Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

One Touch Pay: An Innovative Quick and Secure Payment System

Deepa das[1], Manthan Ghosh[2]

[1]School of Computer Science, Ramdeobaba University;

[2]Department of Electronics Engineering, G H Raisoni College of Engineering

Article History:

Received: *01-03-2025*

Revised: *dd-mm-yyyy*

Accepted: *08-03-2025*

Abstract:
In comparison to conventional payment systems, the suggested biometric-based digital transaction system, which uses fingerprint technology, offers improved security, simplicity, and convenience. By removing the need to carry several cards or remember passwords, it reduces clutter and boosts productivity. Biometric readers are becoming more affordable, making them more accessible to small firms. But for implementation to be successful, privacy issues and technological constraints must be overcome, and broad adoption and integration are essential. All things considered, the biometric payment system offers a safe, convenient, and affordable option for banking transactions in e-payment systems.

Keywords: Biometric payment system, Digital wallets, One-touch payment, Payment gateways.

1. Introduction

The fusion of the digital payment age with artificial intelligence (AI) and deep learning technologies has triggered a significant revolution in the financial domain. The collaboration has greatly improved the effectiveness, safety, and customization of online transactions. Artificial intelligence systems, driven by deep learning, have a crucial function in detecting and preventing fraud. They employ sophisticated analytics to detect anomalies and verify users based on biometric characteristics. Furthermore, chatbots and virtual assistants powered by artificial intelligence optimize consumer interactions, offering immediate assistance and improving the overall user experience on digital payment platforms. Machine learning models process extensive datasets derived from digital transactions, resulting in significant insights into customer behavior and expenditure trends. Financial institutions utilize these insights for focused marketing and personalized services. The introduction of 5G technology is set to revolutionize the digital payment industry, working in harmony with the current advancements in digital payments, artificial intelligence (AI), and deep learning. The future of digital payments will be significantly impacted by the fast and responsive nature of 5G networks [20, 21, 22].

AI integration in digital payments enhances security measures and streamlines operational operations, resulting in a smooth and intelligent financial environment. The ongoing development of these technologies will reshape the future of banking by combining the digital payment era with AI and deep learning [17, 18, 19]. This convergence will provide unparalleled convenience, innovation, and data-driven intelligence. Every payment method we use on a regular basis—cash, checks, debit cards, credit cards, etc.—has the difficulty of identifying the authorised person. When making a payment, our attention is mostly focused on the issue with the e-payment system, which relies on traditional features

such a user name, password, or security PIN. What happens if something goes wrong? is a significant question. We put forth a very user-friendly model called the "One Touch Pay" that is very easy to use. The goal of this endeavour is to create an electronic payment system based on one-touch biometric user authentication that completes payments quickly. We came to the conclusion that the Password is the weakest link in our payment system as a result. We must therefore consider the next-generation payment mechanism. i.e., a biometric system, in which they prefer not to wait if the password is incorrect. Human physiological and occasionally behavioural features are used in biometrics. In order to uniquely identify a person, fingerprint authentication uses capture-in to analyse and compare certain biological traits present on the surface of a human finger. Since fingerprints do not change over the course of a person's lifetime, authorities use them to link biometric information (for instance, passport information and a social security number). We utilise a four-digit passcode to improve privacy. A user-friendly user interface is offered by the system. This technology offers fingerprint payment as a more convenient and safer alternative to cash or IC card payments.

2. Related Works

The paperback submits appropriate identity and bank account details to register for a biometric payment card programme at a retail pavilion. The paperback uses the pavilion's cutlet check-up anthology to scan their indication cutlet. The cutlet check-up anthology of the store encrypts several point-to-point measures of the point and keeps a central database of the client's biometric data and banking information. At the POS register, the paperback provides the option of biometric payment. If they opt biometric payment, they enter their Leg law instead of their cutlet at the checkout register using the store's electronic anthology. The electronic anthology either accepts or rejects payment verification by comparing the data from the fresh cheque up to the translated data in the database. Nevertheless, if accepted, the money is electronically sent from the paperback's account to the trafficker. This procedure looks for ways to account for differences in lighting, discrepancies, and other irregularities that the detector introduces during the accession process. There are a variety of similar methods for creating a picture, but some of the more well-known and common ones right now are Gaussian blurring, sliding window discrepancy adaptation, and histogram-based intensity adaptation. In order to extract meaningful information from the input image, point recognition algorithms differ and are based on several approaches. The availability of the system increases with an increase in image concurrency. The smallest unit of print spots, or "pixels," make up an image detector. The amount of light that each pixel of an image detector is exposed to is recorded and divided into smaller units of cells. The improved quantum of pixel is formed application increases with light strength.

3. Proposed Model

The science of fingerprint identification uses a person's physiological and behavioural traits to identify them. In this model, we're going to suggest that instead of using credit cards or debit cards to make purchases in stores, consumers should instead use finger print scanners. To complete the transaction, all a customer needs to do is touch a single item on the screen. We built a system that does not require the use of any passwords or OTPs. It is incredibly simple to use and only accessible to users who have been authenticated. The model's conclusion is that the card-less payment system needs to be replaced with a simpler, more trustworthy, secure, cash-free, and stress-free payment system, such as a biometric payment system, so that no one has to carry around dozens of cards for shopping, travel

passes in offices, universities, or banks, or use them as door locks. Hardware components are mentioned in Table I, which are required to build the prototype.

Table I: Hardware Component Required

SL. No.	List of Hardwares with Quantity		
	Component	Specification	Quantity
1	Power supply	12V/1Amp DC	1
2	Voltage Regulator	FC7805	1
3	LCD Display	16x2 display	1
4	Keypad	4x3 keypad	1
5	Fingerprint Sensor	AS608 Optical Scanner	1

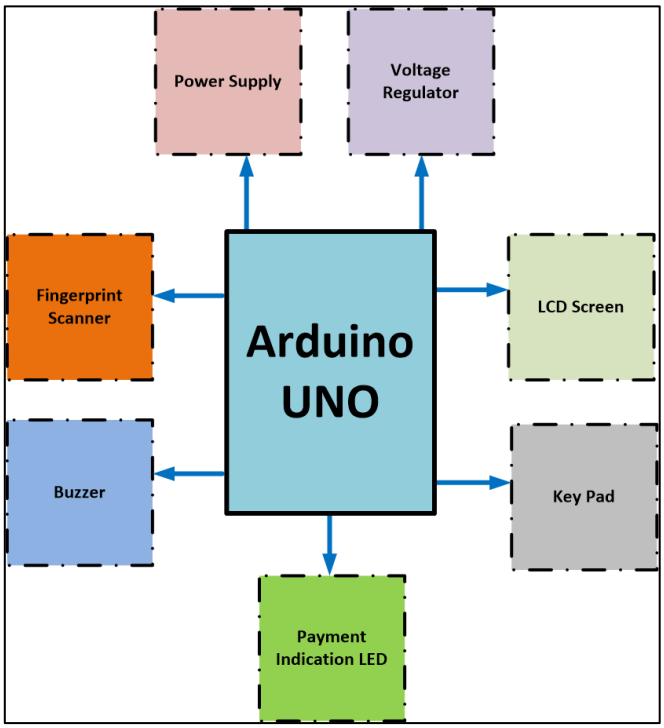

Figure 1: Block Diagram

4. Block Diagram

This block diagram represents an Arduino UNO-based system integrating multiple components for user interaction and control. At the center of the system is the Arduino UNO, a microcontroller that serves as the brain of the project, processing inputs from sensors and peripherals while controlling outputs accordingly. The power supply provides the necessary electrical energy to run the entire system, ensuring stable operation. Connected to it is a voltage regulator, which helps maintain a consistent voltage level, protecting the components from potential fluctuations that could cause

damage or malfunction. For user authentication, a fingerprint scanner is included, allowing biometric verification. This scanner captures and processes fingerprint data, which is then compared to stored records for authentication. If the fingerprint matches, the Arduino UNO processes the next steps accordingly. To provide audible feedback, a buzzer is included, which can generate sounds to indicate successful authentication, errors, or other system notifications. A Liquid Crystal Display (LCD) screen is connected to the Arduino to display messages, prompts, and system status updates to the user. It enhances user interaction by showing real-time feedback, such as authentication results or transaction details. Alongside the LCD screen, a keypad is included, enabling manual input for tasks like entering a PIN, selecting options, or confirming actions. For visual feedback, the system includes a payment indication LED, which lights up to confirm successful authentication or payment completion. This provides an intuitive way for users to understand the system's status without needing to check the display. Overall, this setup appears to be designed for a biometric-based authentication system, possibly for secure transactions or access control. The Arduino UNO acts as the central processing unit, managing inputs from the fingerprint scanner and keypad while controlling outputs such as the LCD screen, buzzer, and LED to ensure a smooth and secure user experience.

5. Algorithm

The algorithm of the proposed system is explained below and the flowchart is shown in figure:2.

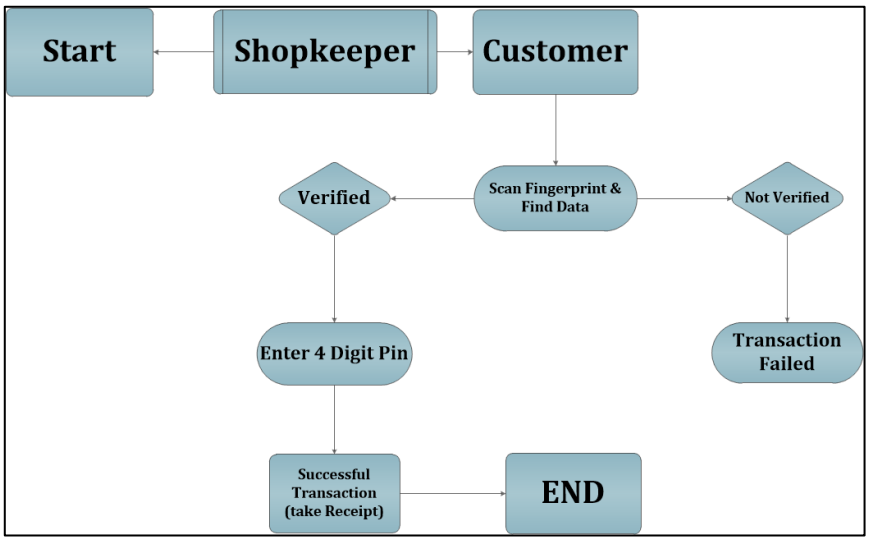

Figure 2: Algorithm Flowchart

All the algorithm steps are mentioned below:

1) The first step starts with the entering the amount by the shopkeeper.
2) Then the customer needs to scan their fingerprint and find customer data.
3) If the customer scan fingerprint verified then they need to enter four-digit pin.
4) If there is a mismatch in the fingerprint then it will generate the error message.
5) After entering the four digits pin the transaction get successful.
6) Finally, it will generate a receipt after successful transaction.

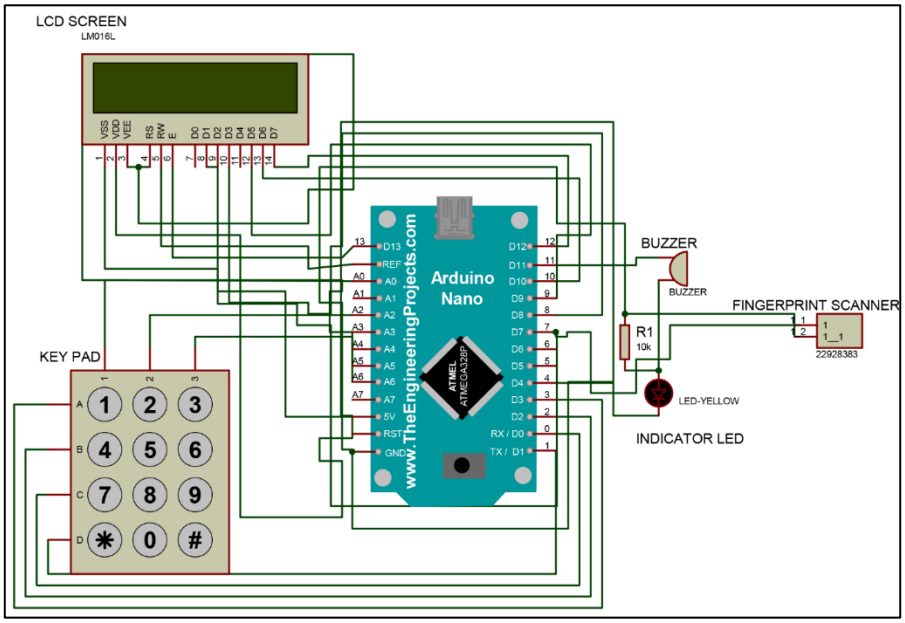

Figure 3: Circuit Diagram

6. Result and Performance Analysis

Therefore, biometric payment operation got designed, developed and enforced successfully. Also, a new fashion of material less payment got introduced to society. It reduces the pressure of people securing their wallets, cash, cards etc. The operation uses point and Leg for security which is simple and causes lower confusion for the guests, unlike OTP and two- step authentications. The sale gets completed with lower number of inputs. It saves druggies from entering long account integers and pets up the process. The use of fingerprints makes it accessible to help unauthorized use as it's unique for every stoner. The sensitive data similar as fingerprints are converted into bytes and stored as a byte array. In terms of data security, the operation is safe to use. No sensitive data gets lost. Eventually, the payment sale is done seamlessly and snappily without involving any mediators similar as payment

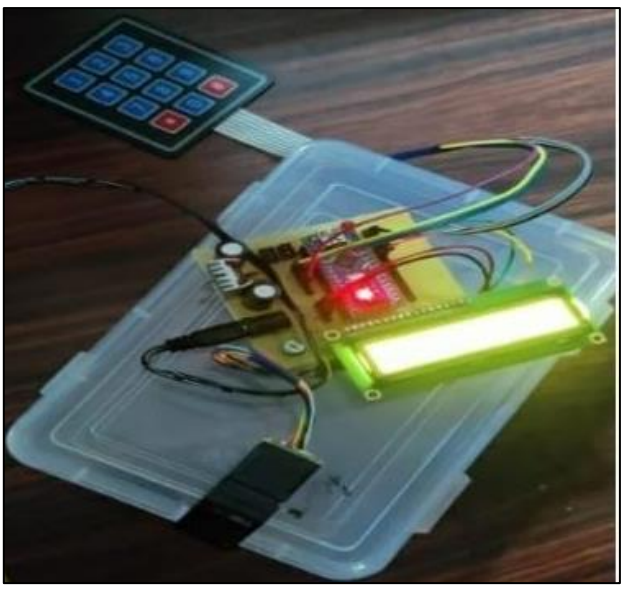

Figure 4: Prototype

gateways. Also, it's a good volition rather of a card swiping machine which requires a periodic subscription. All test cases were successfully tested. The system developed is user friendly, there is no special training is required to use the one touch payment system. The implementation of the biometric payment system brings about numerous benefits to both users and businesses. With the elimination of physical wallets and the need to remember complex passwords, individuals can experience a hassle-free and secure payment experience. The system's user-friendly design ensures that individuals of all backgrounds can easily adapt to and use the one-touch payment method without requiring any special training. Furthermore, businesses can benefit from the system's efficiency and speed, as transactions can be completed swiftly, reducing waiting times and increasing customer satisfaction. The removal of mediators such as payment gateways simplifies the payment process and minimizes transaction costs for businesses. Overall, the biometric payment system offers a convenient, secure, and efficient alternative to traditional payment methods, transforming the way transactions are conducted in society.

7. Conclusion

The model's conclusion is that the card-less payment system needs to be replaced with a simpler, more trustworthy, secure, cash-free, and stress-free payment system, such as a biometric payment system, so that no one has to carry around dozens of cards for shopping, travel passes in offices, universities, or banks, or use them as door locks. The independent third parties who developed the technology are the ones who pay for fingerprinting, though. Market expansion is being slowed down by a lack of credibility, coordination, funds, and other resources. The primary issue in the fingerprint payment sector is credibility. Second, as the market becomes more appealing, more consumers will be willing to accept some technological difficulties, therefore the banks are the ones who need to deal with this issue. Union pays interventions with fingerprint payments priorities fingerprint payments.

Refrences

[1] B. S. Reddy, G. J. Reddy, and E. S. Reddy, "A broad survey on fingerprint recognition systems," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1428–1434, IEEE, 2016.

[2] D. Kumar and Y. Ryu, "A brief introduction of biometrics and fingerprint payment technology," Int. J. Adv. Sci. Technol., vol. 4, pp. 25–38, 2009.

[3] T. K. Kanakam, A. Jubilson, B. Emani, M. Anuhya, S. Sighakolli, V. Chintala, K. Vanamala, D. Kadiri, K. Nayineni, and P. Dhanavanthini, "A concise survey on biometric recognition methods," Int. J. Comput. Digit. Syst., vol. 14, no. 1, pp. 1–1, 2023.

[4] L. Nanni and A. Lumini, "Local binary patterns for a hybrid fingerprint matcher," Pattern Recognit., vol. 41, no. 11, pp. 3461–3466, 2008.

[5] S. M. Rajbhoj and P. B. Mane, "An improved binarization-based algorithm using minutiae approach for fingerprint identification," Int. J. Eng. Adv. Technol. (IJEAT), vol. 1, no. 6, pp. 219–222, 2012.

[6] A. Fatima, "E-banking security issues - Is there a solution in biometrics?," J. Internet Bank. Commer., vol. 16, no. 2, pp. 1–1, 2011.

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," Comput. Netw., vol. 170, p. 107118, 2020.

[9] R. Brown, G. Bendiab, S. Shiaeles, and B. Ghita, "A novel multimodal biometric authentication system using machine learning and Blockchain," in Selected Papers from the 12th International Networking Conference: INC 2020, pp. 31–46, Springer, 2021.

[10] B. Alemu, R. Kumar, D. Sinwar, and G. Raghuwanshi, "Fingerprint-based authentication architecture for accessing multiple cloud computing services using single user credential in IoT environments," in J. Phys.: Conf. Ser., vol. 1714, no. 1, p. 012016, IOP Publishing, 2021.

[11] S. Sarhan, S. Alhassan, and S. Elmougy, "Multimodal biometric systems: A comparative study," Arab. J. Sci. Eng., vol. 42, pp. 443–457, 2017.

[12] M. H. Ali, A. Ibrahim, H. Wahbah, and I. Al-Barazanchi, "Survey on encode biometric data for transmission in wireless communication networks," Period. Eng. Nat. Sci., vol. 9, no. 4, pp. 1038–1055, 2021.

[13] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in 2013 Proceedings IEEE INFOCOM, pp. 2652–2660, IEEE, 2013.

[14] A. O. Ekpezu, E. E. Umoh, F. N. Koranteng, and J. A. Abandoh-Sam, "Biometric authentication schemes and methods on mobile devices: A systematic review," in Modern Theories and Practices for Cyber Ethics and Security Compliance, pp. 172–192, 2020.

[15] R. P. Sharma and S. Dey, "Fingerprint liveness detection using local quality features," Vis. Comput., vol. 35, no. 10, pp. 1393–1410, 2019.

[16] D. Nigam, S. N. Patel, P. M. R. Vincent, K. Srinivasan, and S. Arunmozhi, "Biometric authentication for intelligent and privacy-preserving healthcare systems," J. Healthc. Eng., vol. 2022, 2022.

[17] N. Sinha, M. Ghosh, S. Majumder, and B. B. Bhowmik, "Deep learning-based noise identification in optical fiber communication using variational mode decomposition," in 2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC), pp. 1–5, IEEE, 2021.

[18] M. Ghosh, "Comparative DNN model analysis for detection of various types of optical noise," Authorea Preprints, 2023.

[19] M. Ghosh, M. Raut, R. Parteki, D. Das, L. P. Thakare, R. Jichkar, S. S. Rathore, and S. Bawankar, "An analysis of deep-neural-network model for the determination of the bit-rate of optical fiber signals," in 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP), pp. 1–4, IEEE, 2023.

[20] R. Jichkar, S. Paraskar, R. Parteki, M. Ghosh, T. Deotale, A. S. Pathan, S. Bawankar, and L. P. Thakare, "5G: An emerging technology and its advancement," in 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP), pp. 1–6, IEEE, 2023.

[21] Ghosh, Manthan, and Deepa Das. "Voice-Activated SOS: An AI-Enabled Wearable Device." In Impact of AI on Advancing Women's Safety, pp. 251-277. IGI Global Scientific Publishing, 2024.

[22] Pradhan, Devasis, Prasanna Kumar Sahu, Hla Myo Tun, and Prasenjit Chatterjee, eds. Artificial and Cognitive Computing for Sustainable Healthcare Systems in Smart Cities. John Wiley & Sons, 2024.