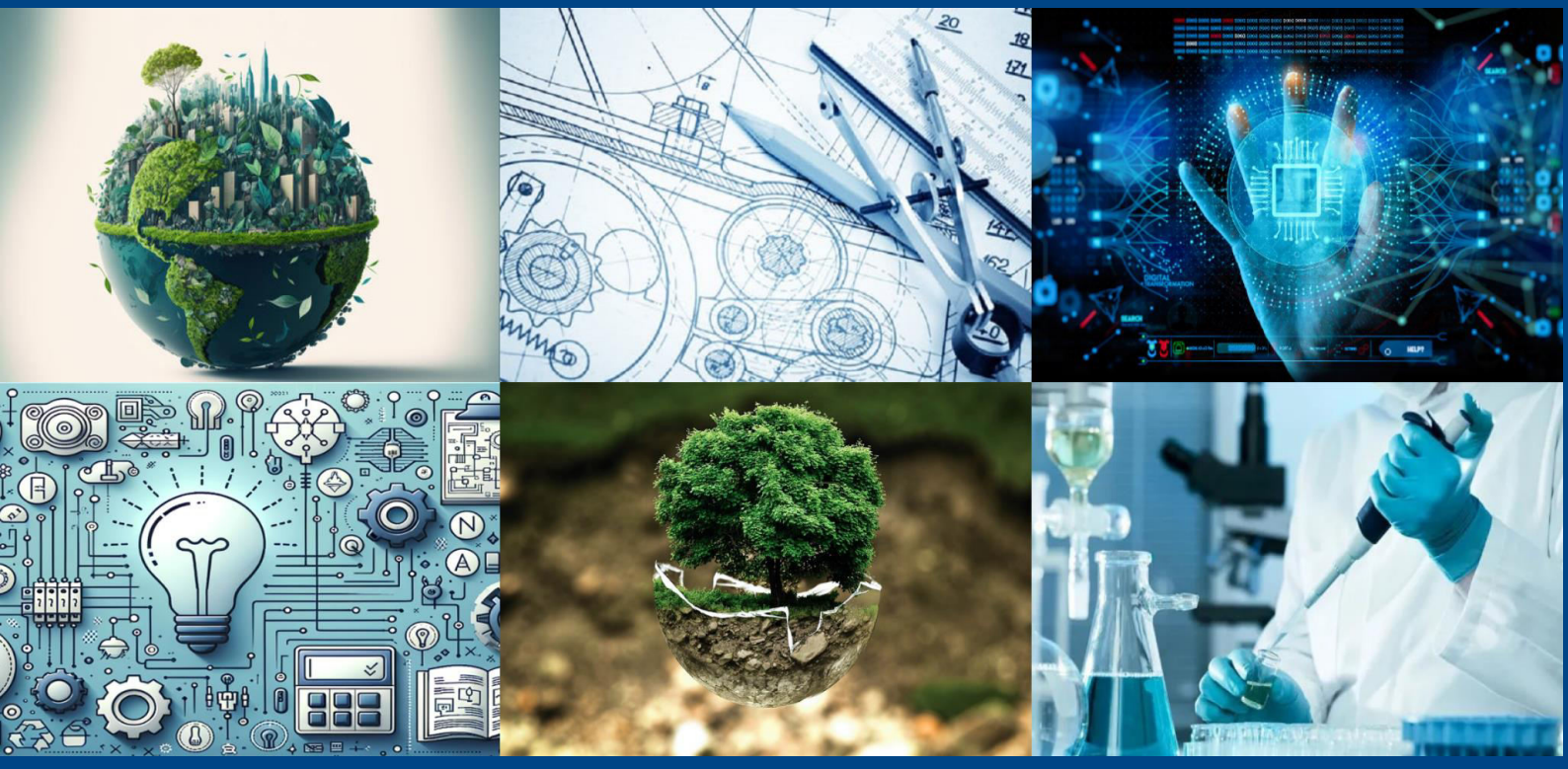
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805157

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Payment by Facial Recognition using Haar Cascade Algorithm

Dr. V. Seedha Devi [1], Muhilan.P [2], Mugundhan.G [3], Raghul.M [4],

Associate Professor, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India [1]

UG Student, Dept. of IT, Jaya Engineering College, Chennai, Tamil Nadu, India[2],[3] & [4]

ABSTRACT: In today's fast-paced digital world, time is a crucial resource. Traditional payment methods—cash, credit cards, and mobile wallets—often involve several steps such as authentication, card insertion, PIN entry, and network processing, which can cause delays and inefficiencies. To address these issues, we propose a Face Recognition Payment System that enables users to make payments instantly through facial authentication, eliminating the need for physical cards or manual input. This system uses the Haar Cascade algorithm, a machine learning-based technique for rapid and accurate face detection. The process begins with user registration via a mobile application, where facial data and payment credentials are securely stored in a database. When a payment is initiated, the user's face is captured using a scanner and matched against the stored data. Upon successful verification, the payment is processed and a confirmation message is sent. The system enhances security by reducing risks associated with card fraud, PIN theft, and unauthorized transactions. It also provides a contact-less, hands-free experience, which is especially useful in public spaces where hygiene and speed are essential. By integrating facial recognition into payment systems, transactions become faster, more secure, and more convenient. This approach has the potential to transform payments in retail, dining, transportation, and other commercial environments.

KEYWORDS: Artificial intelligence, Machine learning, Contactless payment, Haar Cascade, Biometrics, Secure payment, Fast and Convenient payment.

I. INTRODUCTION

In the modern digital age, there is an increasing demand for secure, efficient, and contact-less payment systems. Traditional payment methods such as cash, cards, and mobile wallets often come with drawbacks like the risk of theft, loss, or fraud, making them less reliable in today's fast-paced world. To address these issues, this project introduces a Facial Recognition Payment System that leverages artificial intelligence and computer vision to provide a seamless and secure transaction experience. The system allows users to register by submitting personal details and facial images, which are then stored and processed using the Local Binary Pattern Histogram (LBPH) algorithm for facial recognition. Face detection is handled using the Haar Cascade classifier to ensure real-time and accurate identification. Once registered, users are assigned wallet points that can be used for payments without the need for physical cards or smartphones.

At the point of transaction, a scanner application captures the user's face, verifies it against the trained model, and deducts the specified amount from the user's wallet. A shopkeeper dashboard displays real-time transaction logs including user name, amount transferred, and timestamp for transparency. Developed using Python, Flask, Open-CV, and SQLite, the system ensures smooth back-end operations and secure data handling. It supports anti-spoofing measures and encrypts sensitive information to enhance privacy. Designed for cross-platform compatibility, the system is ideal for environments such as retail outlets, educational institutions, and hospitals. It also promotes hygienic, contactless interactions, which are particularly relevant in a post-pandemic context. With its modular design and future-ready framework, the Facial Recognition Payment System sets the stage for smarter, faster, and safer financial transactions driven by biometric authentication.

II. SYSTEM MODEL AND ASSUMPTIONS

The proposed Facial Recognition Payment System is designed as a three-tier architecture consisting of a user-facing web application, a face recognition scanner module, and a shopkeeper dashboard. The system operates in both local and cloud environments and assumes access to a webcam-enabled device for capturing facial data. The user module enables registration by collecting personal details, card information, and facial images. These images are processed and stored

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805157

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

locally or remotely, and a facial recognition model is trained using the LBPH (Local Binary Pattern Histogram) algorithm. During login or payment, the user's live facial image is captured and matched with the trained data using Haar Cascade for detection and LBPH for recognition. The scanner module installed at merchant points of sale verifies users and deducts wallet points upon successful face match. It assumes that users are pre-registered and have sufficient wallet points. The shopkeeper dashboard fetches and displays real-time transaction data from a secure database, showing user ID, name, transferred points, and timestamp.

The system assumes that each user's facial data is unique and consistent under controlled environmental conditions, such as adequate lighting and a frontal face view. It also assumes that the user database and trained facial models are secure and tamper-proof. The model operates under the assumption that users will not attempt to spoof the system using photos or videos; however, basic liveness detection measures are considered. The system expects reliable internet or local network connectivity for communication between modules, and the database is assumed to be synchronized and backed up. Hardware assumptions include a minimum of a 720p webcam, a standard desktop or Raspberry Pi for processing, and basic server configurations for hosting the backend. On the software side, it assumes compatibility with Python, OpenCV, Flask, and SQLite or MySQL. Lastly, it is assumed that the system operates within a trusted environment where both users and shopkeepers are verified entities and adhere to ethical usage of biometric data.

III. EFFICIENT COMMUNICATION

The Facial Recognition Payment System is designed with efficient communication protocols to ensure seamless interaction between the user web application, face recognition scanner, and shopkeeper dashboard. Communication occurs primarily through RESTful APIs built on the Flask backend, enabling smooth data exchange in JSON format. When a user registers, their personal and facial data are securely transmitted to the server and stored in the database. During authentication, the face scanner captures live facial input and sends it to the recognition service, which promptly verifies the identity by matching it against stored templates. Upon successful authentication, the wallet deduction request is sent back to the server, which updates the user's balance and logs the transaction in real time. The shopkeeper dashboard periodically queries the transaction database to fetch and display the latest payment records, ensuring transparency. To minimize latency and improve responsiveness, data transfers are optimized and occur asynchronously where possible. Secure HTTPS communication encrypts all sensitive data, safeguarding biometric information and financial details against interception. This well-structured communication flow maintains data integrity, provides rapid feedback during payments, and supports concurrent transactions without compromising system performance

IV. SECURITY

Security plays a central role in the Facial Recognition Payment System to ensure that users' sensitive data—like their face images, personal details, and transaction history—remains safe and protected at all times. To achieve this, the system applies multiple layers of security mechanisms. First, all biometric and personal data is encrypted, meaning the data is converted into a secure code that cannot be easily read or understood by unauthorized parties. This prevents hackers from accessing or misusing stored information, even if they breach the system.

The system strictly follows international privacy regulations, such as:

- **GDPR (General Data Protection Regulation):** A data protection law enforced in the European Union that gives users full control over their personal data. It ensures that user data is collected with consent, used only for specific purposes, and stored securely. It also gives users the right to view, update, or delete their data at any time.
- **CCPA (California Consumer Privacy Act):** A similar law in California, USA, that gives users the right to know what data is being collected, opt out of data sharing, and request the deletion of their information. This law ensures transparency and protects users from the misuse of their personal information.

By complying with these laws, the system ensures that all personal and biometric data is handled ethically and legally, giving users peace of mind that their privacy is respected. To protect data in motion, the system uses HTTPS (HyperText Transfer Protocol Secure), which encrypts all communication between the user's browser, the face scanner, and the backend server. This prevents third parties from spying on or stealing information during data transmission, such as login details or face data. To stop fraudsters from tricking the system using photos or videos, liveness detection

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805157

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

is implemented. This ensures that only a real, live person can authenticate, adding another level of safety to facial recognition.

The face recognition functionality uses:

- Haar Cascade for detecting where the face is in an image (fast and lightweight).
- LBPH (Local Binary Pattern Histogram) for recognizing whose face it is, even under different lighting or facial expressions.

To further secure access, role-based access control is applied. This means that only certain people (like shopkeepers or admins) can view or manage sensitive data such as transaction logs. Regular users cannot access or modify data they're not authorized to see. Every transaction is logged in a tamper-proof database. This means no one can alter the records after a transaction is completed. This ensures full transparency and creates a clear record in case of disputes or audits. Before a transaction is allowed, the system checks if the user has enough wallet balance, preventing unauthorized deductions or overdrafts. In addition, the software components used in the system—like OpenCV for face recognition and Flask for backend communication—are regularly updated to patch any known security flaws, keeping the system protected from new threats. Lastly, users have full control over their biometric data. If they wish to update or delete their face data, the system allows them to do so, giving users ownership and flexibility over their personal information.

V. RESULT AND DISCUSSION

In the fig 1, In This figure welcome page of the FacePay system, offering users the option to either register a new account or log in to an existing one. The clean and simple interface features a blue gradient background with clearly visible buttons for easy navigation

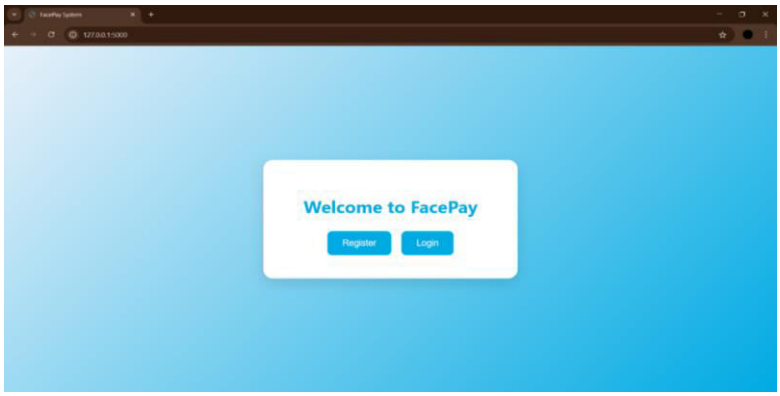


Fig.1 Welcome page of the Face-pay system

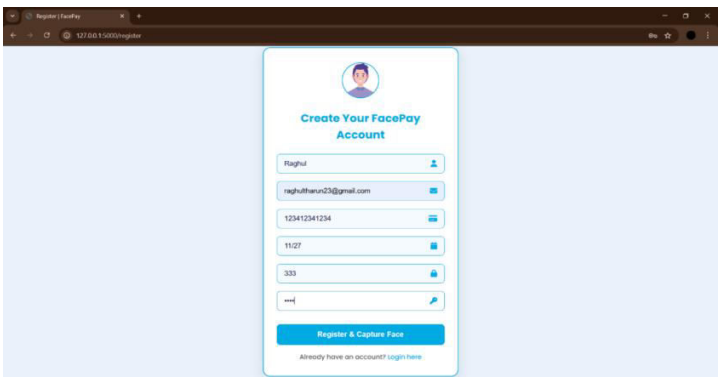


Fig.2 Face Pay registration page

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805157

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This is the FacePay registration page where users enter personal and card details to create an account. The "Register & Capture Face" button initiates facial data capture for secure authentication.

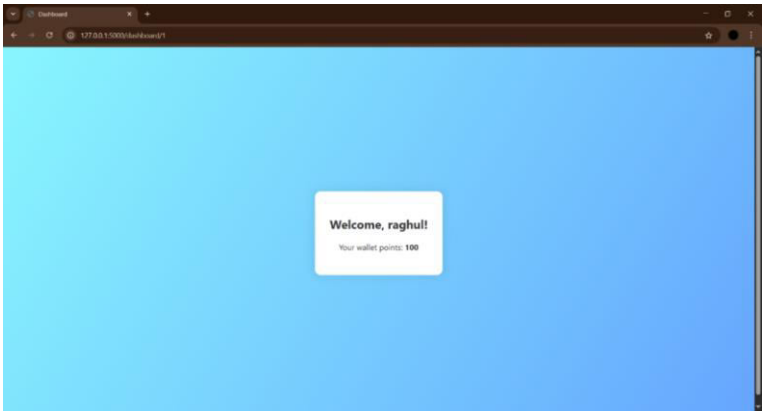


Fig.3 Login page

The login page allows users to access their Face-pay account by entering their registered email and password. It features a simple, clean design for quick and secure sign-in.

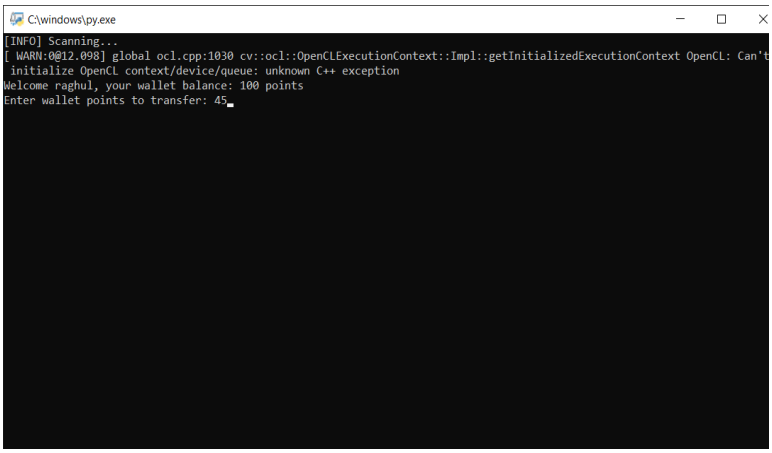


Fig4 Face capturing and wallet transferring

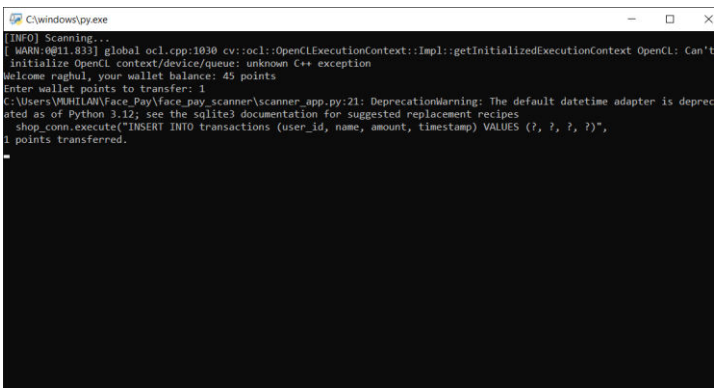


Fig.5 Wallet transferred

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805157

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

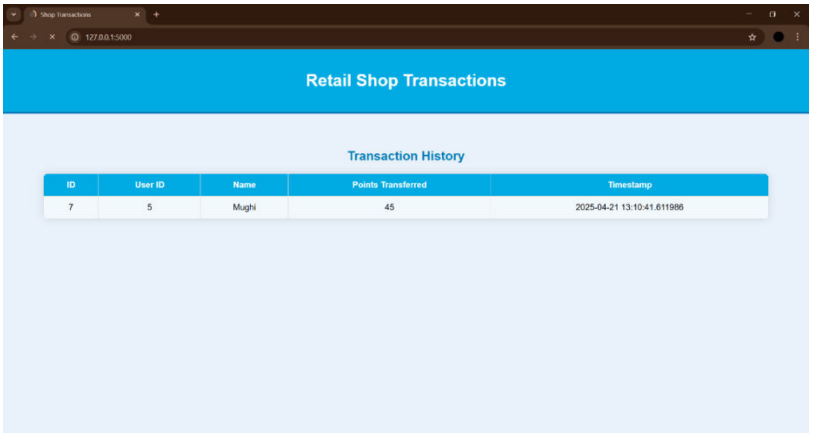


Fig.6 Shop Website

VI. CONCLUSION

The Facial Recognition Payment System provides a secure, contactless way to make payments using biometric authentication. It eliminates reliance on physical cards and passwords, enhancing convenience and security. Real-time face recognition and wallet management enable fast transactions. Robust security features protect user data and prevent fraud. This project showcases the potential of AI-driven biometric solutions in modern payment systems

REFERENCES

[1] Facial-Recognition Payment: An Example of Chinese Consumers, Wen Kun Zhang ; Min Jung Kang, IEEE Access, Year: 2019
[2] Secure multifactor authentication payment system using NFC, Anirudhan Adukkathayar ; Gokul S Krishnan ; Rajashree Chinchole, 2015 10th International Conference on Computer Science & Education (ICCSE)
[3] Biometric Face Recognition Payment System , Surekha. R. Gondkar Saurab. Dr. C. S. Mala International Journal of Engineering Research & Technology NCESC- 2018 Conference Proceedings
[4] Facial Recognition in Banking – Current Applications, Niccolo Mejia,2019 Conference Proceedings
[5] "Face Detection and Recognition for Bank Transaction ", International Journal of Emerging Technologies and Innovative Research , Sudarshan Dumbre ,Shamita Kulkarni ,Devashree Deshpande ,P.V.Mulmule Journal of Emerging Technologies and Innovative Research 2018
[6] Continuous User Identity Verification Using Biometric Traits for Secure Internet Services, Dr.SHAIK ADBUL MUZZER, 2GOSALA SUBHASIN
[7] Skin color based Face detection Method, Devendra Singh Raghuvanshi,Dheeraj Agrawal
[8] Face Detection system based on retinal connected neural network (RCNN), Rowley, Baluja and Kanade
[9] Combining Skin Color based Classifiers and HAAR Feature using VJ Algorithm, N.Gobinathan, Abinaya and Geetha. P
[10] Face Detection and Recognition for Bank Transaction, Sudarshan Dumbre1, Shamita Kulkarni2 , Devashree Deshpande3 , Prof P.V.Mulmule4
[11] 'Haxby, J.V., Ungerleider, L.G., Horwitz, B., Maisog, J.M., Rapoport, S.I., and Grady, C.L. (1996). Face encoding and recognition in the human brain. Proc. Nat.Acad. Sci. 93: 922 – 927
[12] Li, S. Z., & Jain, A. K. (Eds.). (2011). Handbook of Face Recognition. Springer.
[13] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer.
[14] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM Computing Surveys, 35(4), 399–458.
[15] Yang, J., Lei, Z., & Li, S. Z. (2014). Learn face representation from scratch. arXiv preprint arXiv:1411.7923.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com