International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1(s) (2026)



ijerst.editor@gmail.com

editor@ijerst.com

www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Implementation of a Digital Daily Pass and E-Ticketing Mobile Application for Local Public Transport

Wathore Shivaji [1], Prof. M. A. Wakchaure [2]
Amrutvahini College of Engineering, Sangamner A/P-Ghulewadi-422608, Tal. Sangamner, Dist. Ahilyanagar

***Abstract*— The current public transportation system primarily relies on traditional paper-based ticketing and manual fare collection methods, which lead to operational inefficiencies, revenue leakage, increased boarding time, and inconvenience for passengers and transport authorities. This dissertation presents the design and implementation of a Digital Daily Pass and E-Ticketing Mobile Application aimed at modernizing local public transport fare management. The proposed system replaces conventional ticketing with a secure, mobile-first solution that enables instant purchase, digital storage, and real-time validation of single-journey e-tickets and digital daily passes.**

The system follows a three-tier architecture consisting of a customer mobile application, a conductor mobile validation application, and a cloud-based backend infrastructure. A key security feature of the system is the use of dynamic QR codes generated using a Time-Based One-Time Password (TOTP) mechanism. This ensures that each digital pass produces a time-sensitive encrypted token, preventing screenshot fraud and unauthorized sharing. The conductor application validates tickets in real-time through a secure Validation API, ensuring that responses are delivered within a minimal time frame to reduce passenger dwell time.

The backend infrastructure manages transaction processing, pass generation, audit logging, and real-time reporting for administrative oversight. The system enhances operational transparency, reduces paper waste, eliminates cash handling complexities, and enables data-driven decision-making through accurate transaction records. By integrating mobile technology, secure tokenization, and scalable cloud architecture, the proposed solution contributes to improved efficiency, enhanced passenger convenience, reduced fraud, and the advancement of smart, sustainable public transportation systems.

Keywords: Digital Daily Pass, E-Ticketing System, Mobile Application, Public Transport, Dynamic QR Code, TOTP, Validation API, Cloud Architecture, Secure Payment Gateway, Fraud Prevention, Real-time Validation, Microservices, Operational Transparency, Smart Mobility, Sustainable Transport.

I. INTRODUCTION

The digitization of public services has become a global priority, and public transportation systems stand to benefit significantly from modernization. Traditional fare collection methods in local public transport systems primarily rely on paper tickets, manual cash handling, and static pass mechanisms. These conventional approaches introduce several operational challenges, including revenue leakage, fraud vulnerability, extended passenger boarding time, and lack of real-time data availability. Such inefficiencies negatively impact both commuters and transport authorities.

This project focuses on the design and implementation of a Digital Daily Pass and E-Ticketing Mobile Application to address these challenges. The proposed system leverages mobile technology and cloud-based infrastructure to create a secure, efficient, and user-friendly digital ticketing platform. The solution enables passengers to purchase single-journey e-tickets and digital daily passes directly through a mobile application. Upon successful payment, a secure digital pass is generated and displayed using a dynamic QR code.

A key innovation of the system is the use of a Time-Based One-Time Password (TOTP) mechanism to generate time-sensitive QR tokens. These dynamically changing codes prevent screenshot fraud and unauthorized sharing of passes. The conductor application scans and validates tickets in real time through a secure Validation API, ensuring minimal validation delay and improved passenger flow.

The system follows a three-tier architecture consisting of a presentation layer (mobile apps and admin portal), an application layer (validation and pass generation services), and a data layer (SQL/NoSQL database). By eliminating paper-based processes and introducing secure digital validation, the proposed solution enhances operational efficiency, reduces fraud, improves customer convenience, and supports data-driven decision-making for smarter public transport management.

II. RELATED WORK

Existing research highlights the importance of digital

transformation in public transportation systems as a key component of Smart City initiatives. Studies on Intelligent Transportation Systems (ITS) emphasize that traditional paper-based ticketing systems fail to provide real-time, granular data necessary for demand-responsive transit planning. Researchers have identified that digital fare collection systems enable improved operational transparency, optimized route planning, and better resource allocation.

The concept of Mobility-as-a-Service (MaaS) has further influenced the development of mobile ticketing platforms. MaaS integrates multiple transportation services into a unified digital interface, allowing users to book and pay through a single application. Literature suggests that Level 2 MaaS integration, which focuses on unified booking and payment systems, requires account-based ticketing platforms where fare media is independent of physical cards. Mobile-based digital passes align directly with this framework by enabling smartphone-based ticket storage and validation.

Several studies compare QR code and NFC-based ticket validation technologies. QR code systems are recognized for their low infrastructure cost and ease of deployment, requiring only camera-equipped devices for scanning. However, static QR codes pose security risks due to screenshot fraud. To address this, researchers recommend dynamic, time-sensitive QR codes using Time-Based One-Time Password (TOTP) mechanisms. NFC and Host Card Emulation (HCE) technologies provide faster validation speeds but require specialized hardware and higher infrastructure investment.

Security-focused literature emphasizes tokenization, server-side verification, encryption protocols (HTTPS/TLS), and real-time validation APIs as essential components of secure e-ticketing systems. Additionally, microservices-based architectures are recommended for scalability, high availability, and efficient transaction handling in high-volume public transport environments.

Despite extensive research on individual components, limited work integrates dynamic QR security, real-time validation, and scalable cloud architecture into a unified mobile ticketing solution for local public transport, which this project aims to address.

III. BACKGROUND

Public transportation systems traditionally rely on manual, paper-based ticketing methods and cash transactions for fare collection. While these systems have been functional for decades, they present significant operational and financial limitations. Manual ticket issuance increases passenger boarding time, contributes to longer vehicle dwell time at stops, and creates bottlenecks during peak hours. Additionally, cash handling introduces risks related to revenue leakage, fraud, reconciliation delays, and administrative overhead.

With the advancement of digital technology and the widespread adoption of smartphones, transport authorities worldwide are transitioning toward digital fare collection systems. The evolution of Smart Cities and Intelligent Transportation Systems (ITS) emphasizes the need for real-time data collection, operational transparency, and sustainable mobility solutions. Traditional ticketing systems fail to provide granular, real-time transaction data, making route optimization and demand-responsive planning difficult.

The concept of Mobility-as-a-Service (MaaS) further strengthens the need for integrated digital ticketing platforms. MaaS promotes unified booking and payment systems through mobile applications, enabling seamless travel experiences. In this context, account-based ticketing systems, where tickets are stored digitally rather than on physical media, have gained prominence.

Security remains a major concern in digital ticketing. Static digital tickets are vulnerable to duplication and screenshot fraud. To mitigate this, modern systems adopt tokenization techniques and dynamic QR codes generated through Time-Based One-Time Password (TOTP) mechanisms. These time-sensitive tokens ensure secure validation and prevent unauthorized sharing.

Cloud computing and microservices architecture have enabled scalable, high-performance backend systems capable of handling high transaction volumes with low latency. These technological advancements provide the foundation for implementing a secure, efficient, and data-driven Digital Daily Pass and E-Ticketing system for local public transport.

IV. CHALLENGES IN THE FOUNDER JOURNEY

The journey of developing and implementing the Digital Daily Pass and E-Ticketing Mobile Application involves multiple technical, operational, and strategic challenges. As identified throughout the project

desertation 2 shiva

, building a secure and scalable digital fare collection system requires careful planning, risk management, and continuous adaptation.

One of the primary challenges is **ensuring system security and fraud prevention**. Traditional paper tickets are vulnerable to counterfeiting, while digital tickets risk screenshot sharing. Implementing dynamic QR codes using a Time-Based One-Time Password (TOTP) mechanism requires strong cryptographic design and accurate time synchronization between client and server. Any security flaw could result in revenue leakage and loss of trust.

Another major challenge is **achieving high-performance validation**. The system must process ticket validation in under three seconds, even during peak hours with high

concurrent usage. This requires optimized database queries, caching mechanisms, scalable cloud infrastructure, and efficient API design. Maintaining low latency while handling large transaction volumes is technically demanding.

Network dependency and offline validation also pose difficulties. Conductors may operate in areas with unstable internet connectivity. Designing an offline validation mode that securely verifies tickets while maintaining data integrity adds architectural complexity.

Payment gateway integration introduces additional challenges such as transaction failures, secure encryption, and compliance considerations. Ensuring smooth user experience during payment processing is critical for adoption.

User acceptance and adoption represent non-technical challenges. The application must be intuitive for passengers and conductors with varying levels of digital literacy. Resistance to change from traditional systems can slow implementation.

Finally, resource constraints such as development time, team coordination under Agile methodology, testing requirements, and risk mitigation add pressure to the founder journey. Successfully overcoming these challenges ensures a secure, efficient, and sustainable digital ticketing solution.

V. FRAMEWORK AND DESIGN PRINCIPLES

The The Digital Daily Pass and E-Ticketing System is designed using a structured architectural framework and well-defined software engineering principles to ensure scalability, security, performance, and usability.

A. Architectural Framework

The system follows a **Three-Tier Architecture**, ensuring modularity and separation of concerns:

1. **Presentation Tier (Client Layer):** Includes the Passenger Mobile Application, Conductor Mobile Application, and Administrator Web Portal. This layer is responsible for user interaction, ticket purchase, QR code display, and validation feedback.
2. **Application Tier (Business Logic Layer):** Implements core services such as Pass Generation Service, Validation API, Payment Gateway Integration, and Logging & Reporting Services. A microservices-based approach is adopted to allow independent scaling of critical components like validation and payment processing.
3. **Data Tier:** Utilizes SQL/NoSQL databases (e.g., PostgreSQL or MongoDB) to store user profiles, pass records, transaction logs, and audit data securely.

The Agile/Scrum methodology is used for development to enable iterative improvements, rapid testing, and early feedback integration.

B. Design Principles

The system is developed based on the following key design principles:

- **Security by Design:** Dynamic QR codes generated using TOTP ensure time-sensitive token validation, preventing fraud and screenshot sharing. End-to-end encryption (HTTPS/TLS) protects data in transit.
- **Scalability:** Microservices architecture supports horizontal scaling to handle increasing transaction volumes.
- **High Availability & Reliability:** Cloud-based deployment ensures minimal downtime and consistent performance.
- **Performance Optimization:** Validation responses are designed to occur within 3 seconds to reduce passenger dwell time.
- **Usability & Accessibility:** Simple, intuitive UI for passengers and high-contrast scanning interface for conductors improve adoption.
- **Modularity & Maintainability:** Independent services enable easy updates, bug fixes, and future feature expansion.

These framework and design principles ensure a robust, secure, and future-ready digital ticketing solution.

VI. REFERENCE SYSTEM ARCHITECTURE

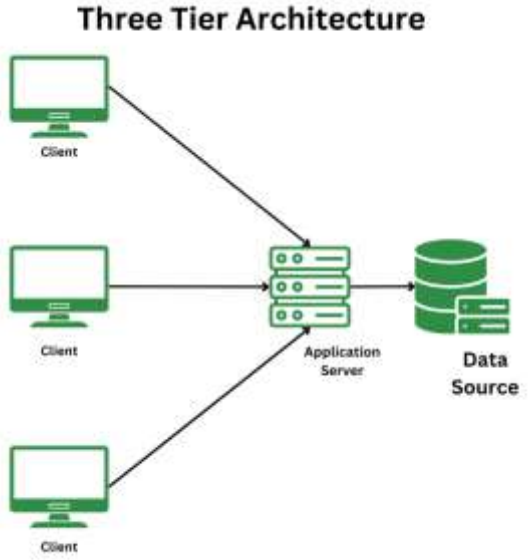


Fig 1: REFERENCE SYSTEM ARCHITECTURE

The Digital Daily Pass and E-Ticketing System is built on a structured and scalable **Reference System Architecture** designed to ensure security, performance, and modularity desertation 2 shiva

. The architecture follows a **Three-Tier Model** combined with a microservices-based backend to support high transaction volumes and real-time validation.

1. Overall Architectural Structure

The system consists of three primary layers:

A. Presentation Tier (Client Layer)

This layer includes:

- **Passenger Mobile Application** – Used for registration, ticket/pass purchase, payment processing, and displaying dynamic QR codes.
- **Conductor Mobile Application** – Used for scanning and validating QR codes in real time.
- **Administrator Web Portal** – Used for fare management, user management, monitoring transactions, and generating reports.

This layer handles all user interactions and communicates securely with backend APIs.

B. Application Tier (Business Logic Layer)

This layer contains core microservices responsible for:

- **Validation API** – Verifies dynamic QR tokens in real time.
- **Pass Generation Service** – Generates unique Pass IDs and encrypted tokens.
- **Payment Gateway Service** – Handles secure digital transactions.
- **Logging & Reporting Service** – Maintains audit logs and analytics.

The backend processes validation requests within a targeted time limit (under 3 seconds) to ensure minimal passenger dwell time.

C. Data Tier

The data layer includes:

- **Relational Database (PostgreSQL)** – Stores user data, pass records, and transaction logs.
- **Optional NoSQL Database** – Manages high-volume validation logs for real-time analytics.

2. Security Architecture

The system uses:

- Time-Based One-Time Password (TOTP) for dynamic QR generation
- Server-side token verification
- HTTPS/TLS encryption
- Role-Based Access Control (RBAC)

3. Deployment Model

The architecture is cloud-based, enabling horizontal scalability, high availability, and performance optimization.

This reference architecture ensures a secure, scalable, and high-performance digital ticketing platform suitable for modern public transport systems.

VII. REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1666–1689, 2016.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1654–1682, 2020.

[4] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[5] H. F. Atlam, A. Alenezi, and G. B. Wills, “Blockchain with Internet of Things: Benefits, Challenges, and Future Directions,” International Journal of Intelligent Systems and Applications, vol. 10, no. 6, pp. 40–48, 2018.

[6] X. Liang, S. Shetty, D. Bowden, J. Liu, and D. Li, “Towards Decentralized Accountability and Self-Sovereignty in IoT Systems,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3016–3025, 2018.

[7] H. Tian, M. Dong, J. Wu, and J. Li, “Secure and Scalable IoT Data Access Control Using Blockchain-Based Capability Tokens,” IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8754–8767, 2020.

[8] R. Kumar and P. Goyal, “Blockchain-Based IoT Security: A Comprehensive Survey,” IEEE Access, vol. 8, pp. 117134–117153, 2020.

[9] Y. Zhang, J. Wen, and X. Xu, “Smart Contract-Based Access Control for IoT Systems Using Blockchain,” IEEE Access, vol. 8, pp. 155779–155791, 2020.

[10] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things,” Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.

[11] M. Banerjee, J. Lee, and K. Choo, “Blockchain-Based Secure Device Management Framework in IoT,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2179–2190, 2021.

[12] P. K. Sharma and S. Y. Moon, “Message Authentication and Route Security in IoT Using Blockchain Technology,” IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3163–3170, 2019.

[13] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in Proc. IEEE Security and Privacy Workshops, pp. 180–184, 2015.

[14] A. Sharma, M. Tiwari, and S. Kumar, “Decentralized

Access Control and Data Security in IoT Using Blockchain and Smart Contracts," Journal of Network and Computer Applications, vol. 180, 2021.
[15] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979–33001, 2018.
[16] S. Malik, P. Dutta, and S. K. Singh, "Blockchain-Based Authentication and Trust Management in IoT: A Systematic Review," Computer Networks, vol. 190, 2021.
[17] S. Cha, J. Park, and S. Kim, "IoT Security Enhancement Using Blockchain Technology," Sensors, vol. 21, no. 10, p. 3491, 2021.
[18] M. Samaniego and R. Deters, "Hosting Virtual IoT Resources on Edge-Hosts with Blockchain," in Proc. IEEE Int. Conf. Edge Computing, pp. 43–50, 2016.
[19] S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," in Proc. IEEE Symposium on Cloud Computing, 2016.
[20] J. Kang, R. Yu, X. Huang, M. Wu, and S. Maharjan, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660–4670, 2019.