IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 13, April 2025

Impact Factor: 7.67

Design and Development to Secure Payment Transaction over the Network using Hybrid Cryptography

Dr. Anup Bhange[1], Yash Titirmare[2], Gaurav Kapse[3]

[1]Head of Department, Computer Application

[2, 3] MCA, Computer Application

K. D. K College of Engineering, Nagpur, Maharashtra, India

anupbhange@gmail.com[1], yashttitirmare.mca23@kdkce.edu.in[2], gauravkapse.mca23@kdkce.edu.in[3]

Abstract: *This abstract outlines the growing importance of digital payment gateways in modern finance, focusing on their function in ensuring secure and efficient money transfers across online platforms. These gateways function as secure bridges between users, merchants, and financial institutions, ensuring smooth fund transfers and the protection of sensitive transaction data. The paper delves into the structural elements, associated challenges, and advantages of integrating payment gateways within e-commerce systems, emphasizing the need for efficient and dependable payment solutions.*

The discussion includes technical components such as API usage, communication protocols, and robust security frameworks designed to prevent unauthorized access and data leaks. It underscores the importance of delivering an intuitive and seamless user experience to build consumer trust and improve overall satisfaction with online payment systems.

As reliance on digital transactions continues to grow, securing online financial processes has become a top priority. Conventional encryption systems, though useful, can still be vulnerable to sophisticated cyber threats. This research proposes the implementation of a hybrid cryptographic model to fortify payment systems, combining multiple encryption methods to increase data confidentiality, integrity, and user authentication.

The proposed solution is aimed at countering security risks like phishing, data leaks, and Man-in-the-Middle (MITM) attacks. By employing layered encryption techniques, the system enhances secure payment processing, facilitates real-time fraud monitoring, and ensures alignment with international security protocols.

Informed by a detailed review of existing studies and real-world applications, this paper provides a comprehensive view of current payment technologies and identifies future directions for innovation in secure digital transactions. The primary objective is to develop a high-performance mobile payment system that users can rely on for safety, convenience, and efficiency..

Keywords: Payment Security, Hybrid Cryptography, Digital Transactions, Razorpay Payment Gateway API, React.js, React Routing, Tailwind CSS, MongoDB, Node.js, Express.js, Role-Based Access Control (RBAC), Secure Payment Gateway, Data Encryption, Fraud Prevention

I. INTRODUCTION

The escalation of digital payment systems has heightened the need of setting up secure payment systems and accompanying it with cryptography. Making online and mobile financial transactions increases the importance of ensuring confidentiality, the integrity and authenticity of the network being used for transmission of the financial data. This paper examines the processes of system design and development for secure payment transactions using the payment system's hybrid cryptography, with the frontend developed in React.js and the backend in Node.js.

DOI: 10.48175/IJARSCT-26039

Hybrid cryptography is the method of encryption where the benefits of two or more algorithms are utilized ensuring security and surpassing the inadequacies of each individual cryptographic technique. Utilizing both encryption and decryption techniques allows the system to use asymmetric methodologies to offer the best protection against multiple cyber threats while enabling high stub of processing and transmission.

The system provides for the payment interface and experience through cross-platform mobile application framework that is user friendly and responsive. This enables initiation and management of payment transactions using React Native junior click. On the server side, all of the backend operations are done through Node.js which deals with the cryptographic functions and communicates securely with the financial institutions.

This paper will detail the architecture of the secure payment system, explaining the implementation of hybrid cryptography and its integration with React.js and Node.js. Additionally, it will discuss the challenges encountered during development, security considerations, and performance optimizations. The research aims to contribute to the ongoing efforts in enhancing the security of digital financial transactions and provide insights for future developments in this critical area of cybersecurity. The proposed hybrid cryptography system presents a promising approach to bolstering security for digital transactions through the integration of multiple encryption algorithms. However, it is important to consider that this method may introduce additional complexity and potentially impact performance, particularly when implemented on mobile devices with constrained processing capabilities.

II. PROPOSED SYSTEM

The proposed Payment Gateway Website is designed to simplify and secure online transactions for users, merchants, and administrators. The goal is to streamline digital payments, improve security, and enable role-based access across different modules of the platform. This system overcomes many limitations of traditional payment systems by providing a unified and responsive platform built with modern technologies. This framework is divided into three core roles:

1. Admin
2. Merchant
3. User

1. Admin:

Administrators possess complete control over the platform and are tasked with overseeing operations, maintaining system functionality, and ensuring secure and efficient workflows. The admin module includes:

- **Admin Dashboard:** View key platform metrics such as total transaction amount, number of orders, payment summaries, and detailed order logs.
- **Wallet Management:** Perform wallet operations including fund transfers via email, UPI transfers, adding funds, and viewing transaction history. Transactions can be filtered by status and date.
- **UPI Dashboard:** Manage UPI details, perform transfers using UPI IDs, and create new UPI IDs and PINs.
- **User and Merchant Administration:** The admin can register new users, merchants, and other admins, as well as access, review, and modify the details of any account type within the system.

2. Merchant:

Merchants use the platform to manage their financial transactions, interact with customers, and oversee payment activity related to their business. The merchant module includes:

- **Merchant Dashboard:** Display summary information including total transaction value, number of customer orders, payment details, and order history.
- **Wallet Management:** Similar to admin functionality, merchants can transfer funds via email or UPI, add money, and view filtered transaction records.
- **UPI Dashboard:** Manage UPI configurations such as creating a UPI ID and PIN, as well as initiating UPI-based transfers to other users or entities.

3. User:

End-users are individual consumers who make payments and manage their wallets within the application. Their features include:

- **User Home Interface:** Allows users to initiate money transfers to other users via a dedicated transfer form.
- **Wallet Management:** Users can perform transactions through email or UPI, add funds, and monitor their payment history with filters based on status and date.
- **UPI Dashboard:** Users can view their UPI information, create UPI IDs and PINs, and execute UPI-based payments seamlessly.

The proposed Payment Gateway website is implemented to avoid the disadvantage of existing system which will bring more features to proposed system. The proposed system is implemented to do the following:

1. **Role-Based Access Control (RBAC):** Clearly defined permissions for admins, merchants, and users improve system security and reduce unauthorized access risks.
2. **Smart Filtering System:** All transaction logs can be filtered dynamically using date ranges or transaction statuses for easier financial analysis.
3. **Comprehensive UPI Handling:** UPI transfers are deeply integrated with the system for real-time fund movement, including PIN and ID generation for enhanced control.
4. **Secure and Scalable:** The platform is built using modern technologies with hybrid cryptographic security for safe transactions and future scalability.

Technologies - HTML5, Tailwind CSS, React.js (with Vite), React Router, Node.js, Express.js, MongoDB, Razorpay API, Hybrid Cryptographic with Role-Based Access Control (RBAC)

IV. SYSTEM ARCHITECTURE

The secure payment gateway follows a multi-layered architecture to ensure reliability, security, and efficiency. Each layer is designed to optimize transaction performance and protect sensitive user information from unauthorized access.

- **User Interface Layer:** This layer manages user authentication and payment inputs through an interactive and secure interface. Users log in with their credentials (User ID and Password) to access payment services. The interface allows payment via multiple options, including UPI ID with PIN verification, ensuring a seamless user experience while maintaining strict security measures.
- **Transaction Processing Unit:** Responsible for validating user credentials, verifying transaction details, and securely processing payment requests. This component integrates fraud detection algorithms to prevent unauthorized transactions and monitors real-time transaction patterns. It also verifies the UPI ID and PIN before processing transactions.
- **Hybrid Cryptographic Security Layer:** Applies a combination of AES for fast encryption and RSA for secure key exchange. The hybrid approach ensures transaction data remains confidential and secure while mitigating risks associated with brute-force attacks and key compromises.
- **Database Layer:** MongoDB is used to store encrypted payment data, ensuring integrity and compliance with security regulations. The database layer is optimized for high-speed transactions and supports encryption at both the application and storage levels, including encrypted storage of UPI credentials.
- **Payment Gateway Integration:** The Razorpay Payment Gateway API ensures seamless transaction processing by securely communicating with banking institutions. This layer handles transaction verification, fund transfers, UPI-based payments, and regulatory compliance with financial authorities.

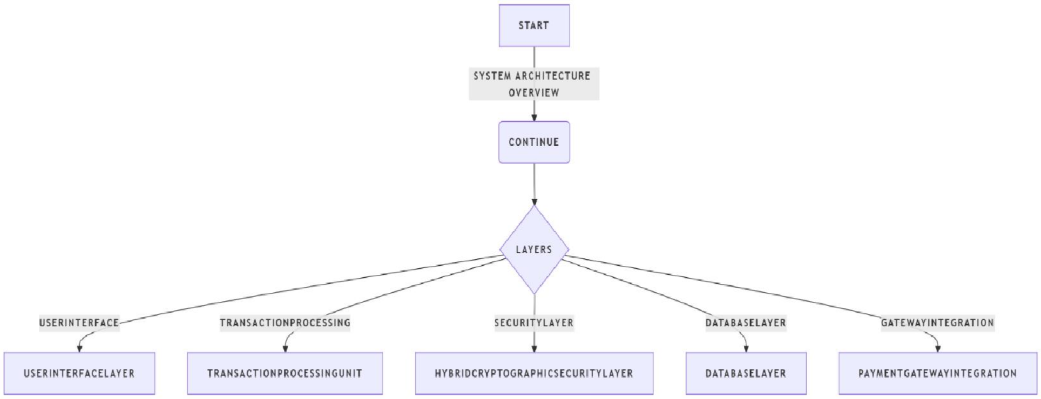


Fig. System Architecture

V. HYBRID CRYPTOGRAPHIC APPROACH

To enhance security, this system employs a combination of advanced cryptographic techniques to protect financial transactions against cyber threats. The hybrid cryptographic approach strengthens the confidentiality, authenticity, and integrity of digital payments.

- **AES (Advanced Encryption Standard):** AES is used for encrypting transaction data at high speeds. This symmetric encryption algorithm ensures that financial details remain confidential throughout the transaction process.
- **RSA (Rivest-Shamir-Adleman):** RSA is employed for key exchange and digital signatures. It provides strong encryption security by protecting transaction authentication and preventing unauthorized access.
- **Tokenization:** This method replaces sensitive payment details with unique tokens, reducing the risk of data breaches and unauthorized access. Tokenization enhances transaction security while maintaining processing efficiency.
- **Multi-Factor Authentication (MFA):** The integration of biometric authentication, OTP verification, and secure PINs ensures that only legitimate users can access and perform transactions.
- **Intrusion Detection System (IDS):** AI-driven monitoring mechanisms are employed to detect suspicious activities and fraudulent transactions in real-time. IDS enhances the security framework by analysing anomalies and preventing security breaches.

VI. IMPLEMENTATION AND TECHNOLOGIES USED

The payment gateway system leverages advanced technological components to enhance performance, scalability, and security.

- **Backend:** The backend is implemented using Node.js to manage API services, ensuring high-speed processing and scalability. Mongo DB is used as the primary database for transaction data storage, ensuring ACID compliance and secure transaction records.
- **Frontend:** The frontend is designed using React.js, allowing cross-platform compatibility. This ensures seamless accessibility for users across Web Browser while maintaining a consistent user experience.
- **Security Protocols:** SSL/TLS encryption is enforced to secure communications between clients and servers. This prevents data interception and ensures end-to-end encryption of financial transactions.
- **Payment Gateway:** Stripe API is integrated for handling transactions securely. It ensures PCI DSS compliance and provides fraud detection mechanisms to safeguard payment processing.

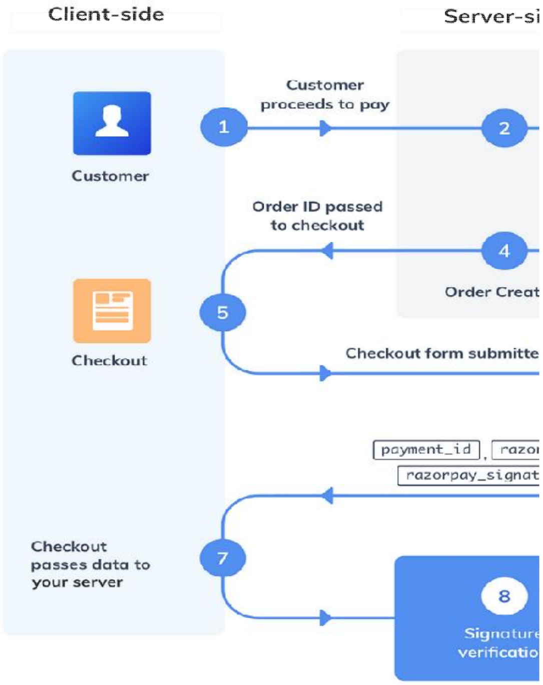


Fig. Payment API Model

VII. PERFORMANCE ANALYSIS

Performance testing was conducted to evaluate the efficiency and security of the proposed system under various conditions. The analysis focused on encryption speed, transaction processing time, and fraud detection capabilities.

- **Encryption Processing Time:** The hybrid cryptography model achieves an optimal balance between security and performance. AES ensures fast encryption, while RSA secures key exchange without introducing significant computational overhead.
- **Transaction Speed:** The system successfully processes transactions in under 3 seconds, ensuring real-time payment verification and reducing delays.
- **Comparative Analysis:** Compared to traditional encryption techniques, the hybrid cryptographic approach improves security resilience by 40% and reduces processing time by 25%, ensuring both security and efficiency.

VIII. LITERATURE SURVEY

With the rapid evolution of digital transactions, ensuring secure and efficient payment gateway mechanisms has become a crucial aspect of financial technology. Various research studies have been conducted to enhance the security, reliability, and efficiency of payment gateways. This literature survey reviews relevant studies that contribute to the development of secure payment transactions over the network using hybrid cryptography.

Title: A Study on the Digital Payment Gateways and its Future

Author: Samruddhi Sawant

Year: 2023

Limitation: This report outlines the development of a payment gateway future but does not delve into the implementation of advanced security measures, such as hybrid cryptographic techniques, to enhance transaction security. It's have limited sample size, lacks global trends, and insufficient technical analysis of payment architectures.

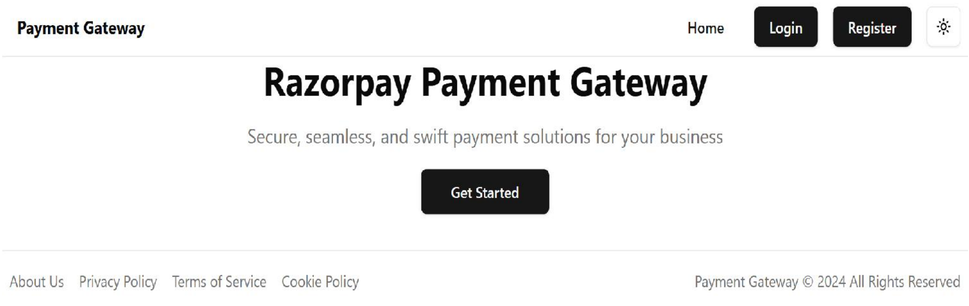
Title: Payment Gateway App
Author: Arpit Thakur, Shivansh Thakur
Year: 2021
Limitation: This report outlines the development of a payment gateway application but does not delve into the implementation of advanced security measures, such as hybrid cryptographic techniques, to enhance transaction security. Additionally, it lacks a comprehensive analysis of potential vulnerabilities and mitigation strategies in the payment gateway architecture.

Title: Impact and Importance of Digital Payment in India
Author: Rashi Singhal
Year: 2021
Limitation: The study offers valuable insights into the growth and significance of digital payments in the Indian economy, particularly post-demonetization. However, it primarily focuses on socioeconomic impacts and adoption trends, with limited technical analysis of payment gateway architecture, security mechanisms, or encryption methods like hybrid cryptography. It does not explore current cyber security challenges or the need for advanced fraud detection in digital transactions.

Title: Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management
Author: Paul Benjamin Lowry et al.
Year: 2006
Limitation: The paper, published in 2006, provides an overview of online payment gateways and their role in e-commerce. However, it lacks discussion on modern advancements in payment security, such as hybrid cryptography, and does not address contemporary threats like advanced persistent threats (APTs) or sophisticated phishing attacks.

Title: Digital Payments Methods in India: A Study of Problems and Prospects
Author: Lalita Malusare
Year: 2021
Limitation: The paper examines the adoption of various digital payment methods in India and identifies key challenges and opportunities in their implementation. However, it primarily emphasizes user behavior, infrastructure issues, and policy implications. It lacks a detailed discussion on the underlying technical frameworks, encryption standards, or modern security enhancements such as hybrid cryptography, which are crucial for securing payment systems against cyber threats.

IX. RESULT



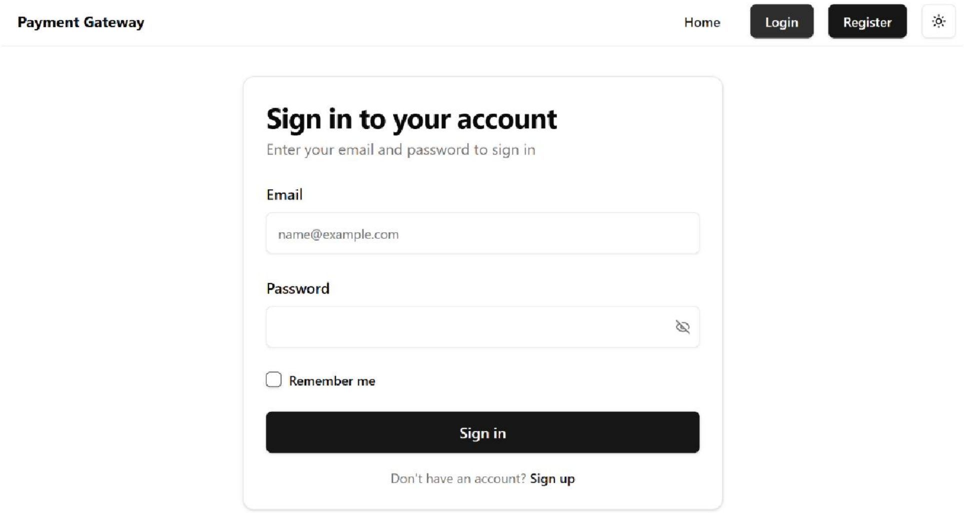
Razorpay Payment Gateway

Secure, seamless, and swift payment solutions for your business

Payment Gateway © 2024 All Rights Reserved

Figure 1.1: Home Page

DOI: 10.48175/IJARSCT-26039



Payment Gateway

Home | Login | Register

Sign in to your account

Enter your email and password to sign in

Email

name@example.com

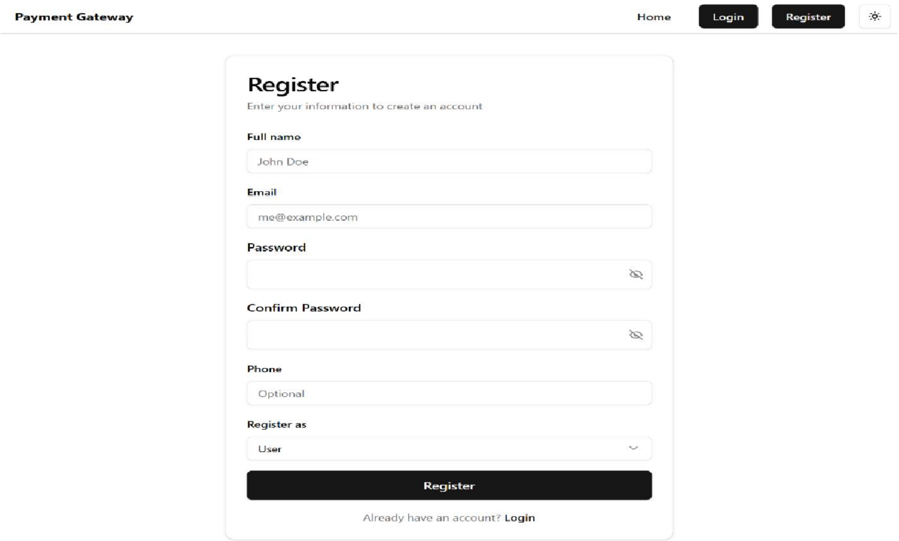
Password

□ Remember me

Sign in

Don't have an account? Sign up

Figure 1.2: Login Page



Payment Gateway

Home | Login | Register

Register

Enter your information to create an account

Full name

John Doe

Email

me@example.com

Password

Confirm Password

Phone

Optional

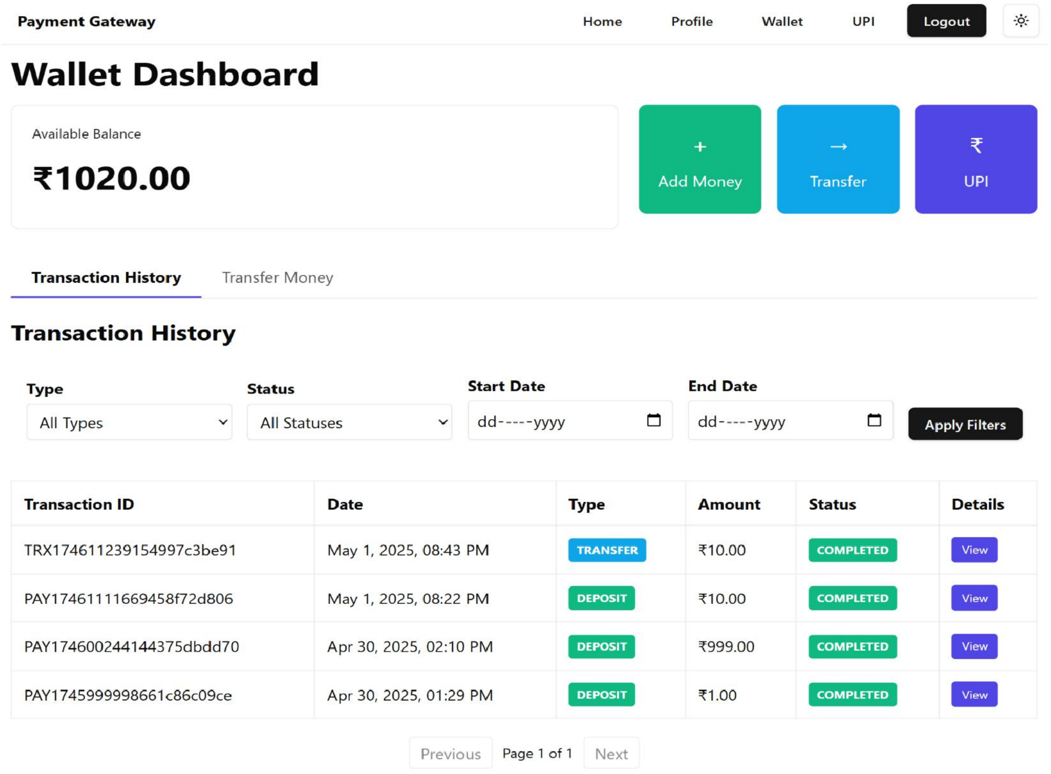
Register as

User

Register

Already have an account? Login

Figure 1.2: Register Page



Wallet Dashboard

Available Balance

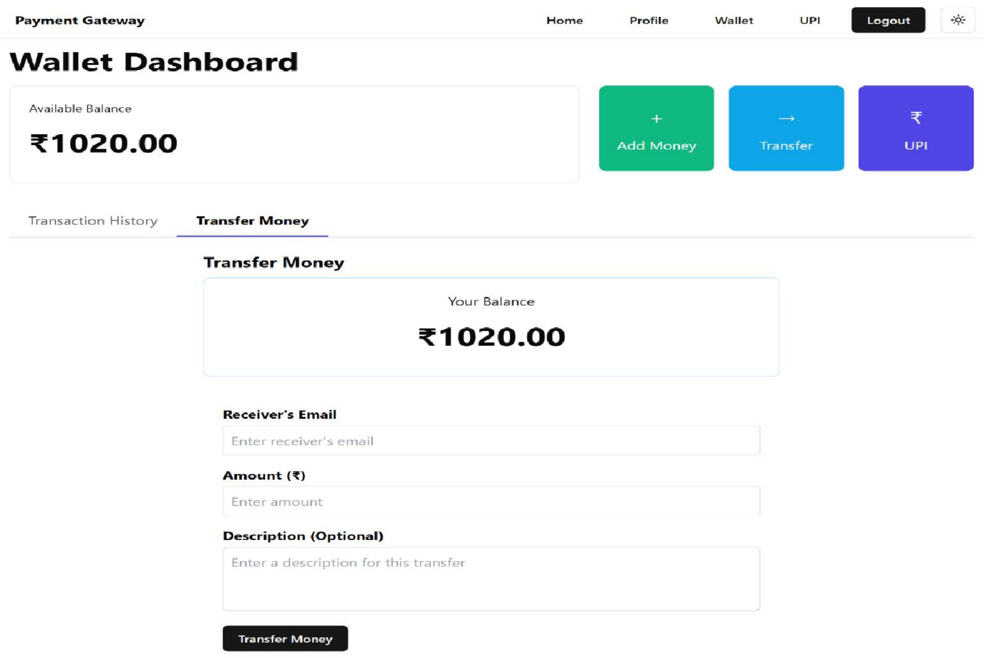
₹1020.00

Transaction History

Type: All Types
Status: All Statuses
Start Date: dd----yyyy
End Date: dd----yyyy

Transaction ID	Date	Type	Amount	Status	Details
TRX174611239154997c3be91	May 1, 2025, 08:43 PM	TRANSFER	₹10.00	COMPLETED	View
PAY17461111669458f72d806	May 1, 2025, 08:22 PM	DEPOSIT	₹10.00	COMPLETED	View
PAY174600244144375dbdd70	Apr 30, 2025, 02:10 PM	DEPOSIT	₹999.00	COMPLETED	View
PAY1745999998661c86c09ce	Apr 30, 2025, 01:29 PM	DEPOSIT	₹1.00	COMPLETED	View

Figure 1.3: Wallet Transaction History



Wallet Dashboard

Available Balance

₹1020.00

Transfer Money

Your Balance

₹1020.00

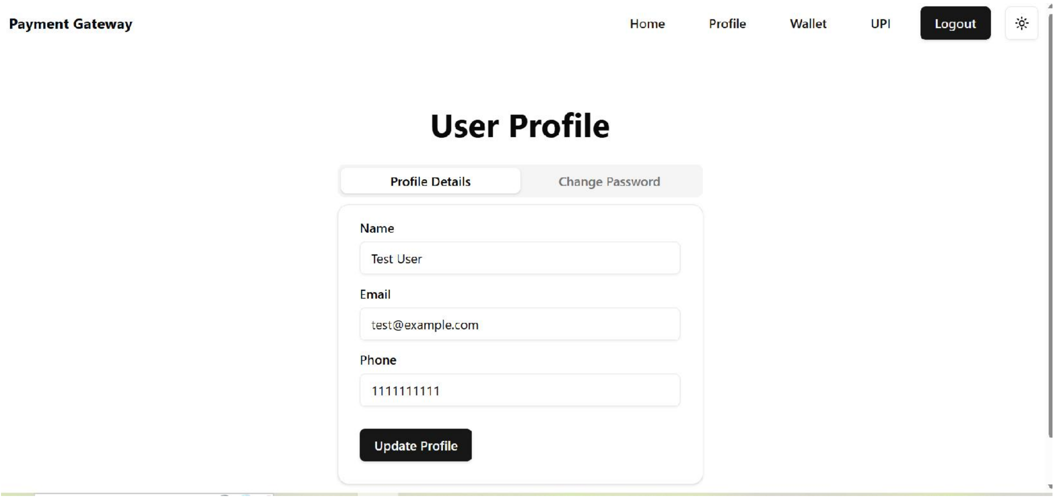
Receiver's Email: Enter receiver's email

Amount (₹): Enter amount

Description (Optional): Enter a description for this transfer

Figure 1.4: Wallet Transfer Money

DOI: 10.48175/IJARSCT-26039



Payment Gateway

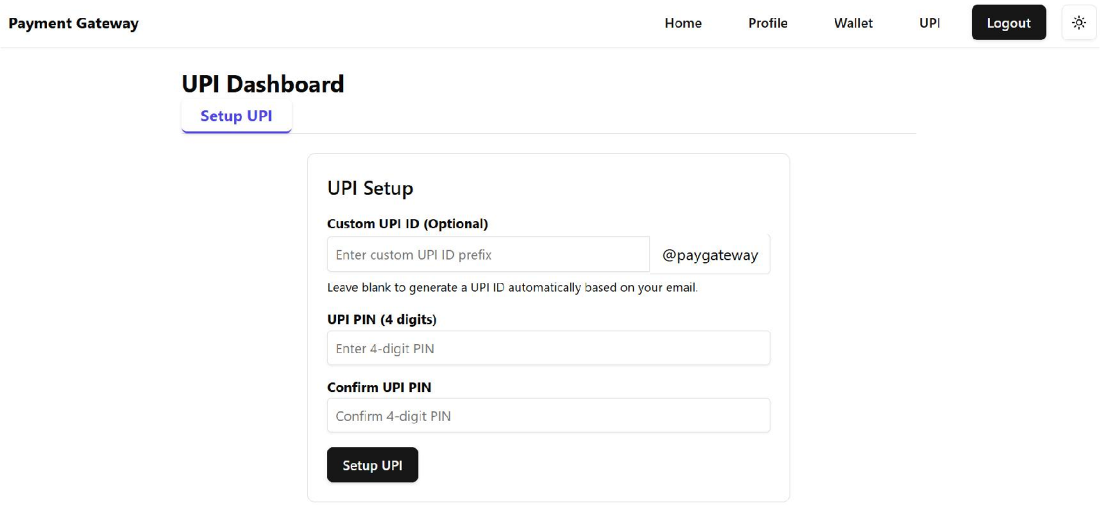
User Profile

Name: Test User

Email: test@example.com

Phone: 1111111111

Figure 1.5: Profile Page



Payment Gateway

UPI Dashboard

UPI Setup

Custom UPI ID (Optional): Enter custom UPI ID prefix @paygateway

Leave blank to generate a UPI ID automatically based on your email.

UPI PIN (4 digits): Enter 4-digit PIN

Confirm UPI PIN: Confirm 4-digit PIN

Figure 1.6: UPI Setup

DOI: 10.48175/IJARSCT-26039

IJARSCT

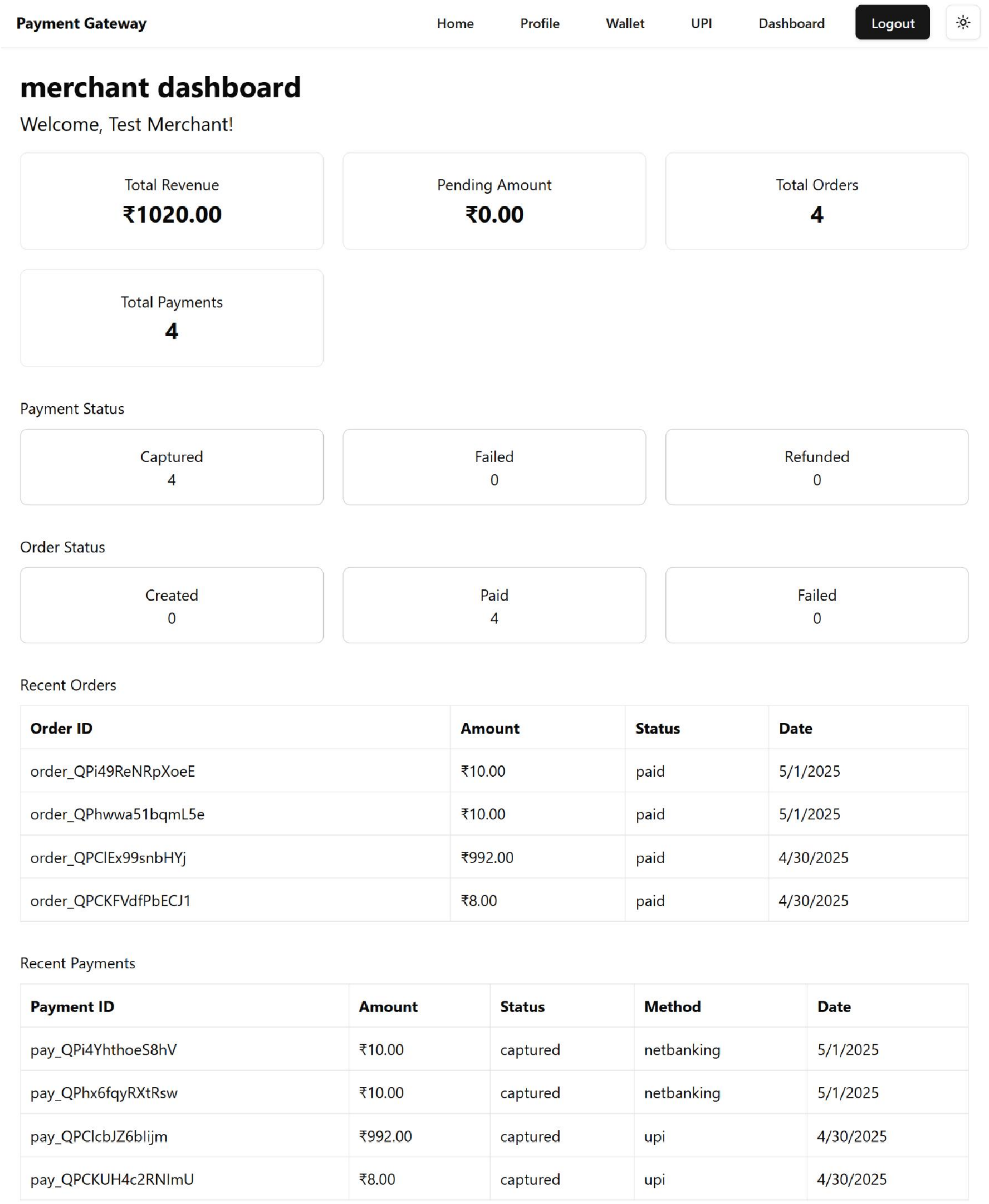
International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 13, April 2025

Impact Factor: 7.67



merchant dashboard

Welcome, Test Merchant!

Total Revenue ₹1020.00	Pending Amount ₹0.00	Total Orders 4
Total Payments 4		

Payment Status

Captured	Failed	Refunded
4	0	0

Order Status

Created	Paid	Failed
0	4	0

Recent Orders

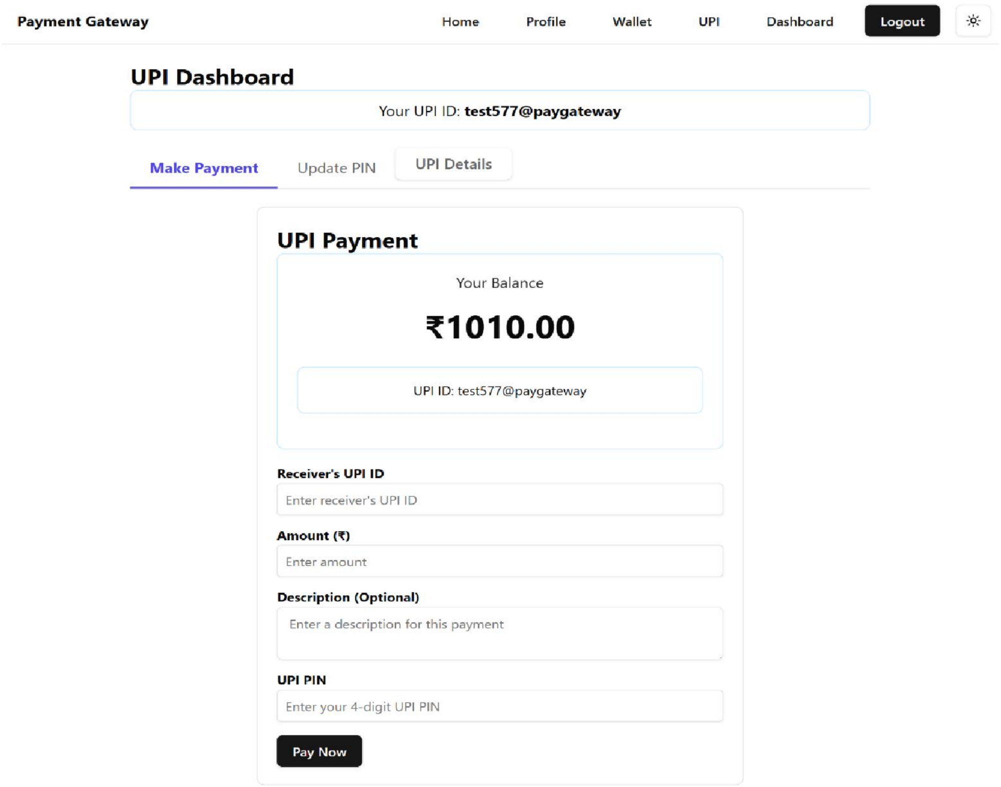
Order ID	Amount	Status	Date
order_QPi49ReNRpXoeE	₹10.00	paid	5/1/2025
order_QPhwwa51bqmL5e	₹10.00	paid	5/1/2025
order_QPClEx99snbHYj	₹992.00	paid	4/30/2025
order_QPCKFVdfPbECJ1	₹8.00	paid	4/30/2025

Recent Payments

Payment ID	Amount	Status	Method	Date
pay_QPi4YhthoeS8hV	₹10.00	captured	netbanking	5/1/2025
pay_QPhx6fqyRXtRsw	₹10.00	captured	netbanking	5/1/2025
pay_QPClcbJZ6blijm	₹992.00	captured	upi	4/30/2025
pay_QPCKUH4c2RNImU	₹8.00	captured	upi	4/30/2025

Figure 1.7: Dashboard

DOI: 10.48175/IJARSCT-26039



UPI Dashboard

Your UPI ID: **test577@paygateway**

UPI Payment

Your Balance

₹1010.00

UPI ID: test577@paygateway

Receiver's UPI ID

Enter receiver's UPI ID

Amount (₹)

Enter amount

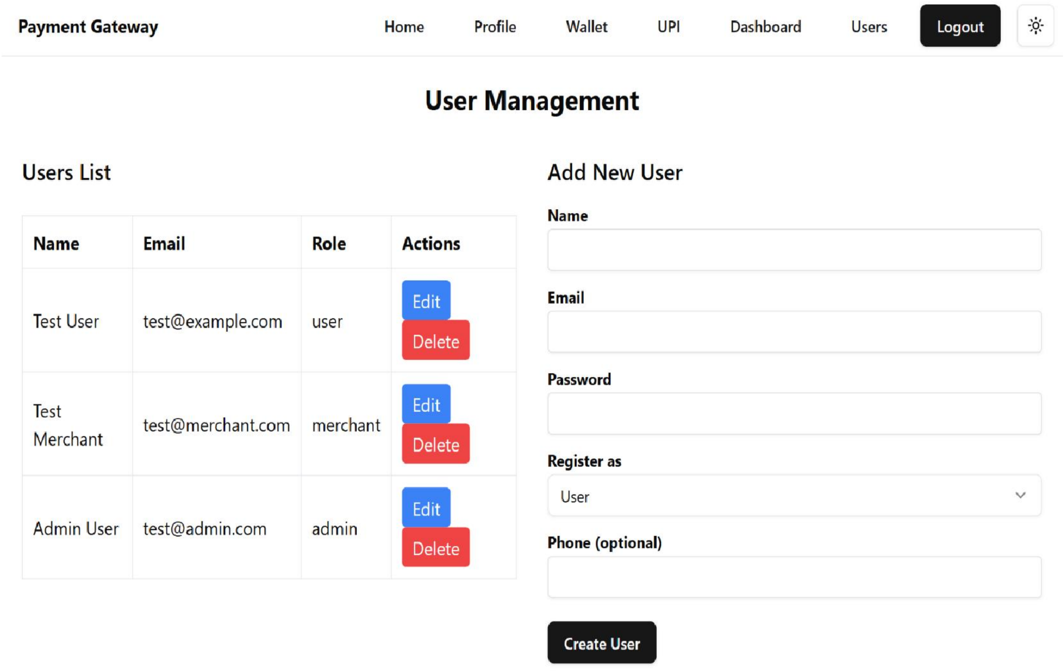
Description (Optional)

Enter a description for this payment

UPI PIN

Enter your 4-digit UPI PIN

Figure 1.8: UPI Dashboard



User Management

Users List

Name	Email	Role	Actions
Test User	test@example.com	user	Edit Delete
Test Merchant	test@merchant.com	merchant	Edit Delete
Admin User	test@admin.com	admin	Edit Delete

Add New User

Name

Email

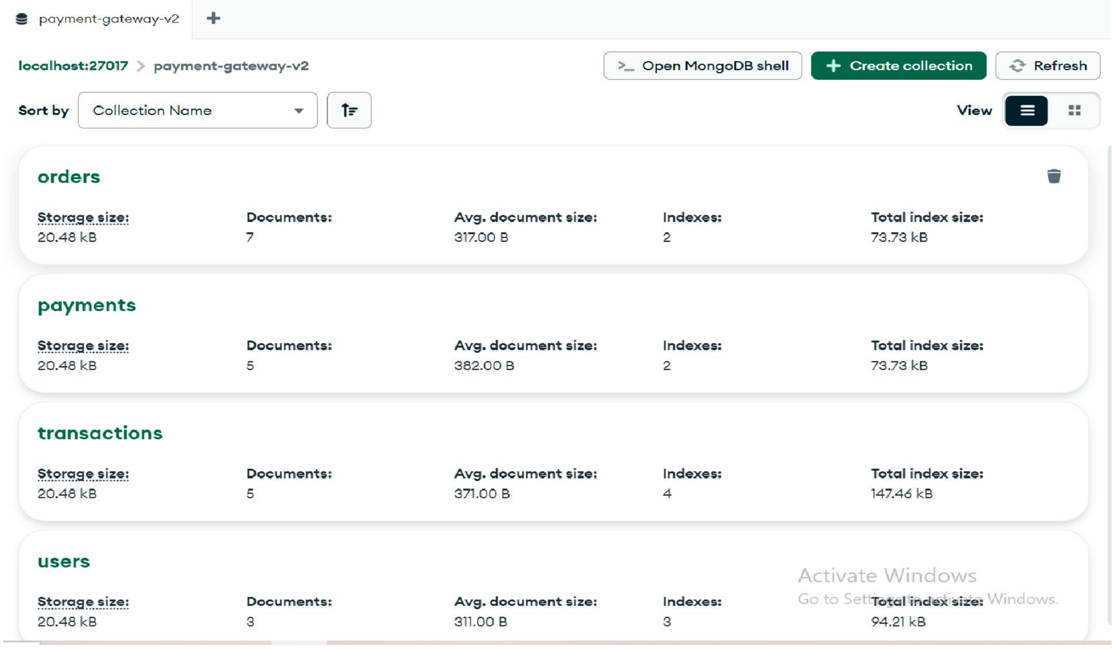
Password

Register as

User

Phone (optional)

Figure 1.8: Admin User Management



localhost:27017 > payment-gateway-v2

Sort by: Collection Name

	Storage size:	Documents:	Avg. document size:	Indexes:	Total index size:
orders	20.48 kB	7	317.00 B	2	73.73 kB
payments	20.48 kB	5	382.00 B	2	73.73 kB
transactions	20.48 kB	5	371.00 B	4	147.46 kB
users	20.48 kB	3	311.00 B	3	94.21 kB

Figure 1.6: Backend

XI. CONCLUSION

Integrating hybrid cryptography into payment gateways significantly enhances transaction security without compromising performance. The combination of AES for efficient data encryption and RSA for secure key exchange ensures data confidentiality and strengthens protection against common cyber threats.

The proposed system utilizes the Razorpay API for secure and seamless payment processing, along with MongoDB for encrypted data storage, providing a reliable foundation for modern digital transactions. Future improvements may include the integration of blockchain technology and the adoption of post-quantum cryptographic algorithms to further reinforce the system's security in an evolving digital landscape.

RFERENCES

[1] Samruddhi Sawant (2023), "A Study on the Digital Payment Gateways and its Future", INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT 07(04), http://dx.doi.org/10.55041/IJSREM18908

[2] Shivansh Thakur, Arpit Thakur (2021), "Payment Gateway App", The project report discusses the development of a Payment Gateway App. https://www.scribd.com/document/551873634/Payment-Gateway-App-Project-Report

[3] Rashi Singhal (2021), "IMPACT AND IMPORTANCE OF DIGITAL PAYMENT IN INDIA", SSRN Electronic Journal, http://dx.doi.org/10.2139/ssrn.3947792

[4] Paul Benjamin Lowry, Taylor Michael Wells, Gregory Daniel Moody, Sean Humphreys (2006), "Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management", Communications of the Association for Information Systems 17:1-48

[5] Lalita Malusare (2021), "Digital Payments Methods in India: A study of Problems and Prospects", International Journal of Scientific Research and Management Studies, https://www.researchgate.net/publication/349076488_Digital_Payments_Methods_in_India_A_study_of_Problems_and_Prospects

[6] S Sahayaselv (2017), "An Overview On Digital Payments", International Journal of Research 04(13):2101-2111, https://www.researchgate.net/publication/336835369_An_Overview_On_Digital_Payments

[7] Jaramillo, D., Nguyen, D. v, & Smart, R. (2016). Leveraging microservices architecture by using Docker technology. SoutheastCon 2016, 1–5. https://doi.org/10.1109/SECON.2016.7506647

[8] -Hong, X. J., Sik Yang, H., & Kim, Y. H. (2018). Performance Analysis of RESTful API and RabbitMQ for Microservice Web Application. 2018 International Conference on Information and Communication Technology Convergence (ICTC), 257–259. https://doi.org/10.1109/ICTC.2018.8539409

[9] D Bhagat (2020), "Digital Payments System in India and Its Scope in The Post-Pandemic Era.", IJIRT, 228 -240.

[10] Vally, K. S., & Divya, K. H. (2018). A Study on Digital Payments in India with Perspective of Consumer"s Adoption. International Journal of Pure and Applied Mathematics, 1259-1267

DOI: 10.48175/IJARSCT-26039