IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Biometric Payment System Using Fingerprint Authentication And Esp32

Sahana S Shegunasi[1], Savitri S Halakarni[2], Shivanand Bendigeri[3], Vadiraj A Inamdar[4], Ashwini Garaddi[5]

1,2,3,4 Students of Dept of ECE, KLS VDIT, Haliyal

5, Assistant Professor of Dept of ECE, KLS VDIT, Haliyal

Abstract: The rapid shift to digital and cashless transactions has led to a greater need for secure and reliable authentication methods. Traditional payment systems often depend on cards, PINs, or passwords, which are at risk of theft and unauthorized access. This research presents a Biometric Payment System that uses Fingerprint Authentication with the ESP32 microcontroller to improve security and user convenience. The system uses a fingerprint sensor to confirm the identity of a registered user before allowing payment. The ESP32 provides wireless connectivity for real-time data transfer. This model offers an efficient, low-cost, and scalable solution for retail environments, educational institutions, and smart canteens. Experimental results show that biometric authentication greatly improves security while allowing for quick transaction processing.

Keywords: Biometric authentication, fingerprint recognition, ESP32 microcontroller, secure payment system, IoT-based payment, digital transactions, wireless communication, embedded systems, identity verification, real time processing.

I. INTRODUCTION

Biometric authentication has become popular as a good alternative to older methods. Passwords PIN codes and even RFID tags are now being outdone. It provides improved reliability and increased security. Fingerprint verification is a leading option among biometric choices. It is uniquely personal easy to obtain, and known for its high accuracy.

Digital payments are surging across the planet, and so strong identity verification becomes essential in order to stop fraud, and unauthorized access. This work shows a fingerprint-based payment system using the ESP32 microcontroller and is relatively important to me believe. Can it provide affordable security, with simpler transactions perhaps? The ESP32 which includes Wi-Fi and Bluetooth offers real-time connections, to cloud services or payment gateways. These connections authorize us and give a detailed log of every activity, which protects us from fraud guys, isn't that so? Nice. When the reader is connected, it can perform the reading of fingerprints and match them against a database .Hence, only authorized people can make such payments for transactions or services. Coupling the biometric authentication with internet-connected gadgets secures the payment systems. Plastic cards may soon be a thing of the past. It is working fine in every environment, whether it is a store, school, or restaurant. It has applications to cashless scenarios, where secure payments are really critical, you see. The idea serves as a practical solution in order to enhance electronic banking safety.

II. LITERATURE SURVEY

2.1 “Biometric Payment Systems” by R. Sharma, P. Verma, S. Gupta(International Journal of Emerging Technology and Advanced Engineering (IJETAE) -2024)

This paper presents the design and implementation of a secure biometric payment system using an ESP32 microcontroller. The methodology involves fingerprint enrolment and verification for user authentication.

Secure transactions are ensured through SHA-256 encryption, which strengthens data protection during communication.

2.2 "Secure Transactions with Biometric Fingerprint Authentication" by K. Patel, A. Rao, M. Singh (International Journal of Computer Applications (IJCA)-2023)

This research focuses on developing a transaction system that utilizes fingerprint matching combined with server-side validation. The methodology includes HTTP-based communication where the fingerprint data is cross-verified with records stored in a MySQL database.

2.3 "ESP32-Based Biometric Payment Platform with Cloud Integration" by D. Mehta, L. Das, R. Nair (International Journal of Advanced Research in Electronics and Communication Engineering -2022)

This paper introduces a cloud-enabled biometric payment system built using an ESP32 controller. The methodology includes real-time fingerprint verification supported by AES-128 encryption to ensure secure data exchange. The system incorporates cloud storage for transaction monitoring, enabling remote access and improved scalability.

III. RESEARCH METHODOLOGY

The biometric payment system proposed in this study is created by combining hardware, software, and secure communication protocols. The hardware setup includes an ESP32 microcontroller, which connects to a fingerprint sensor and is powered by a stable supply. For user interaction, a display unit or mobile interface can provide real-time feedback. The programming uses Arduino IDE or ESP-IDF, incorporating libraries for fingerprint enrolment, identification, and Wi-Fi connectivity. User credentials and transaction records, are kept safe in a backend service. These services include, things like Firebase or even MySQL. Fingerprint enrolment starts the process. The captured print is turned into a digital template, that's then stored. This is done securely of course. Later, when you try to make a payment, the ESP32 scans your fingerprint. It verifies it, against those stored templates. Verification happens, and the ESP32 sends a payment authorization request. It communicates with the server. This communication utilizes an encrypted wireless connection; it's all rather technical. The server checks your account, and your current account status. Then the transaction, is processed swiftly. The database gets an update and it returns the result quickly enough. The database guys make sure it runs efficiently. All communications between the microcontroller and server, must be encrypted to enhance security. Also each fingerprint template, is stored in a very unique way. That way we prevent duplication or outright forgery, of your delicate templates. This entire setup makes for reliable biometric authentication. Plus it's efficient for data exchange and ensures the integrity of your financial transactions you see.

IV. Block Diagram

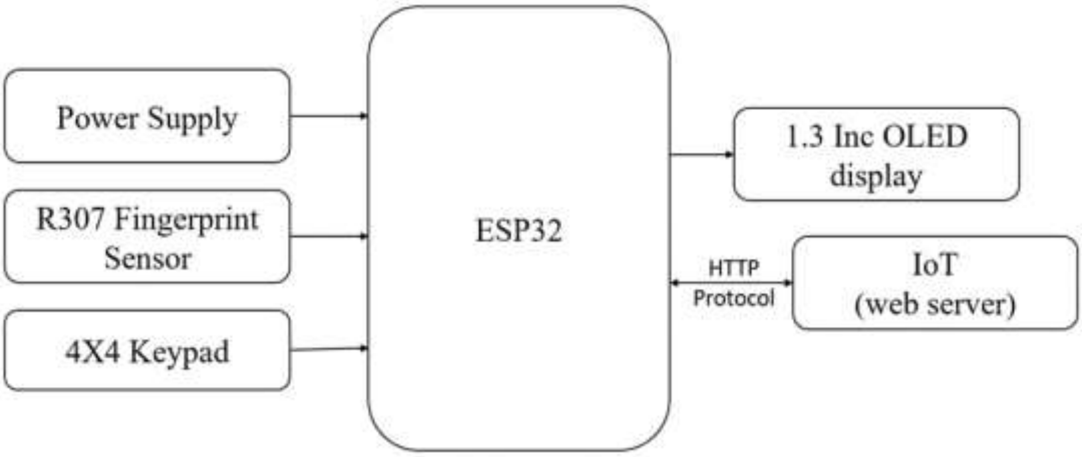
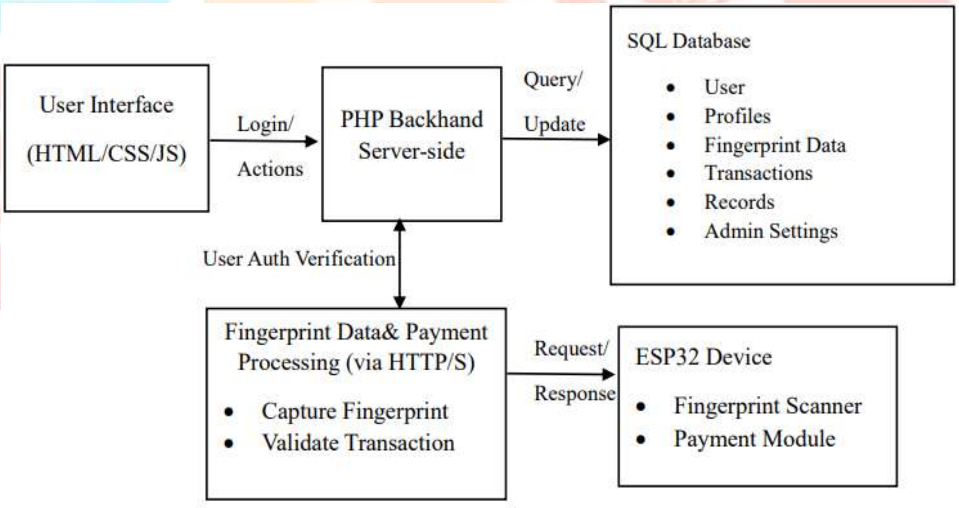


Fig.1 Block diagram of Biometric Payment System Using Fingerprint And ESP32

The block diagram shows how different components work together to ensure a secure payment process. The fingerprint sensor collects biometric data first, you see; then, it extracts essential key features, obviously. This info is sent to the ESP32 microcontroller and that does its work. The ESP32 operates as the main central unit of the system and it seems efficient. It handles user authentication processes as it starts the request for payment. And it is responsible for ensuring overall Wi-Fi connectivity with the backend server system. Information regarding payment is transmitted to the database server once authorization of authentication has been approved. The server verifies credentials that you know .It verifies the account balance is adequate, and then, the entire transaction is recorded. Finally, the server, "Gives you the ultimate status, so you know what's up.". User interfaces; perhaps like LCD displays; or mobile applications are a tool of some use, offering feedback very fast, but maybe there's some other possibilities? They keep users completely updated in a timely manner as things are going on. The configuration is to make sure that there is coordination of components; and that the information goes safely throughout the system as expected.

V .Software flow

The biometric payment system's software flow combines secure user authentication with smooth transaction handling. It starts with an interface design developed using HTML, CSS, and JavaScript. This configuration enables users to login, subscribe, and begin payment. All these actions are processed by a PHP backend, which acts as a main controller .It is responsible for handling input validations, processing requests, and handling communications between hardware and the database. The backend is linked to an SQL database that holds information about the users, fingerprints, transactions, and admin information .Upon making a payment request, an authentication command is sent by the backend to the ESP32 module. Such a device, which features fingerprint scanning technology, acquires the fingerprint information of the users and matches the data with the already fingerprint templates. After the verification is completed successfully, the result is sent back to the server. Then the backend verifies the transaction, modifies the related database records accordingly, and returns a response to the user interface. This ensures proper biometric authentication, with secure data transfer as well as payment execution throughout the system.



VI. System Test

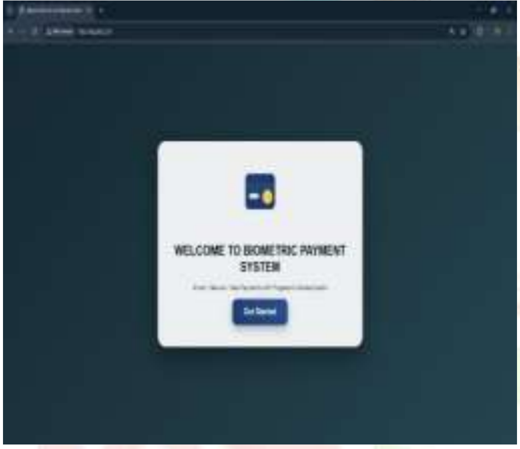
A functional prototype was created. The project used an ESP32 Dev Kit V1 together with an R307 fingerprint sensor. This makes for a cost-effective solution, which can be used in real-life scenarios, and it's very effective .We tested the system. The tests covered fingerprint registration. They also included user account recharging. Furthermore, we tested payment processing, alongside management of the user interface. The project places considerable emphasis on biometric data protection. We are focused on safeguarding it properly; it's key ESP32 Device to protecting everyone. Data integrity, is also vital. We used SHA-256 hashing to achieve some measure of safety. Additionally, HTTPS communication, assures good connections; safety, we feel, should be key. A centralized MySQL database manages the system's backend operations or database. This plan effectively backed practical deployment. And, additionally it promoted stronger safety regarding biometric information that's quite sensitive

VII. Application

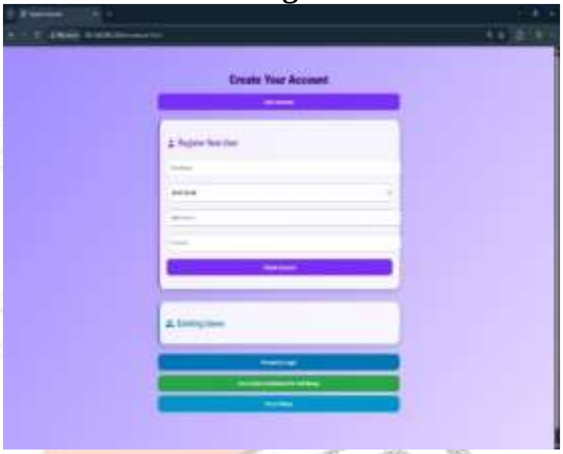
- It can be used in schools and colleges for a variety of functions. This includes fee payments library transactions and canteen billing. You do not need cash, or even your ID cards.
- It is quite useful in retail shops. It's useful for and supermarkets too; This usage enables fast checkout for customers and it is also contactless. This is a better safer method of payments.
- Workplaces will find it helpful. One can use it to manage cafeteria billing or employee service payments. The system allows access controlled purchases that are simple, and secure too.
- This is applicable in hospitals. Clinics will benefit from it and it is appropriate too. Use it for secure patient billing as it is faster and secure. Consider medication dispensing which allows quick verification of services medical too.
- Can be implemented in transportation systems for ticketing, fare collection, and access to restricted areas.
- Ideal for community centers, government service counters, and local kiosks that require verified microtransactions. Beneficial for rural service points and small businesses needing a low-cost, reliable, and secure payment method.

VIII. Result

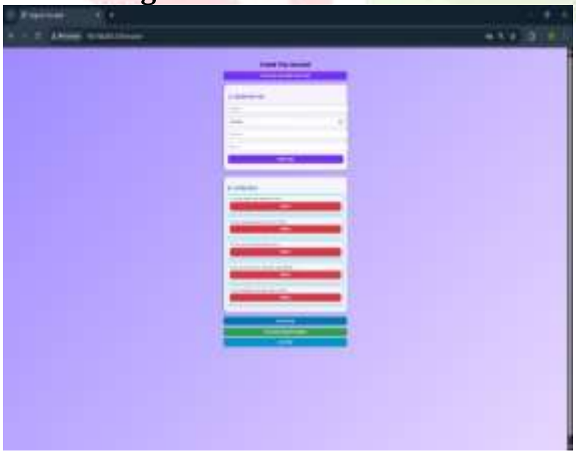
1.Welcome Page



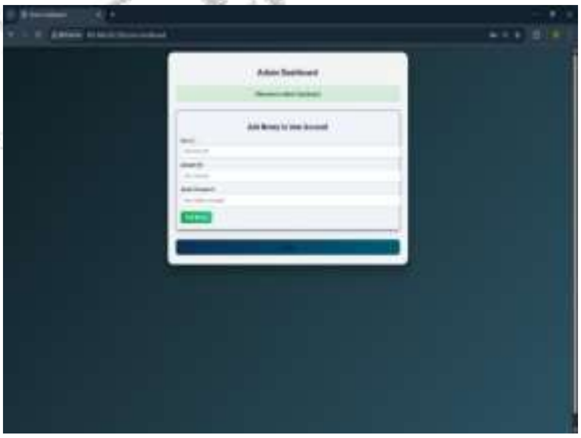
2.Before Registration



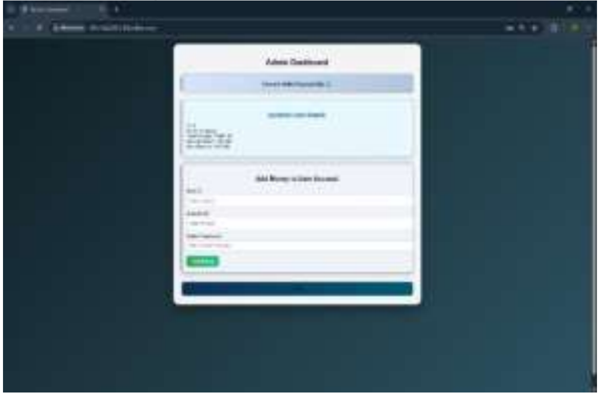
3. After Registration



4.Add Money



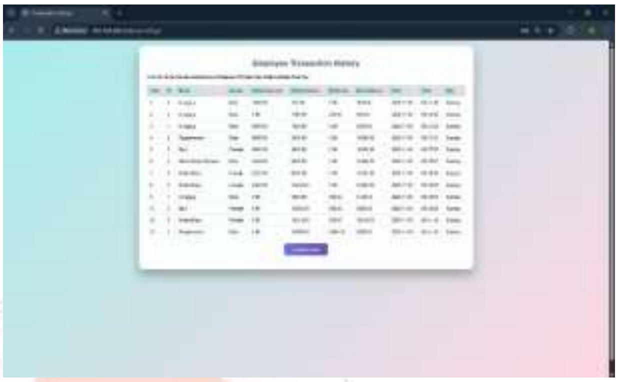
5.After Adding the Money



6.Before Owner Login

7.After Owner Login

8.History Page



IX. Conclusion

This paper presents a Biometric Based Payment System designed to balance security, convenience, and affordability. The system uses fingerprint authentication, which is a reliable method for user verification. A user friendly interface with a keypad and an OLED display allows for easy interaction during enrolment and payment. To protect sensitive user information, the system uses SHA-256 encryption throughout. This encryption secures fingerprint templates in storage and maintains data integrity during transmission to a centralized MySQL database. The system communicates effectively with the central server using the HTTP protocol, allowing for features like transaction history management through a web interface. Lastly, the implementation focuses on affordability by choosing readily available components, such as the ESP32 microcontroller and the R307 fingerprint sensor, making this solution easy to adopt.

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.

References

1. 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.
2. 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.
3. 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.
4. L. Y. Leong, K. B. Ooi, A. Y. L. Chong, and B. Lin, ''Modelling 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. 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.
5. 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
6. 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.
7. 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.
8. M. Ringle, S. Wende, and A. Will, Smart PLS Computer Software. Accessed: Apr. 10, 2015. [Online]. Available: https://www.smartpls.de
9. Ranganathan and S. Ganapathy, ''Key dimensions of business-to consumer Web sites,'' Inf. Manage., vol. 39, no. 6, pp. 457–465, 2002.
10. 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