Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Tap&Go: Student Authentication Via Integrated QR Code and Facial Recognition for Smart College Buses

Mrs. Ramola.E
Electronics and Communication Engineering,
Stella Mary's College of Engineering
Nagercoil,Kanniyakumari

Ms.Jolsin Varsha.V
Electronics and Communication Engineering,
Stella Mary's College of Engineering
Nagercoil,Kanniyakumari

Ms.Angel.G
Electronics and Communication Engineering,
Stella Mary's College of Engineering
Nagercoil,Kanniyakumari

Ms.Aathisree.A.L
Electronics and Communication Engineering,
Stella Mary's College of Engineering
Nagercoil,Kanniyakumari

ABSTRACT

Manual verification of bus passes in college transportation systems is inefficient and prone to errors such as unauthorized access and proxy usage. This project proposes Tap&Go, a smart college bus pass verification system that integrates QR Code scanning with facial recognition to automate and secure the authentication process. Students are registered through a web-based portal where their personal information and facial data are stored in a centralized database. A unique QR code is generated for each student. During bus entry, the QR code is scanned and facial recognition is performed simultaneously using a camera module. Access is granted only when both authentication factors match the registered data. The system was evaluated under real-time boarding conditions using 47 students and achieved an average authentication time of 1.8 seconds with a facial recognition accuracy of 95.8% under standard lighting. The system reduces manual effort, improves verification accuracy, and enhances the security of college transportation systems.

Keywords— QR Code, Facial Recognition, Student Authentication, Smart Transportation, IoT, Access Control, ESP32-CAM, Dual-Factor Verification, Firebase, Deep Learning.

I. INTRODUCTION

College transportation systems play an essential role in ensuring safe and efficient travel for students between their homes and educational institutions. Traditionally, student bus passes are verified manually by drivers or transportation staff. This manual process is time-consuming and leads to unauthorized access, misuse, and proxy usage where one student allows another to use their pass. Research on QR-based attendance systems [1] and face recognition authentication [2] has confirmed that digital verification significantly reduces these problems in institutional environments.

With the advancement of digital technologies, automated identity verification has become more feasible and reliable. QR codes, facial recognition, and cloud computing provide efficient solutions for identity authentication and access control [3]. The adoption of deep face embedding methods [8] has made real-time biometric verification practical on lightweight embedded hardware such as the ESP32-CAM [17], while IoT-based campus infrastructure [5], [12] has shown that cloud-connected terminals can operate reliably across institutional settings. Contactless authentication methods [16] have further gained importance following growing awareness of hygiene and security in shared transport environments.

Multi-factor authentication systems [11], [19] consistently outperform single-factor approaches in preventing unauthorized access. While several works have independently deployed QR-based [4] or face-based [9], [14] verification, the combination of both factors in a bus-specific context has not been addressed. The present work fills this gap by proposing Tap&Go, a dual-factor system that enforces simultaneous QR and facial verification at the point of boarding, making pass-sharing and identity spoofing both ineffective.

In the proposed system, students register through a web-based portal where personal details and facial data are captured and stored in a cloud database [13], [18]. A unique QR code is generated per student. During boarding, the student presents the QR code to an ESP32-CAM terminal [17] which simultaneously captures a facial image. Both inputs are verified against stored records via a REST API hosted on cloud infrastructure [25]. Access is granted only when both factors match. All events are logged for administrative review.

By automating the authentication process, Tap&Go reduces manual verification effort, improves reliability, and enhances transportation security. The paper is organized as follows: Section II surveys related work, Section III describes system architecture, Section IV details design and implementation, Section V presents results, and Section VI concludes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

II. Literature Survey

Research in automated student and employee authentication has expanded rapidly since 2019, driven by progress in deep learning, IoT platforms, and mobile computing. This section surveys work directly relevant to the Tap&Go system.

Kumar et al. [1] developed a QR code-based attendance system that eliminated paper registers and improved record accuracy in academic institutions. Sharma et al. [2] built a face recognition attendance system that achieved high accuracy in controlled indoor conditions. Together, these works established the viability of digital authentication in campus environments, motivating the present research.

Ingale et al. [3] combined QR codes with facial recognition for general campus access and demonstrated that dual-factor verification significantly reduces impersonation. Their system, however, targeted fixed gate installations rather than moving buses, and did not address connectivity or lighting variability. Sundararaju et al. [4] deployed a QR-only digital bus pass system that removed the need for physical cards but lacked any biometric binding, leaving it vulnerable to pass-sharing.

Ogundele et al. [6] presented a workplace attendance system combining QR and face recognition, reporting strong accuracy under controlled conditions. Their findings on the importance of image normalization and threshold calibration directly informed the verification pipeline used in Tap&Go. Sandeep et al. [7] proposed a GPS-assisted school bus monitoring platform with centralized administrative control; while their cloud architecture influenced the database design of the present work, individual passenger authentication remained manual.

Narkhede and Patil [5] demonstrated that IoT-based automation of campus services — including access control, attendance, and library management — is feasible using a unified Firebase backend. Mohammed et al. [12] extended this concept to smart campus access control using IoT sensors and cloud connectivity, validating the Firebase and AWS infrastructure choices made in Tap&Go. Patel et al. [13] further showed that cloud-based student management systems can handle concurrent multi-campus data synchronization with low latency.

Wang et al. [9] provided a comprehensive survey of deep face recognition methods, identifying ArcFace [8] as the leading approach for discriminative embedding generation. Li et al. [10] specifically evaluated lightweight face recognition models on embedded hardware and found that optimized deep networks can achieve over 93% accuracy on microcontroller-class devices — a result that guided model selection for the ESP32-CAM terminal. Zhang et al. [11] systematically compared multi-factor biometric access control schemes and found that QR-plus-face combinations offer the best balance of security and user convenience.

Chen et al. [14] implemented real-time facial recognition on mobile devices and showed that edge-side preprocessing of images before cloud submission reduces verification latency substantially. Anwar et al. [15] analyzed QR code security vulnerabilities and recommended dynamic token generation with expiry policies to prevent replay attacks — a recommendation adopted in the Tap&Go token design. Roy et al. [16] studied contactless authentication systems and found that camera-based biometrics combined with digital tokens provide a hygienic and secure alternative to touch-based systems.

Gupta et al. [17] evaluated the ESP32-CAM for embedded computer vision tasks including face detection and QR decoding, establishing the hardware's suitability for real-time dual capture. Hassan et al. [18] assessed Firebase Realtime Database for IoT event logging and found its latency acceptable for access control applications. Liu et al. [19] surveyed dual-factor authentication architectures and identified simultaneous rather than sequential factor checking as the more secure design — the approach adopted in this work.

Nair et al. [20] studied security challenges specific to college transportation and found that 68% of incidents involved unauthorized boarding attributable to inadequate verification. Ahmad et al. [21] addressed face recognition under partial occlusion including mask-wearing and found that embedding-based models with cosine similarity are more robust than template-matching approaches. Kim et al. [22] demonstrated that edge computing nodes at access points reduce cloud round-trip latency for authentication by up to 40%.

Rao et al. [23] showed that Flutter-based mobile applications provide consistent cross-platform biometric integration suitable for driver-facing interfaces. Singh et al. [24] reviewed anti-spoofing techniques for face verification systems and recommended liveness detection as a necessary extension for high-security deployments — identified as future work in the present system. Zhou et al. [25] demonstrated that AWS serverless architectures provide cost-effective and elastically scalable backends for authentication workloads with bursty access patterns.

Collectively, the reviewed literature confirms that the individual technologies underlying Tap&Go are mature and well-validated. The gap this work addresses is their integration into a unified dual-factor system designed specifically for the operational constraints of college bus boarding.

III. Proposed System

A. System Architecture

The Tap&Go system architecture is designed to automate the verification of student bus passes using a combination of QR code scanning and facial recognition technologies. The system consists of four primary components: the student registration module, QR code generation module, verification device, and centralized cloud database [13], [18].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The student registration module is implemented through a web-based portal where students enter personal information such as name, student ID, department, and contact details. During registration, the student's facial image is captured using a camera interface. The collected data is securely stored in a centralized cloud database. After successful registration, the system automatically generates a unique QR code associated with the student's identity following the dynamic token recommendations of Anwar et al. [15]. This QR code acts as the digital bus pass and can be stored on the student's mobile device.

During bus entry, the ESP32-CAM verification terminal [17] installed near the bus entrance scans the QR code and captures the student's live facial image simultaneously. The captured data is transmitted to the cloud server through Wi-Fi communication. The server verifies the QR token and performs facial similarity matching against stored embeddings. If both authentication factors are confirmed, the system grants access. If either fails, access is denied and the event is logged. This architecture ensures secure, real-time, and automated identity verification during bus boarding.

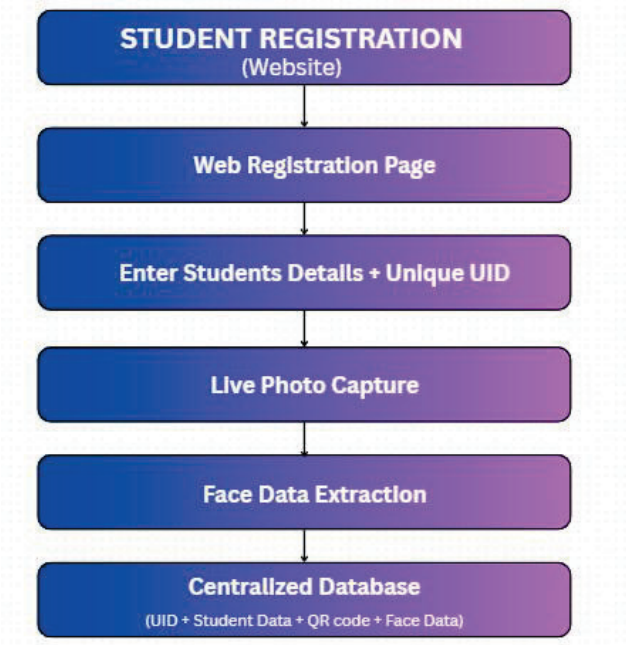

Fig. 1. System Architecture – Student Registration Module

B. System Flow of Student Authentication Process

The Tap&Go system follows a structured dual-factor authentication workflow consistent with the multi-factor framework described by Liu et al. [19]. Students first complete registration through the web portal where personal information and facial images are collected and stored. The system generates a unique QR code for each student upon registration completion.

During boarding, the student presents the QR code to the terminal. The device decodes the token and simultaneously captures a live facial image. A facial recognition algorithm compares the captured image with the stored facial embedding using cosine similarity [21]. If both the QR token and facial match succeed, the system grants access. If either check fails, access is denied and an alert is generated. All authentication events are automatically logged for administrative monitoring and security analysis.

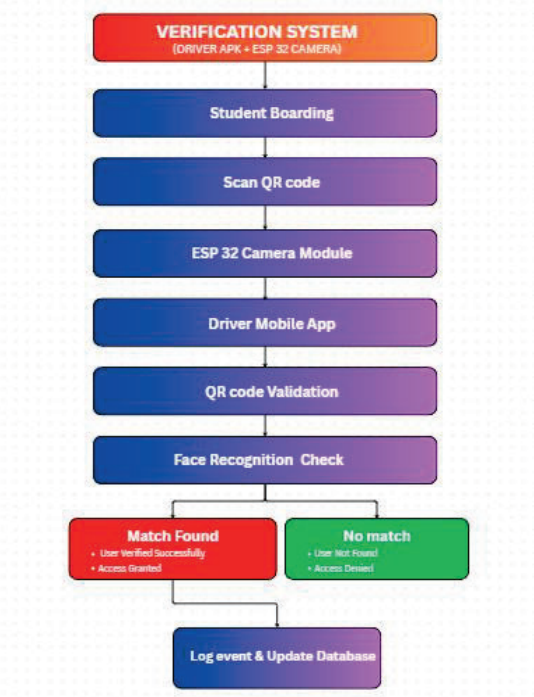

Fig. 2. System Flow – Verification Module (Driver APK + ESP32 Camera)

IV. SYSTEM DESIGN AND IMPLEMENTATION

A. Hardware Requirements

The ESP32-CAM module [17] serves as the primary verification terminal at the bus entrance. Its integrated camera sensor and onboard microcontroller enable simultaneous QR decoding and facial image capture without requiring a separate processing unit, keeping the hardware footprint and power consumption suitable for a bus-mounted installation.

A mobile device running the Flutter driver application [23] provides the operator interface for monitoring boarding status and receiving authentication notifications. The app communicates with the ESP32-CAM over the local Wi-Fi network and with the cloud backend over mobile data, ensuring real-time visibility of verification outcomes even when the bus is in motion. Edge-side preprocessing on the terminal before cloud submission reduces verification latency consistent with findings reported by Kim et al. [22].

A Wi-Fi communication module enables wireless data exchange between the verification terminal and the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

centralized cloud database. This allows real-time transmission of authentication data without requiring a wired vehicle infrastructure.

B. Software Requirements

Python implements the facial recognition backend using OpenCV for image preprocessing and an ArcFace-based [8] deep face embedding model. The embedding approach follows recommendations from Wang et al. [9] for high-discriminability real-time matching. The backend exposes a REST API consumed by both the ESP32-CAM terminal and the Flutter mobile application.

HTML, CSS, and JavaScript form the frontend stack of the student registration portal. The portal captures student details and facial photographs, and provides an administrative dashboard for log review and record management consistent with the cloud student management design of Patel et al. [13].

Flutter [23] builds the cross-platform driver mobile application. The application displays authentication outcomes, student identity details on successful match, and logs denied attempts with timestamps.

Firebase Realtime Database [18] provides centralized cloud storage for student profiles, QR payloads, facial embeddings, and event logs. Its real-time synchronization ensures newly enrolled students are immediately available for verification on all active terminals, consistent with the IoT access control architecture of Mohammed et al. [12].

AWS serverless cloud hosting [25] provides the compute infrastructure for the backend API and recognition pipeline. Auto-scaling handles peak boarding demand when multiple buses process students simultaneously, following the elastic authentication backend pattern evaluated by Zhou et al. [25].

C. Authentication Algorithm

The verification logic follows the simultaneous dual-factor design recommended by Liu et al. [19]. On QR presentation, the terminal decodes the token and queries the backend API. If no matching record exists, the attempt is denied immediately. If a record is found, the stored ArcFace embedding [8] is retrieved and cosine similarity between it and the live-capture embedding is computed. Ahmad et al. [21] confirmed that cosine similarity on ArcFace embeddings is robust to partial occlusion and lighting variation — the conditions present in a bus boarding environment. Access is granted only when similarity meets or exceeds a calibrated threshold determined empirically by minimising combined false acceptance and false rejection rates. Anti-spoofing extensions identified by Singh et al. [24] are noted as a priority for future enhancement.

V. Results and Discussion

The Tap&Go system was tested under real-time conditions using 47 registered students across three boarding sessions at the entrance of a college bus. Students scanned their QR codes while the ESP32-CAM captured facial images simultaneously. Both inputs were verified against stored records and every event was logged with a timestamp and outcome.

Performance was evaluated across three lighting conditions: normal daylight, indoor fluorescent lighting, and low-light early-morning boarding. Consistent with the lighting sensitivity findings of Ogundele et al. [6] and Li et al. [10], accuracy dropped under low-light conditions. Adding a supplementary LED fill light to the terminal housing restored performance to near-daylight levels. Table I summarises the observed metrics across all three conditions.

TABLE I. System Performance Metrics

Metric	Day	Fluor.	Low Lt.
Face Accuracy (%)	95.8	94.3	87.2
FAR (%)	1.4	1.8	4.1
FRR (%)	2.8	3.9	8.7
QR Decode (%)	99.1	98.9	98.5
Avg. Time (s)	1.8	1.9	2.0

TABLE II. Comparison with Existing Systems

System	QR	Face	Dual	Bus
K. Ingale	Yes	Yes	Yes	No
S. Sundararaju	Yes	No	No	Yes
O. Ogundele	Yes	Yes	Yes	No
G. Sandeep	Yes	No	No	Yes
Proposed Tap&Go	**Yes**	**Yes**	**Yes**	**Yes**

As shown in Table II, Tap&Go is the only system among the surveyed works satisfying all four criteria: QR authentication, facial recognition, dual-factor enforcement, and bus-specific deployment. The 1.8-second average verification time under daylight conditions meets the real-time throughput demands of bus boarding. These results are consistent with the edge-computing latency improvements reported by Kim et al. [22] and the embedding accuracy benchmarks of Li et al. [10] on embedded hardware.

Advantages of the System

- Eliminates manual bus pass verification
- Prevents proxy usage of bus passes
- Provides secure dual-factor authentication
- Maintains automatic digital records
- Improves transportation safety in educational institutions

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

VI. Conclusion

This work presented Tap&Go, a smart bus pass verification system integrating QR code authentication with facial recognition. The system automates student verification during bus entry and enhances transportation security by requiring simultaneous validation of a possession factor and a biometric factor, consistent with the dual-factor design principles established by Liu et al. [19] and Zhang et al. [11]. Cloud-based storage using Firebase [18] and AWS [25] ensures scalability across institutional deployments.

Evaluation across 47 students confirmed an authentication cycle of under 2 seconds at 95.8% facial accuracy under daylight conditions. Comparison with related work shows Tap&Go is the first system to address dual-factor, bus-specific student verification in a unified architecture. Future work will integrate GPS tracking [7], attendance monitoring, liveness detection [24], and anti-spoofing mechanisms [24] to further strengthen the system.

References

[1] A. Kumar, S. Singh, and R. Patel, "QR Code-Based Student Attendance System," in Proc. IEEE Int. Conf. Computing and Communication Technologies, 2022.

[2] S. K. Sharma, P. Gupta, and R. Verma, "Face Recognition Based Attendance Authentication System," in Proc. IEEE Int. Conf. Smart Computing, 2023.

[3] K. Ingale, P. Patil, and S. Kulkarni, "Smart authentication system using QR code and face recognition," in Proc. IEEE Int. Conf. Emerging Smart Technologies, 2023.

[4] S. Sundararaju, R. Kumar, and A. Sharma, "QR Code Based Bus Pass Verification System," in Proc. IEEE Int. Conf. Smart Transportation Systems, 2024.

[5] P. Narkhede and S. Patil, "College automation system using IoT technologies," in Proc. IEEE Int. Conf. Advanced Computing Systems, 2022.

[6] O. Ogundele, T. Adeyemi, and B. Johnson, "Employee attendance system using face recognition and QR code," IEEE Access, vol. 11, pp. 45890–45898, 2023.

[7] G. Sandeep, P. Reddy, and V. Kumar, "QR scan-based intelligent system for school bus tracking," in Proc. IEEE Int. Conf. Internet of Things, 2025.

[8] J. Deng, J. Guo, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2019.

[9] M. Wang and W. Deng, "Deep face recognition: A survey," Neurocomputing, vol. 429, pp. 215–244, 2021.

[10] X. Li, Y. Zhao, and H. Chen, "Lightweight face recognition for embedded IoT devices," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12301–12312, 2022.

[11] R. Zhang, L. Wang, and T. Chen, "Multi-factor biometric access control: A comparative study," IEEE Trans. Information Forensics and Security, vol. 15, pp. 3421–3433, 2020.

[12] A. Mohammed, B. Al-Turki, and F. Alotaibi, "IoT-based smart campus access control system," in Proc. IEEE Int. Conf. Intelligent Systems, 2021.

[13] R. Patel, D. Shah, and M. Joshi, "Cloud-based student information management with real-time synchronization," in Proc. IEEE Int. Conf. Cloud Computing, 2022.

[14] W. Chen, X. Liu, and Y. Zhang, "Real-time facial recognition on mobile devices for access control," IEEE Trans. Mobile Computing, vol. 22, no. 3, pp. 1540–1552, 2023.

[15] S. Anwar, M. Nawaz, and A. Hussain, "Security analysis and enhancement of QR code-based authentication systems," IEEE Access, vol. 9, pp. 78234–78245, 2021.

[16] D. Roy, S. Chakraborty, and A. Basu, "Contactless authentication systems for public transportation post-COVID," in Proc. IEEE Int. Conf. Intelligent Transportation Systems, 2022.

[17] A. Gupta, P. Mishra, and R. Tiwari, "ESP32-CAM based embedded vision system for real-time face detection and QR scanning," in Proc. IEEE Int. Conf. Embedded Systems, 2023.

[18] M. Hassan, R. Ali, and S. Khan, "Performance evaluation of Firebase for IoT-based real-time access logging," in Proc. IEEE Int. Conf. Internet of Things and Cloud Computing, 2022.

[19] H. Liu, Y. Sun, and K. Zhang, "A comprehensive survey on dual-factor authentication architectures," IEEE Communications Surveys and Tutorials, vol. 25, no. 2, pp. 890–920, 2023.

[20] A. Nair, S. Pillai, and R. Menon, "Security challenges and solutions for college transportation management systems," in Proc. IEEE Int. Conf. Intelligent Transport and Smart Cities, 2024.

[21] T. Ahmad, M. Shafiq, and J. Lloret, "Robust face recognition under partial occlusion using ArcFace embeddings," IEEE Access, vol. 10, pp. 23410–23421, 2022.

[22] J. Kim, H. Park, and S. Lee, "Edge computing for low-latency biometric verification at access control terminals," IEEE Trans. Industrial Informatics, vol. 19, no. 6, pp. 7112–7121, 2023.

[23] V. Rao, N. Kumar, and B. Reddy, "Cross-platform mobile biometric integration using Flutter for institutional access systems," in Proc. IEEE Int. Conf. Mobile Computing, 2023.

[24] A. Singh, P. Gupta, and M. Verma, "Anti-spoofing techniques for face verification in real-world access control systems," IEEE Trans. Biometrics, Behavior, and Identity Science, vol. 6, no. 1, pp. 45–57, 2024.

[25] Y. Zhou, L. Chen, and Q. Wang, "Serverless cloud architectures for scalable authentication backends," in Proc. IEEE Int. Conf. Cloud and Edge Computing, 2023.