boarding and reducing the need for physical tickets or passes.
- School & Corporate Cafeterias: Implement the system in school or workplace cafeterias, allowing students or employees to pay seamlessly without the need for cash or ID cards.
- Access Control Systems: Integrate biometric authentication with physical access control mechanisms (doors, gates) as an added layer of security in sensitive areas of buildings.
- Event Ticketing: Deploy the system at concerts, sporting events, or festivals to expedite entry and minimize the risk of fraudulent tickets.
- Micropayment Scenarios: Design a modified version for low-value transactions, such as in-app purchases, public internet kiosks, or street vendor payments.
- Remote or Rural Areas: Leverage the system's potential for offline functionality to provide accessible payment solutions in areas with limited connectivity or banking infrastructure.
- Government Subsidy Programs: Integrate the system with government-run welfare or subsidy distribution systems to ensure secure and efficient transfer of funds to beneficiaries.

The prototype of the Biometric Based Payment System, developed using an ESP32 Dev Kit V1 and an R307 fingerprint sensor, was successfully implemented and tested. The system securely enrolled users' fingerprints with SHA-256 encryption, ensuring data integrity. It also enabled seamless account recharging, demonstrating its capability to handle real-time financial transactions effectively. Users could make payments using their enrolled fingerprints, with each transaction securely processed through HTTPS communication with a central MySQL database.

The user interface, featuring an I2C OLED display and a 4x4 matrix keypad, provided clear feedback and was intuitive to navigate, ensuring a smooth user experience. Overall, the results indicate that the Biometric Based Payment System is a viable and cost-effective solution for secure and efficient transactions. Its successful testing across various functionalities highlights its potential for widespread application in diverse payment scenarios.

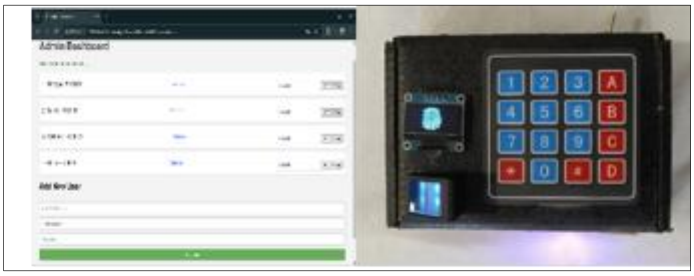

Figure 9 Admin Dashboard and Final set up of the project

6. Conclusion

This paper has presented a Biometric Based Payment System designed to strike a balance between security, convenience, and affordability. The system leverages fingerprint authentication, a well-established and reliable biometric modality, for robust user verification. A user-friendly interface, featuring a keypad and an OLED display, ensures intuitive interaction during the enrollment and payment processes. To safeguard sensitive user information, the system employs SHA-256 encryption throughout. This encryption protects fingerprint templates in storage and ensures data integrity during transmission to a centralized MySQL database. The system communicates efficiently with the central server using the HTTP protocol, enabling features like transaction history management through a web interface. Finally, the implementation prioritizes affordability by carefully selecting readily available components such as the ESP32 microcontroller and the R307 fingerprint sensor, making this solution accessible for wider adoption.

Future Work

- Enhanced Security

Integration of additional biometric modalities (e.g., iris scan, facial recognition) can create a multi-factor authentication system, potentially offering even stronger security safeguards.

- Improved Offline Functionality

Expanding offline capabilities would broaden the system's applicability to scenarios with intermittent network connectivity. This could involve secure local storage of encrypted transaction data and robust synchronization mechanisms.

- Decentralized Security with Blockchain

Utilizing blockchain technology could introduce a decentralized approach to user identity and transaction management, potentially enhancing security and transparency.

- Advanced User Convenience Features

The system's functionality could be extended to incorporate features such as balance top-up functionalities, loyalty program integration, or integration with existing mobile payment ecosystems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Series Fingerprint Identification Module Manual. https://www.adafruit.com/datasheets/ZFM%20user%20manualV15.pd

[2] A. Vinay, A. S. Cholin, A. D. Bhat, K. N. B. Murthy, and S. Natarajan, 'An efficient ORB based face recognition framework for human-robot interaction,'' Procedia Compute. Sci., vol. 133, pp. 913–923, Jan. 2018.

[3] A. Tlili, F. Essalmi, M. Jemni, Kinshuk, and N.-S. Chen, ''Role of personality in computer-based learning,'' Compute. Hum. Behave., vol. 64, pp. 805–813, Nov. 2016.

[4] B. Suh and I. Han, ''The impact of customer trust and perception of security control on the acceptance of electronic commerce,'' Int. J. Electron. Commerce, vol. 7, no. 3, pp. 135–161, 2003.

[5] L. Y. Leong, K. B. Ooi, A. Y. L. Chong, and B. Lin, ''Modeling the stimulators of the behavioral intention to use mobile entertainment: Does gender really matter?'' Compute. Hum. Behave., vol. 29, no. 5, pp. 2109–2121, 2013.

[6] C. Carlsson, P. Walden, and H. Bouwman, ''Adoption of 3G+ services in Finland,'' Int. J. Mobile Common., vol. 4, no. 4, pp. 369–385, 2006.

[7] C. J. Boyce and A. M. Wood, ''Personality and the marginal utility of income: Personality interacts with increases in household income to determine life satisfaction,'' J. Econ. Behave. Org., vol. 78, nos. 1–2, pp. 183–191, 2011. VOLUME 7, 2019 154371 W. K. Zhang, M. J. Kang: Factors Affecting the Use of Facial-Recognition Payment: Example of Chinese Consumers

[8] C. L. Miltgen, A. Popovič, and T. Oliveira, ''Determinants of end-user acceptance of biometrics: Integrating the 'big 3' of technology acceptance with privacy context,'' Deci's. Support Syst., vol. 56, pp. 103–114, Dec. 2013.

[9] C. Liao, J. L. Chen, and D. C. Yen, ''Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model,'' Compute. Hum. Behave., vol. 23, no. 6, pp. 2804–2822, 2007.

[10] C. M. Ringle, S. Wende, and A. Will, Smart PLS Computer Software. Accessed: Apr. 10, 2015. [Online]. Available: https://www.smartpls.de

[11] C. Ranganathan and S. Ganapathy, ''Key dimensions of business-toconsumer Web sites,'' Inf. Manage., vol. 39, no. 6, pp. 457–465, 2002.

[12] C. López-Nicolás, F. J. Molina-Castillo, and H. Bouwman, ''An assessment of advanced mobile services acceptance: Contributions from TAM and diffusion theory models,'' Inf. Manage., vol. 45, no. 6, pp. 359–364, 2008.

[13] F. D. Davis, ''Perceived usefulness, perceived ease of use, and user acceptance of information technology,'' MIS Quart., vol. 13, no. 3, pp. 319–340, 1989.

[14] D. Dmytro and F. M. Sukno, ''Automatic local shape spectrum analysis for 3D facial expression recognition,'' Image Vis. Compute., vol. 79, pp. 86–98, Nov. 2018.

[15] D. N. Parmar and B. B. Mehta, ''Face recognition methods & applications,'' Int. J. Compute. Technol. Appl., vol. 4, no. 1, pp. 84–86, 2013.

[16] D. Turan, ''On recognition of gestures arIsing in flight deck officer (FDO) training,'' Cranfield Univ., Cranfield, U.K., Tech. Rep., 2011.

[17] E. L. Slade, M. D. Williams, and Y. Dwivedi, ''Extending UTAUT2 to explore consumer adoption of mobile payments,'' in Proc. U.K., Acad. Inf. Syst. Conf., Oxford, U.K., 2013, pp. 1–23.

[18] E. M. Rogers, Diffusion of Innovations, 4th ed. New York, NY, USA: Free Press, 1995.

[19] E. Vazquez-Fernandez and D. Gonzalez-Jimenez, ''Face recognition for authentication on mobile devices,'' Image Vis. Compute., vol. 55, pp. 31–33, Nov. 2016.

[20] E. Wright, ''The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector,'' Media Entertainment Law J., vol. 29, p. 611, 2019.

[21] F. Becerra-Riera, A. Morales-González, and H. Méndez-Vázquez, ''Facial marks for improving face recognition,'' Pattern Recognit. Lett., vol. 113, pp. 3–9, Oct. 2018.

[22] G. B. Svendsen, J.-A. K. Johnsen, L. Almås-Sørensen, and J. Vittersø, ''Personality and technology acceptance: The influence of personality factors on the core constructs of the technology acceptance model,''Behav. Inf. Technol., vol. 32, no. 4, pp. 323–334, 2013.

[23] G. Heineck and S. Anger, ''The returns to cognitive abilities and personality traits in Germany,'' Labour Econ., vol. 17, no. 3, pp. 535–546, 2010