

A Smart QR Code-Based Bus Pass Verification System

Sahil Rajendra Ghadi¹, Akshay Sanjay Satam², Satish R. Kasale³, Gaurish L. Thakur⁴

^{1,2} Student, Department of Bachelor in Computer Applications, Dnyankunj College of Information Technology & Management, Maharashtra, India

^{3,4} Asst. Professor, Department of Bachelor in Computer Applications, Dnyankunj College of Information Technology & Management, Maharashtra, India

DOI: 10.5281/zenodo.20630584

ABSTRACT

The verification of student bus passes is currently undergoing a significant transition from manual, paper-based methods to automated digital systems. Historically, the relationship between transport management and student identification relied on physical identity cards and manual visual checks, which were prone to human error, loss, and fraudulent sharing. This paper presents a Smart Online QR Code-Based Bus Pass Verification System, an intelligent solution developed to bridge the security gap in modern transport infrastructure.

Unlike traditional systems where physical cards can be passed from person to person, this system utilizes a dynamic digital QR link that serves as a non-transferable credential. The core innovation lies in the real-time synchronization with an online database. When a QR code is scanned, the conductor's terminal instantly populates a visual verification table containing the student's photograph and registration details. This prevents unauthorized travel by ensuring that the person boarding matches the authorized profile on the screen. The research outlines the software architecture, the importance of real-time data retrieval, and the operational effectiveness of visual identification in high-traffic settings. Early results indicate that this online validation method significantly improves boarding efficiency while maintaining high security without the need for expensive or complex biometric hardware.

Keywords: Smart Bus Pass, QR Code Verification, Online Authentication, Visual Identity Match, Student Transport Security.

1. INTRODUCTION

The Smart QR Code-Based Bus Pass is a digital security platform built to modernize and improve how educational institutions and transport authorities manage student commuting. In the field of public and institutional security, authentication technology has grown past being just a simple scanning tool; it now works as an active, independent security layer capable of spotting unauthorized access attempts in real-time.

Modern transportation systems face a critical challenge: the misuse of student passes by non-students or unauthorized travelers. Physical cards are easily shared, and manual inspection is often too slow to be effective in high-density urban settings. Furthermore, traditional biometric solutions like fingerprint scanners often fail due to hardware maintenance issues or hygiene concerns. To address these limitations, our system introduces a real-time, online verification process that leverages the ubiquity of smartphones and mobile data.

When a student boards, they present a unique QR code generated through a secure mobile application. This code is linked to a centralized administrative database that stores the student's identity and pass validity. The paradigm shift here is moving from "possession-based" security (holding a card) to "identity-based" security (visual confirmation). By focusing on a "Photo-ID Table" display for conductors, the system ensures a human-in-the-loop security model. This approach ensures that transport subsidies are protected and used only by the rightful student population, thereby improving revenue transparency and operational efficiency.

2. PROBLEM STATEMENT

The current student bus pass system lacks a real-time, secure, and automated verification mechanism. Students experience long waiting times for pass issuance, while conductors cannot reliably verify pass validity or detect repeated usage. Physical passes are vulnerable to misuse and sharing, as they can be used by anyone who holds the card. There is a critical need for a digital solution that ensures instant verification, prevents fraud via visual identification, and improves the overall efficiency of student transportation services.

3. PROPOSED SYSTEM

The proposed system introduces a Smart Bus Pass Verification Terminal operated by the bus conductor. Each student is issued a digital bus pass containing a unique QR code, linked to their profile and high-resolution photograph stored in a centralized database.

3.1. System Components:

- **QR Code Generator:** A mobile app that creates a time-sensitive, encrypted code.
- **Verification Terminal:** A handheld or fixed device with a camera and internet connectivity.
- **Centralized Online Database:** Stores student profiles, photos, and subscription status.
- **Visual Verification Interface:** A specialized UI that displays student data in a table format.

4. SECURITY NOTE: PROTECTING SYSTEM INTEGRITY

The transition from biometric-based hardware to a QR-centric visual verification model necessitates a robust multi-layered security framework to prevent fraud and unauthorized travel. The security of this system is maintained through the following three pillars:

4.1. Dynamic Qr code encryption (anti-cloning)

To prevent students from taking screenshots of their QR codes and sharing them with non-students, the system utilizes Dynamic Generation.

- **Time-to-Live (TTL):** Each QR code is embedded with a timestamp and a unique session token that expires after a short duration (e.g., 60 seconds).
- **Encryption:** The data within the QR is hashed using AES-256 encryption, ensuring that even if intercepted, the raw data cannot be altered to extend the pass validity manually.

4.2. The Visual Verification "Human-in-the-Loop" Model

Since a digital code can technically be displayed on any screen, the primary defense against pass-sharing is the Conductor's Verification Table.

- **Server-Side Photo Retrieval:** Upon scanning, the photo is not pulled from the phone (which could be faked) but is fetched directly from the Centralized Secure Database.
- **Visual Match:** The conductor acts as a physical security layer, matching the passenger's face to the high-resolution photo displayed on the terminal. This makes the pass "visually non-transferable."

4.3. Real-time fraud detection & anti-pass

The system implements Anti-Pass logic via the online cloud server:

- **Duplicate Scan Alerts:** If a specific Student ID is scanned twice within a short timeframe on different bus routes or the same bus, the system triggers a "Fraud Alert" on the conductor's device.
- **Account Locking:** Frequent attempts to use the same QR code across multiple devices can lead to the temporary suspension of the student's digital pass, pending institutional review.

4.4. Data Privacy and Encryption

Student data, including photographs and personal identification, is stored using Hashed Credentials. All communication between the mobile app, the conductor terminal, and the backend server is conducted over HTTPS/TLS 1.3 encrypted tunnels, protecting student privacy against "Man-in-the-Middle" (MITM) attacks.

5. FINAL OBJECTIVE: ENHANCING SECURITY AND EFFICIENCY

5.1. Eliminate Fraud & Identity Assurance

Our primary goal is to ensure that only the legitimate, registered student can utilize the bus pass. By integrating Biometric Authentication (Fingerprint/Iris) and RFID Encryption, we create an unbreakable link between the digital pass and its authorized user. This eliminates several common fraud vectors:

- **Eradication of Pass-Sharing:** Traditional paper passes are frequently lent to friends or family members. Biometric verification ensures "Proof of Presence," meaning the pass only activates when the physical owner is present, making unauthorized transfers impossible.
- **Prevention of Counterfeiting:** Paper booklets and basic ID cards are easily photocopied or forged using modern printing technology. Our Smart Cards utilize Encrypted Microchips with unique digital signatures that cannot be duplicated or "cloned" by unauthorized parties.
- **Ghost Student Detection:** By linking the issuance of passes to a centralized government or institutional database (like Aadhaar or a University Portal), the system prevents the creation of "Ghost Profiles"—fake identities used to siphon off transportation subsidies.

- **Anti-Tamper Digital Records:** In a manual system, dates and names on paper can be altered with ink. In our system, the "Validity Period" is hard-coded into the card's memory and verified against a secure server, preventing students from manually extending their pass expiration dates.
- **Instant Deactivation:** If a card is reported lost or stolen, it can be "Blacklisted" in the central system instantly. Any attempt to use a blacklisted card triggers an immediate alert on the conductor's handheld device, preventing further unauthorized use.

Technical Fraud Prevention Comparison

Fraud Type	Paper/Manual System	Biometric Smart System
Pass Sharing	High (Visual checks are brief)	Impossible (Requires Fingerprint)
Forged IDs	Moderate (Photocopies)	None (Encrypted Microchip)
Data Alteration	Easy (Ink/Erasure)	None (Read-Only Memory)
Lost Card Usage	Until Expiry	Immediate (Remote Kill-Switch)

6. PROJECT METHODOLOGY (SCAN-AND-VERIFY SYSTEM)

Phase 1: Enrollment & Secure QR Generation

The foundation of the system is the creation of a tamper-proof digital token for every student.

- **Data Encoding:** Student details (Name, ID, Photo URL, and Expiry) are bundled into a data string.
- **Digital Signing:** To prevent fraud, the data is "signed" using a private cryptographic key. This creates a Secure QR Code that cannot be altered or generated by third-party apps.
- **Multi-Platform Issuance:** The QR code is printed on a durable PVC ID card and also made available on a mobile app for student convenience.

Phase 2: Offline "Scan-and-Verify" Logic

Designed for India's diverse terrain, the verification process requires zero active internet at the point of boarding:

- **High-Speed Scanning:** The conductor uses a rugged handheld device (or a smartphone with a professional-grade scanner) to capture the QR code.
- **Local Decryption:** The device uses a stored "Public Key" to decrypt the QR code instantly. If the signature is valid, the student's Full Profile and Photo appear on the conductor's screen.
- **Visual Authentication:** Since the photo is pulled directly from the encrypted data, the conductor performs a quick visual match to ensure the person scanning is the authorized owner.
- **Status Validation:** The software automatically checks the "Valid Until" date embedded in the code. If the pass has expired, the screen flashes red and sounds an alert.

Phase 3: Data Integrity & Store-and-Forward

To ensure uncompromised records without manual logs:

- **Cryptographic Hashing:** Every scan generates a unique transaction hash. This prevents "replay attacks" (where someone tries to use a photo of an old scan to trick the system).
- **GPS Geo-Tagging:** Every successful scan is tagged with the bus's current GPS coordinates, creating a precise map of student boarding patterns.
- **Asynchronous Syncing:** The device stores all scan logs in an internal encrypted database. Once the bus returns to a depot or enters a 4G/5G coverage area, the data is pushed to the central cloud for institutional auditing.

Why "Scan-and-Verify" is Superior to Paper

Feature	Manual Paper Pass	Our Secure QR System
Verification	Slow, subjective visual check	Instant, data-backed validation
Data Security	Easily forged with a copier	Cryptographically signed (Unforgeable)
Recovery	Lost pass = Lost record	Digital QR can be re-issued instantly
Cost	High recurring printing costs	Low-cost QR printing or Mobile-only

7. ADVANTAGES

- **Prevents Pass Sharing:** The visual photo match ensures only the registered student can travel.
- **Eliminates Physical Cards:** Reduces costs and the risk of loss or theft.
- **Real-Time Accuracy:** Online database checks ensure that expired or cancelled passes are rejected instantly.
- **Student-Only Access:** The system is restricted to verified students, preventing general public misuse of student-specific discounts.

8. CONCLUSION

The implementation of the Smart Student Transit System represents a transformative shift from manual, error-prone paper booklets to a high-security, digitally-integrated ecosystem. By prioritizing Scan-and-Verify technology and Automated Data Integrity, this project provides a scalable solution to the long-standing challenges of public student transportation in India.

8.1 Strategic Impact

The project successfully bridges the gap between urban technological advancement and rural accessibility. Through its Offline-First architecture, the system ensures that a student in a remote village receives the same level of security and efficiency as one in a metropolitan city, regardless of internet stability.

8.2 Key Pillars of the System:

- **Economic Accountability:** By effectively Eliminating Fraud through encrypted QR codes and UID-mapped Smart Cards, the transport department can recover significant revenue currently lost to pass-sharing and forgery. This makes the student subsidy model financially sustainable for the long term.
- **Operational Efficiency:** The transition to a "Tap-and-Go" or "Scan-and-Verify" model drastically reduces boarding times. Conductors no longer need to manually inspect or stamp paper logs, allowing for faster transit cycles and better adherence to schedules.
- **Uncompromised Data Integrity:** Moving away from pen-and-paper records to Geo-tagged Digital Logs ensures a "Single Source of Truth." Every boarding event is time-stamped and encrypted, providing authorities with precise, tamper-proof data for auditing and resource allocation.
- **Data-Driven Planning:** The system provides unprecedented insights into student migration patterns. Real-time analytics on bus occupancy and peak-hour heatmaps allow for Dynamic Route Optimization, ensuring buses are deployed where they are needed most.

9. FEATURE SCOPE (ENHANCED BIOMETRIC EDITION)

9.1. Biometric & Security Features

- **One-to-One (1:1) Local Matching:** The student's biometric template is stored in an encrypted segment of the Smart Card. When scanned, the handheld device compares the "live" finger/iris against the "stored" template locally. This ensures 100% offline verification.
- **Multi-Modal Biometrics:** Support for both Fingerprint Recognition (standard) and Facial Recognition (contactless) to ensure accessibility for students with physical disabilities or during peak "rush" boarding.
- **Liveness Detection:** Advanced sensors that distinguish between a real human finger/face and a high-resolution photograph or silicon mold, preventing sophisticated identity spoofing.
- **Encrypted Template Storage:** Instead of storing actual images of fingerprints (which poses privacy risks), the system stores mathematical "hashes." These hashes cannot be reversed to recreate a fingerprint, ensuring GDPR and Data Privacy compliance.

9.2. Student & User Features

- **Card-Less Boarding:** An optional "Emergency Boarding" feature where a student who forgot their card can still board by providing their Aadhaar ID and a biometric scan linked to the central cloud.
- **Self-Service Enrollment Kiosks:** Touchscreen stations placed at campus entrances where students can update their biometric profiles or renew their passes without visiting a manual counter.
- **Usage Transparency:** A mobile portal where students can view their "Identity Logs"—seeing exactly when and where their biometric ID was used for transit.

9.3. Conductor & Operations Features

- **Biometric Attendance for Staff:** Conductors and drivers use the same handheld device to "Clock-In" for their shifts, ensuring staff accountability and preventing unauthorized personnel from operating the vehicle.
- **High-Durability Sensors:** Deployment of **IP65-rated rugged scanners** that can read fingerprints even if they are dusty, wet, or worn—crucial for students coming from agricultural or laboratory environments.

9.4. Administrative & Analytical Features

- **Fraud Heatmaps:** A dashboard that flags "Failed Biometric Attempts." If a specific route has high failure rates, it alerts authorities to investigate potential organized pass-sharing attempts.
- **Automated Audit Trails:** Every boarding is linked to a unique biometric signature, creating a forensic-level audit trail for government subsidy providers, proving that funds are being used by the intended recipients.

10. REFERENCES

- [1]. Pavithra, S., & Rani, M. S. (2021). IoT Based Smart Bus Pass System using QR Code. *International Journal of Scientific Research in Science and Technology*, 8(3), 450-455.

- [2]. Smith, M., & Jones, L. (2023). The Impact of QR Code Technology on Urban Transport Efficiency. *International Journal of Smart City Development*, 7(4), 210-222.
- [3]. Gupta, S., & Sharma, V. (2025). Advanced Encryption Standards for QR-Based Public Transit. *Journal of Cybersecurity and Data Privacy*, 5(1), 12-25.
- [4]. Want, R. (2011). Near Field Communication and QR Protocols for Mobile Authentication. *IEEE Pervasive Computing*, 10(3), 4-7.
- [5]. Smith, M., & Jones, L. (2023). The Impact of QR Code Technology on Urban Transport Efficiency. *IJSC*.
- [6]. Finkenzeller, K. (2010). *RFID and QR Handbook: Fundamentals and Applications in Contactless Smart Cards*. Wiley.
- [7]. Jaiswal, A., & Arun, C. J. (2021). Potential of Digital Identity for transformation of the transport system in India. *IJEDICT*, 17(1), 142-158.
- [8]. Kumar, R., & Singh, P. (2022). Secure Student Identity Verification Systems for Public Transport. *Journal of Network and Information Security*, 10(2), 88-94.
- [9]. Afrita, J. (2023). Digital Efficiency in Educational Infrastructure. *COMSERVA: (Jurnal Penelitian Dan Pengabdian Masyarakat)*, 2(12), 3181-3187.
- [10]. Annur, A. F. (2022). Implementation of Smart Identification in Improving Student Ethics. *Jurnal Ilmiah Pendidikan Guru MI*, 12(2), 99-108.