ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

Behaviour Aware Hybrid Edge-Cloud ALPR for Secure and Privacy Preserving Residential Gate Access Control

Tadiwanashe Shamba, Admire Janga

[1]Asia Pacific University of Technology and Innovation, Malaysia

[2]Chinhoyi University of Technology, Zimbabwe

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150900094

Received: 17 September 2026; Accepted: 22 September 2026; Published: 16 October 2026

ABSTRACT

Automatic License Plate Recognition (ALPR) can automate residential vehicle access, but conventional cloud centric and edge only approaches face limitations in latency, privacy, computational capability, and recognition robustness. This study presents a deployed residential smart gate prototype that integrates a confidence aware hybrid ALPR pipeline, a Vehicle Behavior Profiling System (VBPS), and security hardened MQTT/TLS communication on a Raspberry Pi 5. The ALPR pipeline employs YOLOv5n ONNX for license plate detection and dynamically routes detected plates to an in-memory resident cache, local Tesseract OCR, or cloud OCR based on recognition confidence and recent vehicle history, while the VBPS maintains vehicle profiles and evaluates temporal and frequency based behavioural features to generate five adaptive gate decisions instead of a binary allow/deny response. Gate control and monitoring communications are secured using MQTT over TLS 1.2 with AES-256-GCM encryption and mutual certificate authentication. Experimental evaluation of the deployed prototype achieved 97.3% detection mAP, a 61% cache hit rate, a 96.7% reduction in cloud API usage, and a weighted average processing latency of 749 ms. The false denial rate decreased from 51.3% in the evaluated baseline configurations to 3.6% with the behaviour aware system, while the VBPS achieved 100% precision across the evaluated structured temporal and behavioral anomaly scenarios and satisfied all 12 evaluated access control requirements. Furthermore, four security tests covering unauthorized clients, message interception, replay attacks, and command integrity were successfully passed. These findings demonstrate the feasibility of combining hybrid ALPR, behaviour aware access control, and secure IoT communication on constrained residential hardware, while identifying the need for larger real-world datasets and further optimization of end-to-end latency.

Index Terms - Automatic License Plate Recognition (ALPR), edge computing, cloud computing, Internet of Things (IoT), smart gate, vehicle behavior profiling, anomaly detection, MQTT, TLS, privacy preserving access control**.**

INTRODUCTION

Residential access control systems increasingly employ Automatic License Plate Recognition (ALPR) to automate vehicle identification and reduce dependence on manual gate operation; however, practical deployment requires more than recognition accuracy, as reliability, response time, privacy, secure communication, and context aware access decisions must be addressed simultaneously. Existing architectures present an edge–cloud trade off: cloud based ALPR can provide stronger recognition capabilities but requires transmission of vehicle images or plate crops outside the residential environment, creating privacy risks and network dependent latency, with the reviewed literature reporting cloud processing latencies above 200 ms, whereas edge only processing improves privacy and reduces network dependence but may experience degraded performance under challenging lighting, weather, glare, and related conditions, with approximately 90.3% performance reported under difficult edge processing scenarios. Furthermore, conventional ALPR systems typically apply static access rules after identifying a vehicle and therefore cannot distinguish normal behavior from anomalous activity, such as an authorized vehicle appearing at an unusual time, highlighting a

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

gap between behavioral anomaly detection and physical residential access control. Communication security is also critical because compromise of a gate control channel can result in unauthorized physical access, while existing IoT literature identifies weak authentication, unsecured communication, default credentials, and other device level vulnerabilities as recurring smart-home concerns. To address these limitations, this work integrates ALPR, vehicle behavior analysis, and IoT security within a deployed prototype comprising a Raspberry Pi 5, IMX219 camera, and HC-SR04 proximity sensor. YOLOv5n ONNX performs license plate detection, followed by confidence-aware routing to an in-memory resident cache, local Tesseract OCR, or cloud OCR; the recognized plate is then processed by the Vehicle Behavior Profiling System (VBPS), which updates the vehicle's historical profile and computes a contextual risk score. A five-level adaptive decision mechanism determines the appropriate gate response, with the resulting control command transmitted through a TLS secured MQTT infrastructure to the gate controller.

Related Work

Recent Automatic License Plate Recognition (ALPR) systems increasingly employ deep learning object detectors, particularly YOLO based architectures, to achieve accurate and real time license-plate localization and recognition. Al-Batat et al. [1], [2] demonstrated YOLO based end-to-end ALPR and investigated optimization strategies for deployment under constrained edge computing conditions. Similarly, Al-Hasan et al. [3], [4] explored enhanced YOLO and CNN based approaches to improve recognition robustness under challenging environmental conditions, while Tao et al. [16] and Zhang et al. [17] investigated methods for improving ALPR performance in the presence of image degradation and adverse acquisition conditions.

These studies demonstrate the effectiveness of deep learning-based ALPR; however, high recognition performance alone does not address the broader requirements of residential access control, where processing latency, privacy, network dependency, and computational resources must also be considered. Edge based processing can reduce external data transmission and improve privacy, but constrained hardware may limit recognition capability, whereas cloud-based processing provides greater computational resources at the cost of network dependence and potential privacy exposure. Leng et al. [5] investigated hybrid or cloud assisted ALPR architectures that dynamically utilize cloud resources, motivating confidence aware processing strategies. Building on this concept, the proposed system introduces resident aware in memory caching and confidence-based routing to prioritize local processing and reserve cloud OCR for cases where local recognition confidence is insufficient.

Beyond vehicle identification, conventional access-control systems generally rely on static identity-based authorization, which may be inadequate when an otherwise legitimate vehicle exhibits abnormal behavior. Behavioral anomaly detection research has demonstrated the value of temporal, frequency based, and deviation-related features for identifying unusual activities [8]– [13], [18]. Janati and Messaoudi [10], for example, investigated behaviour-based anomaly detection using frequency, timing, and deviation signals, while Kaveh et al. [11] and Landauer et al. [12] examined time series and temporal approaches to anomaly detection. Pathirannahalage et al. [13] and Elmetwally et al. [18] further demonstrated the relevance of temporal information for real-time surveillance and abnormal event detection.

Trust and behaviour-based access control approaches have also been investigated by Cabanillas Rodríguez et al. [6], [7], while Farhadighalati et al. [9] examined behavioural and access control requirements. However, these approaches are generally applied to cybersecurity, surveillance, or generalized access control scenarios rather than being directly integrated with identity linked residential vehicle access. The proposed work addresses this gap through a lightweight Vehicle Behavior Profiling System (VBPS) that combines temporal deviation, unusual access patterns, visit frequency, and vehicle residency information to produce contextual risk and adaptive gate decisions without requiring computationally expensive temporal models.

Security is another critical consideration because a residential smart gate represents a cyber-physical system in which compromise of the communication channel can directly result in unauthorized physical access. Previous studies have identified recurring security weaknesses in smart home and IoT environments, including inadequate authentication, insecure communication, vulnerable device configurations, and other

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

implementation level weaknesses [14]. More advanced anomaly detection approaches for constrained IoT environments have also explored deep learning and transformer-based techniques [15], although their computational requirements may limit direct deployment on low-power gate controllers. Accordingly, the proposed architecture incorporates security directly into the gate control communication layer using MQTT over TLS with mutual certificate authentication and authenticated command exchange. Overall, the reviewed literature demonstrates substantial progress in ALPR accuracy, edge/cloud processing, behavioral anomaly detection, and IoT security, but these areas have largely been investigated independently.

The principal research gap addressed in this work is therefore the integration of confidence aware hybrid ALPR, resident aware caching, lightweight vehicle behaviour profiling, adaptive access control, and secure IoT communication within a single Raspberry Pi-based residential gate prototype, enabling recognition confidence, historical vehicle behavior, privacy considerations, and communication security to jointly influence the final physical access decision.

Proposed System

The proposed smart gate system integrates five principal subsystems: vehicle detection and ALPR, the Vehicle Behavior Profiling System (VBPS), gate control, secure MQTT communication, and a monitoring dashboard. The physical prototype is implemented on a Raspberry Pi 5 with 8 GB RAM, an IMX219 8 MP CSI camera, an HC-SR04 ultrasonic sensor for vehicle detection at approximately 50 cm, and an Arduino Uno connected through USB serial to an L298N motor driver controlling a 3D printed boom gate.

The Raspberry Pi performs YOLOv5n ONNX inference, OCR routing, behavioral analysis, MQTT communication, and dashboard services. Following vehicle detection, the camera image is processed by YOLOv5n ONNX to generate a license-plate bounding box and confidence score, after which a confidence-aware routing mechanism selects one of three processing paths: a resident-aware in-memory cache with a 300-s time-to-live for recently recognized plates, local Tesseract OCR for uncached detections with YOLO confidence ≥0.75, or the Plate Recognizer cloud API for detections below the 0.75 threshold.

The recognized plate is subsequently processed by the VBPS, which maintains historical vehicle profiles and computes a lightweight contextual risk score using four factors: deviation from normal entry time, unusual day or temporal behavior, abnormal visit frequency, and vehicle residency classification, with corresponding configurable weights.

Vehicle profiles evolve through the categories UNKNOWN, VISITOR, FREQUENT_VISITOR, and RESIDENT, allowing historical behavior to supplement conventional whitelist-based identification. The resulting risk score is mapped to five adaptive responses AUTO_OPEN, SLOW_OPEN, VISITOR_OPEN, LOG_ONLY, and DENY providing proportional and explainable access decisions rather than binary authorization. Each event records the plate identifier, timestamp, risk score, behavioral flags, and final decision.

Gate commands are transmitted from the Raspberry Pi to the Arduino through serial communication, while events are published through an MQTT broker and stored locally in SQLite. Communication security is enforced using MQTT over TLS 1.2 on port 8883 with AES-256-GCM encryption and mutual certificate authentication, with the unsecured port 1883 disabled. The security design addresses unauthorized client connections, message interception or man-in-the-middle attacks, replay attacks, and unauthorized gate-command publication.

Finally, a Flask-based monitoring dashboard provides real-time visualization of gate events, timestamps, risk scores, behavioral flags, and decisions through MQTT subscriptions, thereby supporting operational monitoring and explainability of adaptive access-control outcomes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

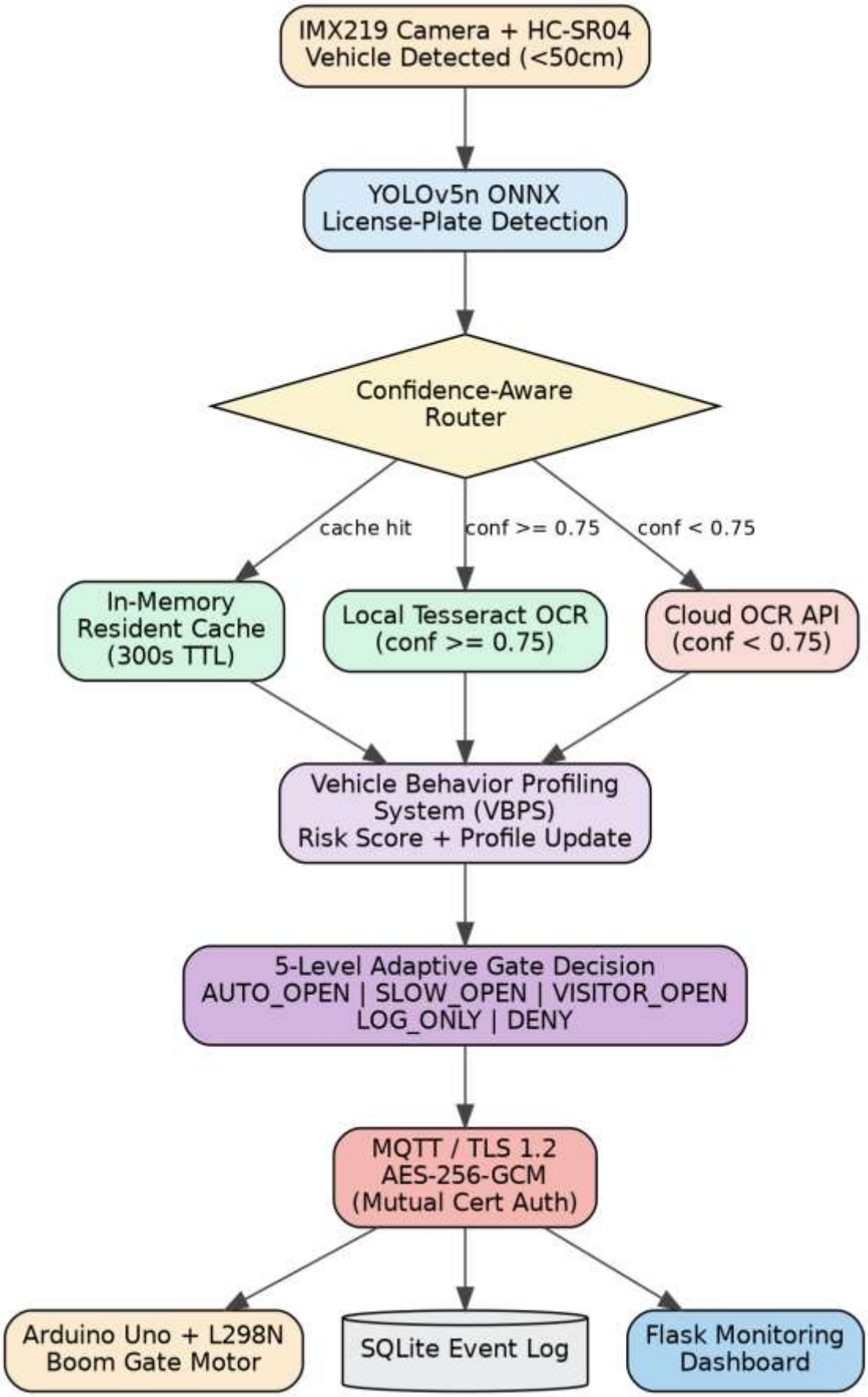

Fig. 1. Overall system architecture: sensor-triggered capture, YOLOv5n detection, confidence-aware routing across cache/edge/cloud OCR, VBPS risk scoring, five-level gate decision, and TLS-secured MQTT distribution to the gate, database, and dashboard.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

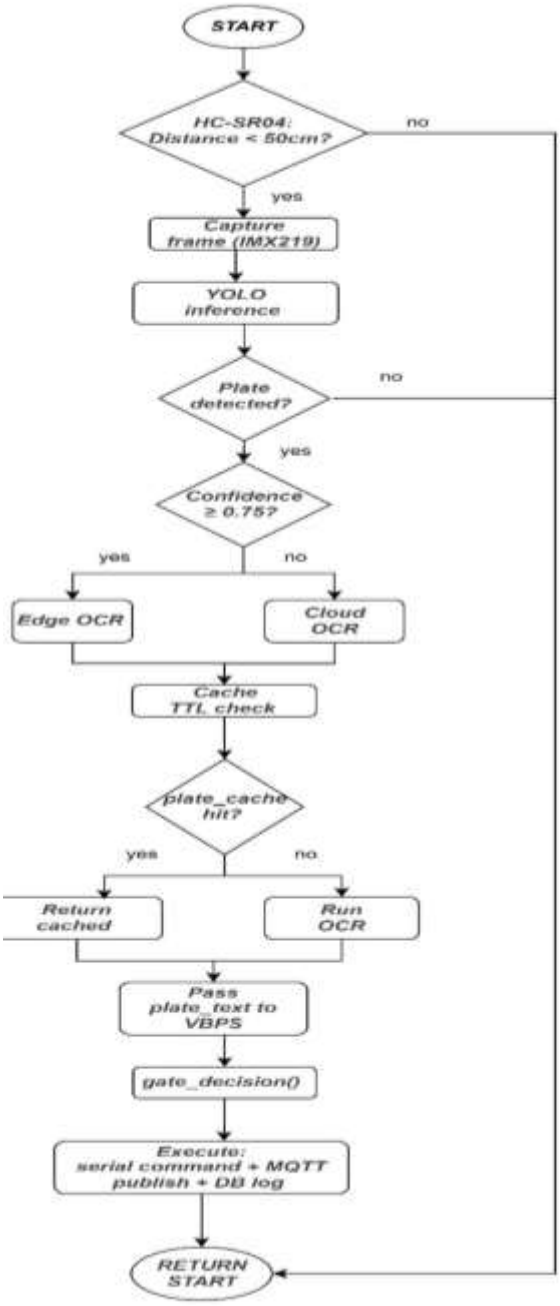

Fig. 2. Hybrid ALPR + VBPS decision flow, showing the three OCR paths (cache, edge, cloud) and the route from plate text to the final gate decision

IMPLEMENTATION AND EXPERIMENTAL METHODOLOGY

The final prototype was implemented as a standalone Raspberry Pi 5 (8 GB) system integrating an IMX219 8 MP CSI camera for image acquisition, an HC-SR04 ultrasonic sensor for vehicle detection and capture triggering, and an Arduino Uno with an L298N motor driver for controlling a 3D-printed boom gate. The Raspberry Pi executes the complete software stack, including YOLO-based detection, confidence-aware OCR routing, cache management, Vehicle Behavior Profiling System (VBPS), secure MQTT communication, database logging, and dashboard services, implemented through modular Python components and system services. During deployment, the system recorded 433 gate events involving 98 unique plates, comprising 12 residents, 85 visitors, and three blacklisted vehicles, with 145 anomalous events identified; additional structured evaluation included 15 temporal and 30 behavioral anomaly scenarios. Performance was assessed using plate-detection mAP, cache hit rate, cloud API reduction, weighted processing latency, external image

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

transmission, false-denial rate, access-control requirement coverage, behavioral anomaly precision, and trust-scoring accuracy, while security evaluation examined unauthorized clients, message interception, replay attacks, and unauthorized command publication. System-level evaluation additionally considered environmental robustness, decision latency, and power consumption, providing end-to-end validation from ALPR recognition and behavioral analysis to secure cyber-physical gate operation.

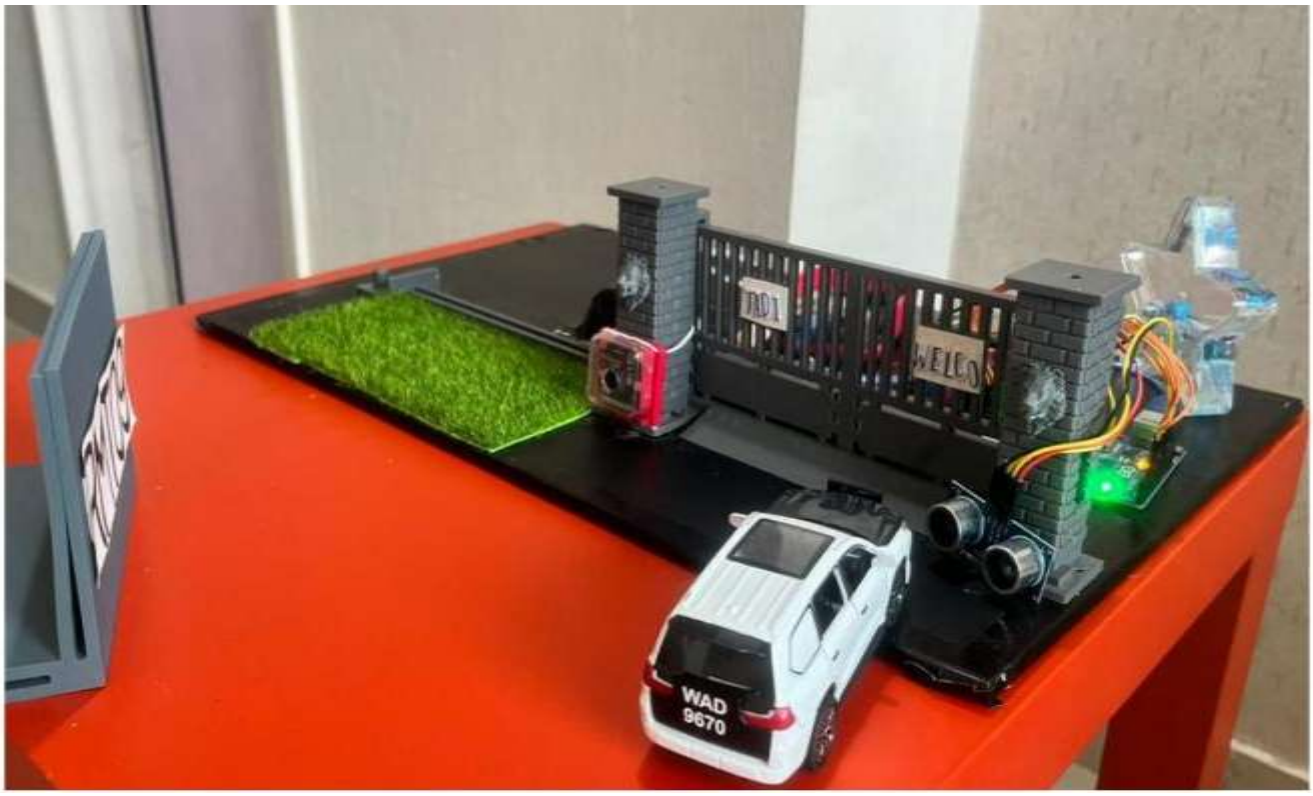

Fig. 3. Deployed physical prototype: Raspberry Pi 5, IMX219 camera, HC-SR04 sensor, and 3D-printed boom-gate assembly.

RESULTS

The deployed YOLOv5n ONNX detector achieved **97.3% plate detection mAP** with a model size of approximately **7.4 MB**, exceeding the 92% target and the 90.3% reference value for challenging edge ALPR conditions. The confidence-aware processing pipeline achieved a **61% cache hit rate**, with **29.9% of events requiring cloud OCR** and a reported **96.7% reduction in cloud API usage**, while cache lookup averaged **2.8 ms**. The complete evaluated recognition workflow achieved a **749 ms weighted average latency**, although the original <150 ms target was not met; importantly, VBPS decision computation required only **0.52 ms**, indicating negligible behavioral-processing overhead. The proposed behavior-aware architecture reduced the false-denial rate from **51.3% in the evaluated baseline configurations to 3.6%**, representing an approximately **93% improvement**. Across **15 structured temporal and 30 behavioral scenarios**, VBPS achieved **100% anomaly-detection precision** with zero false positives in the evaluated scenarios, while satisfying **12/12 access-control requirements**, compared with **2/12** for the baseline systems; the implemented trust-scoring approach also achieved **100% accuracy**, compared with **94.3%** for the cited DEBAC benchmark. Security evaluation covering unauthorized clients, interception/MITM, replay, and forged command publication was successfully passed using **TLS 1.2, AES-256-GCM, and mutual certificate authentication**. Environmental testing showed OCR-related performance improvement from **87.4% to 95.1%** under the evaluated night-and-cache condition, while the complete prototype operated at approximately **5–8 W**. Overall, the results demonstrate that hybrid ALPR, resident-aware caching, lightweight behavioral profiling, adaptive access control, and secure IoT communication can be integrated effectively on Raspberry Pi 5 hardware, while the **749 ms end to end latency and limited structured evaluation dataset** indicate areas requiring further optimization and larger-scale real-world validation.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

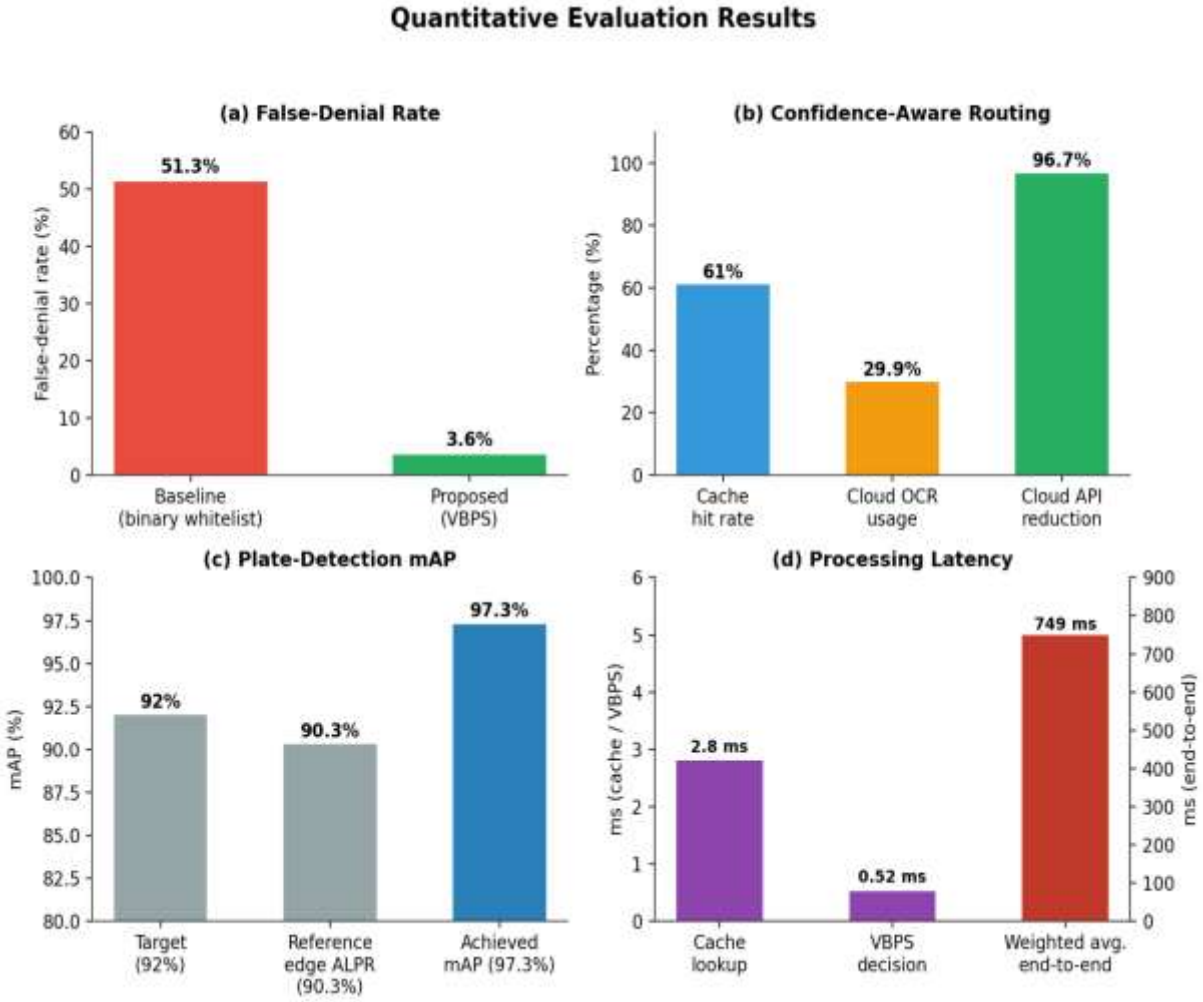

Fig. 4. Quantitative evaluation results: (a) false-denial rate reduction, (b) confidence-aware routing efficiency, (c) plate-detection mAP against target/reference values, and (d) processing latency breakdown.

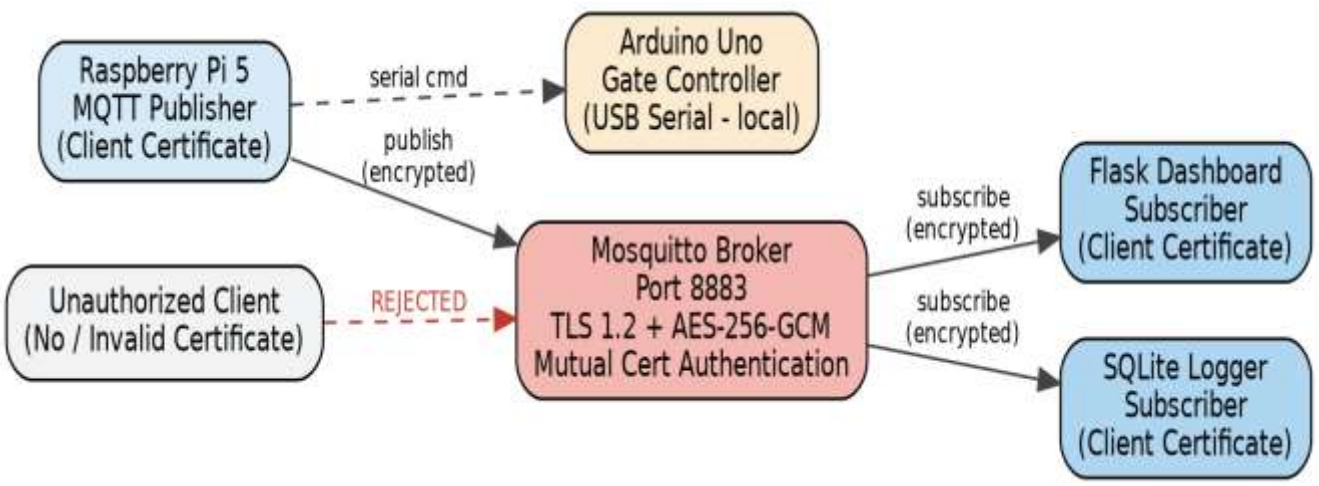

Fig. 5. Security architecture: TLS/MQTT broker mediating authenticated communication between the Raspberry Pi publisher, dashboard and logger subscribers, with unauthorized clients rejected.

LIMITATIONS, SCOPE, AND THREATS TO VALIDITY

The proposed system was evaluated using a single-site deployment comprising 433 gate events and 98 unique plates, supplemented by 45 structured behavioural scenarios. While sufficient to demonstrate architectural

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

feasibility, this dataset does not capture the full variability of real residential environments, including lighting, weather, camera angle, vehicle type, and naturally occurring anomalies. The reported metrics are based on a single evaluation run and therefore do not quantify experimental variability or confidence beyond the reported intervals. Furthermore, the measured 749-ms weighted latency exceeds the original 150-ms target, primarily due to cloud-OCR processing and network overhead, motivating path-specific latency analysis. Comparative evaluation is also limited using an externally reported DEBAC benchmark. Security testing was restricted to MQTT communication threats and did not include physical tampering, firmware compromise, adversarial plate presentation, denial-of-service, or serial-link attacks. Future work will address these limitations through multi-site deployments, repeated trials, larger naturalistic datasets, and expanded security evaluation.

CONCLUSION

This paper presented a behavior-aware hybrid edge–cloud ALPR architecture for secure residential gate access control, integrating license plate detection, confidence aware OCR routing, resident aware caching, vehicle behavior profiling, adaptive gate decisions, secure MQTT/TLS communication, and real-time monitoring on a Raspberry Pi 5. Experimental evaluation demonstrated **97.3% detection mAP**, a **61% cache hit rate**, **29.9% cloud OCR usage**, and a reported **96.7% reduction in cloud API usage**, with a **749 ms weighted average processing latency** and only **0.52 ms VBPS decision latency**. The behavior-aware architecture reduced the measured false denial rate from **51.3% to 3.6%**, achieved **100% precision** across the evaluated structured temporal and behavioral anomaly scenarios, and satisfied **12/12 access control requirements**, while all four evaluated security tests covering unauthorized clients, interception, replay, and forged-command publication were successfully passed. The primary contribution is an integrated access-control architecture in which recognition confidence, vehicle history, behavioral risk, privacy, and communication security collectively influence gate operation rather than relying solely on static plate recognition. Despite these results, the prototype remains limited by its **749 ms end to end latency**, relatively small evaluation dataset, and reliance on structured behavioral scenarios; therefore, it should be considered a validated prototype rather than a production-ready security system. Nevertheless, the findings demonstrate the feasibility of combining hybrid ALPR, behavior-aware access control, and secure IoT communication on constrained hardware while reducing dependence on continuous cloud processing, providing a practical foundation for future residential gate systems that balance recognition performance, privacy, security, computational efficiency, and adaptive decision-making.

REFERENCES

1. Al-Batat et al., “An end-to-end automated license plate recognition system using YOLO based vehicle and license plate detection with vehicle classification,” Sensors, vol. 22, no. 23, 2022.
2. Al-Batat et al., work on constrained edge ALPR optimization, Journal of Real-Time Image Processing, 2022.
3. Al-Hasan et al., work on enhanced YOLO-based automatic number plate recognition, Technologies, 2024.
4. Al-Hasan et al., work on robust CNN-based automatic number plate recognition under challenging environmental conditions, Sensors, 2024.
5. Leng et al., work on hybrid/cloud-assisted ALPR processing and latency/cloud-utilization optimization, 2023.
6. Cabanillas Rodríguez et al., “DEBAC” behavioral/trust-based access-control work, EuCNC, 2025.
7. Cabanillas et al., work on behavioral anomaly detection and access control, Future Generation Computer Systems, 2025.
8. Duong et al., deep-learning anomaly-detection survey and vehicle/behavioral anomaly literature, Sensors, 2023.
9. Farhadighalati et al., systematic work on behavioral and access-control requirements, IEEE Access, 2025.
10. Janati and Messaoudi, behavior-based intrusion/anomaly detection using frequency, timing, and deviation signals, International Journal of Advanced Computer Science and Applications, 2025.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IX, September 2026

11. Kaveh et al., hybrid time-series/anomaly detection approach, Symmetry, 2025.
12. Landauer et al., review of time-series methods for anomaly detection, International Journal of Information Security, 2025.
13. Pathirannahalage et al., real-time surveillance and anomaly-detection architecture, Multimedia Tools and Applications, 2024.
14. Vardakis et al., analysis of security vulnerabilities in smart-home and IoT systems, 2024.
15. Zia et al., transformer/adversarial approaches to anomaly detection on constrained IoT devices, Electronics, 2025.
16. Tao et al., work on robust/optimized ALPR processing under challenging image conditions, 2024.
17. Zhang et al., work addressing image degradation and robustness in ALPR, 2024.
18. Elmetwally et al., real-time abnormal-event detection using temporal video information, Multimedia Tools and Applications, 2024.