International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Digital Wallet with Dynamic Transaction Analytics

Julin Jose[1], Shyma Kareem[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *julinjose20[at]gmail.com*

[2]Associate Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***This project initiative delivers a highly secure and user - centric digital wallet platform integrated with smart transaction analytics. It simplifies personal finance management through a robust user authentication system, guaranteeing that only authenticated individuals can access its features. The platform is equipped to handle multi - currency transactions and supports fast, convenient transfers using either QR codes or mobile numbers, making it ideal for both domestic and cross - border payments. Users benefit from real - time transaction tracking and a rich history view that offers full transparency into their financial activity. A distinctive advantage of the system is its ability to evaluate previous transactions, helping users detect spending habits and set personalized financial targets. For enhanced control and security, the wallet allows users to set transaction limits, with instant alerts issued whenever those limits are breached. This innovative solution effectively merges ease of use with high - level security, providing a powerful tool for financial monitoring, budgeting, and goal setting.***

Keywords: Digital Wallet, Dynamic Transaction Analytics, Secure Platform, User - Friendly Interface, Verified User Registration, Authorized Access, Multi - Currency Transactions, QR Code Payments, Mobile Number Transfers, Domestic and International Transfers

1. Introduction

The mobile app starts with secure user registration and authentication, using privacy - preserving mechanisms and hashing algorithms to protect passwords and prevent unauthorized access. Once authenticated, users can initiate multi - currency transfers via wallets, bank accounts, QR codes, or phone numbers, with real - time exchange rates for better usability and trust. Transactions are encrypted with AES - 256, ensuring data security during processing. The app integrates with multiple payment gateways for seamless, real - time updates on transaction status.

Users can track transactions, view detailed history with filters, and receive real - time notifications on transaction progress, including updates on successful, failed, or pending transfers. Security features include transaction limits, monitoring, and fraud prevention. The app supports multi - currency transfers, with transparent exchange rates before confirmation, and allows users to customize settings, set limits, and link accounts.

On the admin web app, administrators log in securely with role - based access and multi - factor authentication. They can track transactions, investigate suspicious activity, and enforce security measures like transaction limits and regional restrictions. AES - 256 encryption ensures the security of transaction data. Admins can also manage real - time exchange rates, generate analytical reports, and configure system settings. This system ensures a smooth and secure experience for both users and administrators.

2. Related Works

Chaum (2022) explores the significance of privacy-preserving mechanisms in digital financial transactions, emphasizing the role of secure user authentication methods. The paper underscores the critical contribution of cryptographic techniques—particularly those aimed at safeguarding user credentials and transactional data—in strengthening both security and operational efficiency within digital financial ecosystems. Chaum highlights the potential of advanced encryption and authentication frameworks to reduce fraud, enhance user trust, and support the broader adoption of secure financial technologies in a privacy - sensitive environment [1].

Ng and Singh (2021) examine the functionality of multi - currency digital wallet platforms, emphasizing their capability to support seamless international transactions through real - time currency conversion. The study outlines the economic advantages of reduced transaction fees in comparison to conventional banking systems, which often impose higher costs and longer processing times. Furthermore, the authors highlight how these platforms contribute to financial inclusivity by enabling global freelancers and businesses to engage in cross - border transactions efficiently. Their support for real - time forex trading further enhances usability, allowing users to make informed financial decisions based on live exchange rates and market conditions [2].

Srivastava and Prakash (2021) explore the integration of artificial intelligence in fraud detection within digital banking ecosystems. Their study emphasizes the role of machine learning algorithms in identifying anomalies, recognizing transaction patterns, and conducting predictive analysis to flag potentially fraudulent activities. By leveraging real - time data processing, these AI systems can promptly detect irregularities and alert administrators or users, significantly minimizing financial risks. The paper also highlights the adaptability of AI models, which continuously learn from new data to improve detection accuracy over time, making them vital tools for modern digital security infrastructure [3].

Liu, Lu, and Zhu (2019) examine the impact of blockchain technology and smart contracts on enhancing the security and transparency of financial transactions. Their research outlines how decentralized ledgers eliminate single points of failure, making transaction records immutable and resistant to

tampering. Smart contracts further automate processes by executing predefined conditions without human intervention, reducing the risk of fraud and increasing operational efficiency. The authors emphasize the potential of these technologies to revolutionize financial platforms by fostering greater trust, improving traceability, and streamlining complex transactional workflows [4].

Roberts (2019) explores the growing adoption of QR code - based payment systems in emerging markets, emphasizing their low implementation cost and ease of use. The study illustrates how QR codes contribute to financial inclusion by enabling digital transactions in areas with minimal banking infrastructure. It also discusses challenges such as device compatibility, internet connectivity, and the need for user education. Furthermore, the paper addresses security concerns related to QR code spoofing and stresses the importance of encryption and authentication mechanisms to safeguard users against fraud and misuse [5].

Kahn and Roberds (2018) analyse the integration of real - time payment systems and their transformative effects on financial institutions. The study emphasizes improvements in transaction tracking, enabling immediate confirmation and settlement, which enhances transparency and reduces counterparty risk. It also highlights how real - time payments influence liquidity management by allowing institutions to make faster adjustments and minimize idle balances. Additionally, the authors discuss operational efficiencies gained through automation and the potential challenges of infrastructure upgrades and cybersecurity risks in real - time environments [6].

Rainer and Cegielski (2018) provide a comprehensive overview of how information systems support and transform modern business operations, focusing on the evolving financial technology (FinTech) landscape. The book explores how AI - driven analytics enhance decision - making by delivering predictive insights and identifying emerging trends in financial data. It also underscores the necessity of robust risk management frameworks to safeguard digital systems, ensuring data integrity, regulatory compliance, and resilience against cyber threats in increasingly digitized financial environments [7].

Reaves and Morris (2018) explore critical security and privacy features in financial mobile applications, emphasizing the role of real - time push notifications in strengthening user engagement and threat mitigation. The study finds that timely alerts on account activity—such as login attempts, large transactions, or unusual patterns—significantly enhance users' situational awareness. This proactive communication helps detect and prevent potential fraud or unauthorized access, reinforcing the overall security posture of financial mobile apps [8].

Yang and Zhang (2015) analyse the logistics and payment framework of cross - border e - commerce through a case study of Alibaba's Alipay. The paper highlights Alipay's innovative integration of multi - currency support and real - time exchange rate features, which streamline international transactions and enhance user experience for global consumers. It also examines the platform's ability to address common challenges in cross - border trade, such as currency conversion, payment delays, and regulatory compliance [9].
Schneier (2015) offers a comprehensive examination of essential encryption techniques such as AES - 256 and hashing, emphasizing their importance in protecting user information and verifying identities in digital finance. This work acts as a practical manual for designing secure communication mechanisms in software, serving as a valuable reference for developers and security experts [10].
Chandramouli (2014) presents a comprehensive explanation of Role - Based Access Control (RBAC), emphasizing how permission - based system configuration enhances administrative control and minimizes security vulnerabilities. The paper, published by NIST, supports secure and efficient system management through clearly defined access privileges, ensuring operational consistency and regulatory compliance [11].

Zhou (2013) explores the psychological factors behind initial trust in mobile payment platforms, identifying transparency in transaction history and the provision of real - time updates as key drivers of user engagement. The research suggests that enhancing visibility into payment processes builds credibility and encourages user adoption in digital finance ecosystems [12].

Contini et al. (2011) analyse the security landscape of mobile payment systems in the U. S., emphasizing the critical role of fraud detection mechanisms and robust encryption standards like AES - 256. The paper underscores the importance of proactive mobile security strategies to protect sensitive financial data and ensure transactional integrity [13].

Florêncio and Herley (2007) conducted a large - scale empirical study on web user password habits, revealing widespread issues in password strength and reuse. Their findings reinforce the importance of secure password storage practices, including hashing algorithms, as a defence against credential theft in digital financial systems [14].

Ghosh and Swaminatha (2001) examine the security and privacy risks associated with mobile commerce platforms. They emphasize the need for continuous fraud detection, real - time monitoring, and secure architecture to preserve user trust and ensure data protection in evolving digital ecosystems [15].

3. Outlined Method

The methodology delineates the framework for designing and executing a comprehensive system for a digital wallet with dynamic transaction analytics. This methodology encompasses the following essential components:

a) Requirement Gathering and Analysis:
Input from users and market analysis has highlighted the need for a secure and feature - rich digital wallet system that supports seamless financial transactions and insightful money management. The system will include core functionalities such as user registration, multi - currency transaction support, real - time transaction tracking, and personalized financial insights. To ensure clarity and security in operations, role - based access will be implemented, with administrators

managing the system via a web application and users accessing their accounts through a mobile app. Security measure such as OTP authentication, transaction limits, and end - to - end data encryption will be integrated to protect user data and ensure safe, trustworthy transactions.

b) System design and Architecture:
The system architecture will involve frontend development with a Web App (Admin) using HTML, CSS, Bootstrap, and JavaScript (AJAX, jQuery), and a Mobile App (Users) built with Flutter (Dart), while the backend will utilize PHP for REST API communication with the mobile app and MySQL as a centralized database for both web and mobile apps, ensuring secure transactions through encryption, with a scalable database schema to efficiently handle financial transactions and user data.

c) Development and Implementation:
The project will follow an iterative approach, with the backend developed using PHP and MySQL to provide REST APIs for user authentication, multi - currency transactions, tracking, and analytics. Security features like transaction limits and fraud detection will be integrated. The frontend will include a responsive admin panel using Bootstrap and AJAX, and a user - friendly mobile app built with Flutter and Dart. To ensure data safety, the system will implement AES encryption, secure authentication, and fraud monitoring.

d) Testing and Quality assurance:
Testing will cover unit testing for both the PHP backend and Flutter app components, along with API validation using Postman to ensure the proper functioning of REST endpoints. Security testing will be conducted to guard against threats like SQL injection and CSRF attacks. Additionally, load testing will verify that the system can manage high traffic during peak transaction periods.

e) Deployment:
After successful testing, the platform will be deployed with the web app and APIs hosted on a secure server. An AWS EC2 instance running an Ubuntu - based private server with Nginx will be used to ensure high performance, reliability, and enhanced security.

f) Monitoring and Maintenance:
The platform will receive regular updates to apply security patches and introduce feature enhancements, ensuring ongoing reliability and improved user experience.

3.1 Advanced Encryption Standard – 256 (AES - 256)

AES - 256 (Advanced Encryption Standard - 256 - bit) is a symmetric encryption algorithm used for securing sensitive data. It is widely used in banking, government, and security communication systems. AES algorithm is using this project ideas based on various purposes [10].

When someone sets up an account, their password goes through encryption with Bcrypt, a trustworthy hashing system that adds a special salt to each password. This approach ensures that even the same passwords end up with different hashes. The system never keeps the actual password—it stores the hashed version in the database. When users log in, the system hashes the password they type and compares it to the stored hash. If they're the same, the login works. This method offers strong safeguards for user information making it tough for hackers to figure out original passwords even if they break into the database.

When someone signs up, the system turns their password into a jumbled code using safe methods. This code gets saved in the database. During sign - in, the system scrambles the typed password and checks if it matches the saved code. If they're the same, the user can get in. If not, they can't log in.

When a user initiates a transaction, sensitive data is encrypted using AES - 256 and stored in the database. When required, the system decrypts the transaction using the AES - 256 key, allowing users to securely view their transaction details.

The system first checks if the encrypted data from the database is valid. Next, it pulls out the initialization vector (IV) and the encrypted information. Using the secret key and IV, it unlocks the original data. After decryption, the system shows the transaction details in a secure way. This lets users see their sensitive information without risk.

4. Result & Discussion

Businesses under the Digital Wallet System offer advanced financial management capabilities alongside transaction monitoring and security features in transformed wallet systems. The platform enhances bank operations through goal - based financial tracking which pairs with categorized expense evaluation and progress tracking tools for improved financial structure. Users benefit from real - time transaction verification together with fraud detection and anomaly alert functions which help the system prevent potential threats in their transactions. Users gain better financial control by observing complete analytics along with visualization tools to create wiser spending choices. Effective global money transfer becomes accessible through the system which links straightforwardly with banks' credit cards and payment gateways in addition to its capability to support multiple currencies. The system design supports evolving regulations and APIs as well as security standards through adaptive features that benefit from proactive maintenance to deliver high reliability. The platform achieves a new financial benchmark through its administrator controls fraud prevention technology and user - centred functionality to deliver an adaptable secure interface.

5. Conclusion

The Digital Wallet with Dynamic Transaction Analytics serves as a secure and all - in - one financial management tool, tailored to improve user convenience while optimizing financial control. By incorporating essential features such as secure registration, support for multiple currencies, real - time transaction monitoring, and insightful analytics, it empowers users to make informed financial choices. The inclusion of customizable transaction limits and instant alerts strengthens account security, while intelligent analysis of spending patterns helps users stay on track with their financial goals. Altogether, this solution offers a seamless blend of usability,

insight, and protection—making it a reliable companion for managing personal finances in today's digital era.

References

[1] Privacy - Preserving Digital Transactions: Security and Efficiency in the Financial Ecosystem by D. Chaum (2022)
[2] Multi - Currency Transaction Platforms by D. Ng & A. Singh (2021)
[3] AI - Driven Fraud Detection in Digital Banking by S. Srivastava & S. Prakash (2021)
[4] Blockchain Technology and Smart Contracts for Secure Financial Transactions by Q. Liu, Y. Lu & X. Zhu (2019)
[5] Adoption of QR Code Payments in Emerging Markets by M. Roberts (2019)
[6] Real - Time Payments and Their Impact on Financial Institutions by C. M. Kahn & W. Roberds (2018)
[7] Introduction to Information Systems: Supporting and Transforming Business by R. K. Rainer & C. G. Cegielski (2018)
[8] Security and Privacy Enhancements for Financial Mobile Applications by B. Reaves & T. Morris (2018)
[9] Cross - Border E - Commerce Logistics and Payment: A Case Study of Alibaba's Alipay by S. Yang & Y. Zhang (2015)
[10] Applied Cryptography: Protocols, Algorithms, and Source Code in C by B. Schneier (2015)
[11] Role - Based Access Control by R. Chandramouli (2014)
[12] An Empirical Examination of Initial Trust in Mobile Payment by T. Zhou (2013)
[13] Mobile Payments in the United States: Mapping Out the Road Ahead by D. Contini, M. Crowe, C. Merritt, K. Oliver & S. Mott (2011)
[14] A Large - Scale Study of Web Password Habits by D. Florêncio & C. Herley (2007)
[15] Software Security and Privacy Risks in Mobile Commerce by A. K. Ghosh & T. M. Swaminatha (2001)