Development of an Access Control System for Monitoring Vehicle Movement using Computer Vision and Token-Based Authentication

Akintoye A. Onamade[1*], Benjamin Francis Daria1[1], Taiwo Gabriel Aboderin[2], Ilerioluwa Israel Fagbayike[3], Saheed Opeyemi Abioye[4], Jeremiah Ademola Balogun[5], Olusegun Gbenga Lala[6]

onamadeakintoye@adelekeuniversity.edu.ng, benjamin.daria@cpgs.adelekeuniversity.edu.ng, taiwo.aboderin@cpgs.adelekeuniversity.edu.ng, ilerioluwa.fagbayike@cpgs.adelekeuniversity.edu.ng, saheed.abioye@cpgs.adelekeuniversity.edu.ng, balogun.jeremiah@adelekeuniversity.edu.ng, olusegun.lala@adelekeuniversity.edu.ng

Abstract

Securing vehicle access points in places like corporate organisations, university campuses, markets, and residential buildings has long been a challenge. Most existing systems either rely totally on manual checks, which are slow and error-prone, or single-phase methods such as RFID cards that can be cloned. Neither approach offers the security and efficiency that modern environments require. This study addresses that gap by developing an Automated Vehicle Access Control System (AVACS) that combines two phases of verification: Automatic Number Plate Recognition (ANPR) and token-based authentication. Rather than relying on a single phase, the system requires both a valid vehicle plate for entry and an authenticated token for exit, making it significantly harder to bypass. On the technical side, the system uses YOLOv8n for real-time vehicle detection, EasyOCR/Tesseract for plate number character recognition, and a FastAPI backend paired with a React/Tailwind frontend. Data is stored in MongoDB Atlas, and the ANPR component was trained to handle Nigerian Standard Plate Number formats, an area that has been largely underserved in existing research. The system was evaluated on key performance indicators, including recognition accuracy, authentication response time, and overall reliability. Results demonstrated that the integrated multi-phase approach outperforms single-phase systems in both security and operational efficiency, while also providing better audit trails for incident tracking. This work contributes to the growing body of research on vehicle access control. It lays a foundation for future exploration of multi-factor vehicle authentication in smart infrastructure and IoT environments.

Keywords: Vehicle Access Control, Computer Vision, YOLOv8n, Deep Learning

1. Introduction

As vehicle traffic increases across corporate organisations, residential estates, industrial facilities, and logistics centres, the need for more secure and efficient vehicle access control systems has become increasingly important. Traditional approaches, such as manual verification, paper-based logging, and single-factor authentication methods like Radio Frequency Identification (RFID) cards, are becoming inadequate for modern security demands. These systems are vulnerable to human error, tailgating, credential sharing, cloning attacks, and poor audit tracking, particularly in high-traffic environments [1], [2].

Recent advances in Computer Vision and Machine Learning have enabled the development of Automatic Number Plate Recognition (ANPR) systems for automated vehicle identification. ANPR systems use deep learning and Optical Character Recognition (OCR) techniques to detect and extract license plate information in real time [3], [4]. Although these technologies improve automation and reduce dependence on manual processes, many existing systems still rely on a single verification mechanism, making them vulnerable to spoofing and unauthorised access. In addition, limited attention has been given to systems designed specifically for Nigerian license plate formats and challenging environmental conditions such as low lighting, occlusion, and varying camera angles.

To address these gaps, this study proposes a hybrid vehicle access control system that combines Automatic Number Plate Recognition (ANPR) with token-based authentication. The system integrates YOLOv8n for vehicle detection, OCR for license plate extraction, and JSON Web Token (JWT)-based verification for secure vehicle authentication. By combining visual identification with token validation, the proposed system aims to improve security, reduce unauthorised access, and provide reliable audit tracking. The system is evaluated using recognition accuracy, authentication latency, and overall operational reliability to determine its suitability for real-world deployment in controlled environments such as university campuses, residential estates, and corporate facilities.

2. Related Work

From conventional RFID-based solutions to cutting-edge computer vision techniques, vehicle access control systems have been thoroughly investigated in both academic and industrial domains. Existing works can be broadly categorised into three main groups: sensor-based authentication, vision-based recognition, and hybrid systems combining multiple modalities.

2.1 Sensor-Based Authentication Systems

Radio Frequency Identification (RFID) systems remain one of the earliest widely deployed technologies for vehicle access control. RFID enables contactless vehicle identification using tags attached to vehicles and readers installed at entry points. These systems provide fast authentication and reduce congestion at checkpoints.

Recent studies highlight that RFID continues to be used in smart parking and controlled facility access due to its low latency and simplicity [5], [6]. However, its limitations have become more pronounced in large-scale and security-critical environments. RFID systems are highly vulnerable to tag cloning, relay attacks, and unauthorized signal interception, especially when low-cost passive tags are used [7].

Furthermore, recent security analyses show that many deployed RFID access systems still rely on weak or outdated encryption protocols, making them susceptible to spoofing and replay attacks [8]. Deployment scalability also remains a challenge, as infrastructure costs increase significantly in dense urban environments requiring multiple readers and redundancy mechanisms. These limitations have driven the transition toward more intelligent and adaptive recognition systems

2.2 Vision-Based Recognition Approaches

Vision-based systems, particularly Automatic License Plate Recognition (ALPR), have gained significant traction due to advancements in deep learning. Early ALPR systems relied on handcrafted features such as edge detection, morphological processing, and template matching, which were sensitive to noise and lighting variations.

Recent deep learning-based approaches using architectures such as YOLO and Transformer-based detectors have significantly improved detection accuracy and inference speed [9], [10]. For example, YOLO-based models have demonstrated strong real-time performance in unconstrained environments, making them suitable for intelligent transportation systems.

Despite these advancements, several limitations persist:

- Poor generalisation across regions: Models trained on public datasets often fail when applied to local plate formats due to domain shift [10].
- Environmental sensitivity: Performance drops significantly under low light, motion blur, and occlusion conditions.
- OCR dependency limitations: Tools such as Tesseract and EasyOCR still struggle with non-standard fonts, dirty plates, and region-specific formatting variations [11].
- Dataset bias: Most datasets used in prior work are not representative of African or developing-country plate structures, leading to reduced real-world reliability [12].

2.3 Hybrid and Multi-Phase Systems

Recognising the limitations of single-modality approaches, several researchers have investigated hybrid systems combining multiple authentication factors. [6] Designed a system combining ANPR with RFID, while [17] studied the use of JWT tokens in access control. Blockchain-based systems have also emerged, allowing decentralised authentication with increased security assurances [8]. These systems demonstrate greater security, but frequently at the cost of additional complexity and computational cost.

The system is distinct from existing techniques in several major aspects. First, it combines the precision of modern deep learning-based plate recognition with token validation, addressing both identity and authentication difficulties. Second, the system is specifically designed for Nigerian plate formats and environmental conditions, incorporating preprocessing techniques to handle local variations. Third, the token issuance and verification process offers a secure and lightweight substitute for conventional multi-Phase systems, allowing for effective implementation in environments with limited resources. This integration of computer vision and token-based authentication represents a novel contribution to the field of automated vehicle access control.

2.4 Critical Synthesis and Research Gap

Although significant progress has been made in vehicle access control systems, existing approaches still suffer from a combination of security, adaptability, and deployment constraints.

Therefore, there is a clear need for a lightweight, secure, and region-adaptive system that combines the accuracy of deep learning-based license plate recognition with efficient authentication mechanisms suitable for real-world deployment in developing regions.

Table 1: Comparative Analysis

Study/Reference	Approach	Major Limitation	Improvement in Proposed System
Juels [18]	RFID authentication	Cloning and replay attacks	Adds ANPR-based visual verification
Ng et al. [19]	RFID parking management	High infrastructure cost and tag dependency	Multi-factor authentication with JWT
Mufti and Shah [20]	Traditional ANPR	Poor low-light and occlusion performance	YOLOv8n-based robust detection
Al-Hasan et al. [22]	YOLOv8 ANPR	High computational demand	Lightweight deployment design
Moussaoui et al. [23]	YOLOv8 + OCR	Sensitive to image quality	Enhanced preprocessing and token validation
Siddiqui et al. [24]	Hybrid recognition system	Increased processing overhead	Faster JWT-based authentication
Proposed CVT-AVACS	YOLOv8n + OCR + JWT	Low-light performance challenges	Nigerian plate adaptation and scalable design

3. Methodology

Automated vehicle access control systems rely on several core technologies that enable accurate identification and authentication. These components form the foundation for the proposed token-based access control system, ensuring reliable performance across diverse operational conditions.

3.1 Object Detection for Vehicle Localisation

Modern vehicle recognition pipelines begin with object detection to localise vehicles within an input frame. The YOLO (You Only Look Once) architecture has become a standard choice due to its real-time performance and high accuracy [13]. Unlike traditional sliding-window approaches, YOLO frames detection as a regression problem, predicting bounding boxes and class probabilities in a single pass. This efficiency is critical for access control applications where low latency is essential. Recent iterations, such as YOLOv8n, further optimise computational efficiency while maintaining detection accuracy, making them suitable for edge deployment [14].

3.2 Optical Character Recognition for License Plate Extraction

Once a vehicle is detected, Optical Character Recognition (OCR) techniques extract textual information from license plates. Early OCR systems relied on handcrafted features and template matching, but modern approaches leverage deep learning for improved robustness [15]. Convolutional Recurrent Neural Networks (CRNNs) have proven particularly effective, combining convolutional layers for spatial feature extraction with recurrent layers for sequence modelling. For non-Latin scripts or region-specific plate formats, specialised OCR models are often required to handle unique character sets and layouts [16].

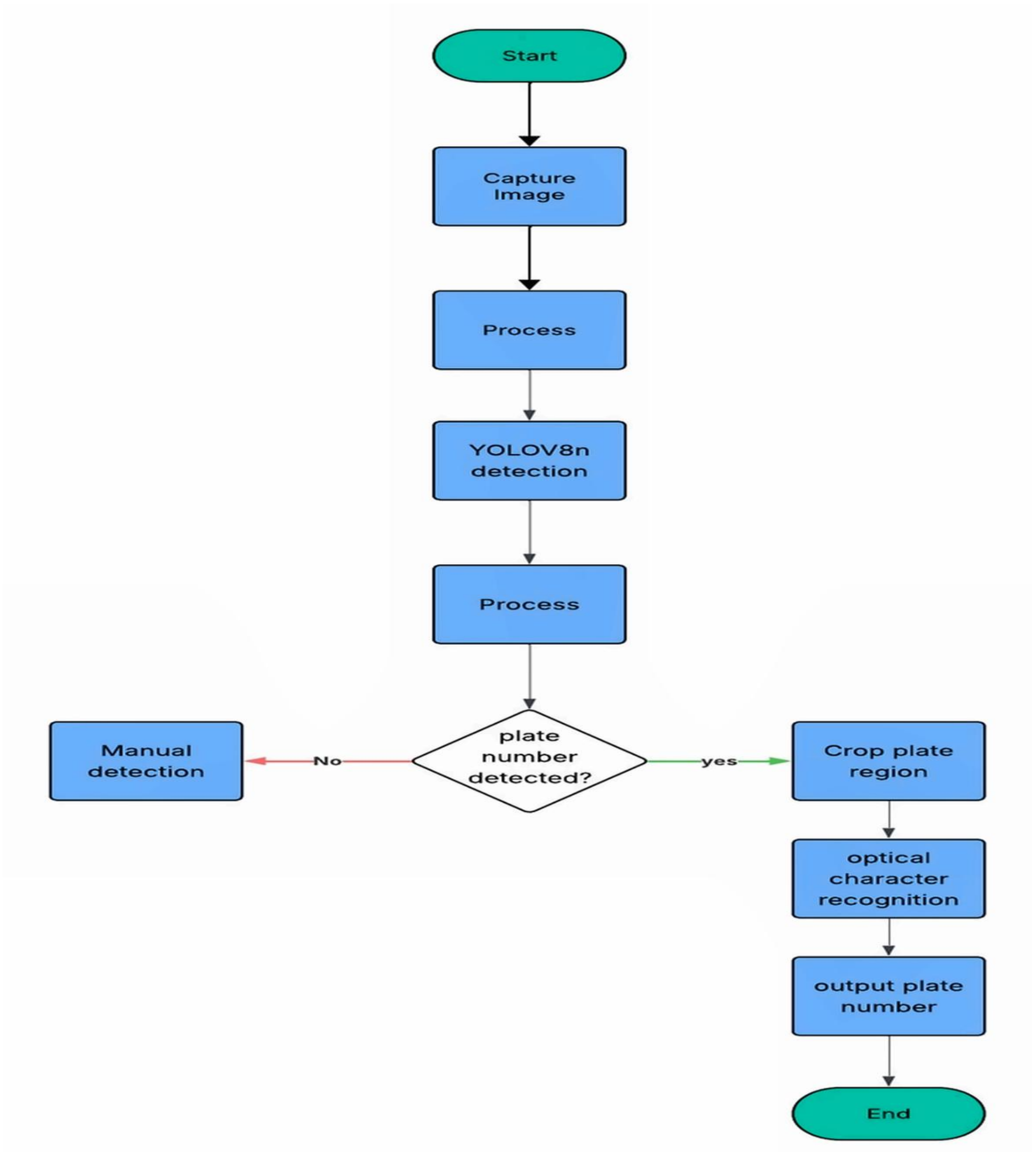

Figure 1: Image Recognition flow

3.3 Token-Based Authentication Mechanism

The token issuance process in AVACS ensures that each authorised vehicle receives a unique, time-bound digital credential for access. Tokens are generated, delivered, and verified using secure algorithms. JSON Web Tokens (JWT) have emerged as a lightweight standard for token-based authentication, encoding claims in a compact JSON format [17]. A JWT typically consists of three components: a header specifying the signing algorithm, a payload containing claims (e.g., vehicle ID, expiration time), and a signature for verification.

3.3.1 Algorithm for Token Issuance (JWT-Based)

Algorithm Steps:

1. **Capture plate number**
    i. Assign parking space
    ii. Store information in the database.
2. **Token Generation**
    i. Generate a unique token (JWT) associated with the vehicle.
    ii. Embed expiry time and metadata in the token.
3. **Token Delivery**
    i. Display token in the dashboard.
    ii. In a simulated environment, the delivery is logged in the console.
4. **Token Verification**
    i. Upon vehicle exit, the token is presented.
    ii. Backend verifies token validity and expiry.
    iii. Parking slot is released
    iv. If valid, the token is passed to the decision engine; otherwise, exit is denied.

Pseudocode:

```
function issueToken(userID, vehiclePlate):
   token = generateJWT (userID, vehiclePlate, expiryTime)
   storeTokenInDB(token, userID, vehiclePlate)
   sendTokenToUser(token)
   return token

function verifyToken(token, vehiclePlate):
   if token.isValid() and token.notExpired():
      if token.vehiclePlate == vehiclePlate:
         return AccessGranted
      else:
         return AccessDenied
   else:
      return AccessDenied
```

3.4 NPR Pipeline Hardening and OCR-Tolerant Validation

During system implementation and iterative testing, several critical deficiencies were identified in the initial NPR pipeline that adversely affected plate detection rates under real-world imaging conditions. These deficiencies, and the architectural decisions taken to address them, are documented in this sub-section as they constitute an integral part of the implemented methodology.

3.4.1 Failure Class 1: Validator false rejections due to erroneous year-code enforcement

The original Nigerian Plate Validator applied a secondary constraint that required the penultimate character of a standard plate to belong to the set {A, B, C…, O}, corresponding to the years 2011-2025. This check was based on a misinterpretation of FRSC plate anatomy: the last two alphanumeric characters of the standard ABC-123DE format are serial batch codes, not year or batch indicators visible on the plate face (FRSC, 2012). As a result, any plate whose serial suffix contained letters outside that set (e.g., PJK-273VB, where V does not belong to {A-O}) was incorrectly rejected with an "Invalid plate format" error. This constraint was removed entirely from the updated validator.

3.4.2 Failure Class 2: OCR output concatenation producing multi-word strings

The initial implementation concatenated all text boxes returned by EasyOCR into a single string before applying character-level filtering: full_text = ''.join(results). When the webcam captured a frame that included surrounding interface text or environmental labels alongside the plate, all detected text regions were merged into a single string of 30-60 characters. The subsequent length validation (5-12 characters) then correctly, but unhelpfully, rejected this merged string. The plate number was present within the merged output but could not be individually identified.

3.5 Architectural Corrections Applied

3.5.1 Per-box OCR evaluation (EasyOCR detail=1 mode)

The OCR invocation was modified from detail=0 mode, which returns a flat list of strings, to detail=1 mode, which returns a list of tuples in the form (bounding_box, text, confidence) for each detected text region. Each box is evaluated independently against the Nigerian plate validator prior to any string concatenation. This ensures that even when the frame contains multiple text regions, the plate number which occupies exactly one bounding box is identified and extracted correctly, while surrounding text regions that fail format validation are discarded.

3.5.2 Plate-zone cropping before OCR

A pre-processing function, crop_plate_zone(), was introduced to crop the input frame to the centre-bottom 75% of the image before OCR is applied, consistent with the typical position of a vehicle plate in the camera field of view at an access gate. This spatial filter reduces the number of non-plate text regions available to EasyOCR, thereby decreasing the probability of false text-box matches and reducing total OCR computation time.

3.5.3 YOLO confidence threshold reduced and decoupled.

The YOLO inference confidence threshold was reduced from the default 0.25 to 0.15 and made configurable via an environment variable (YOLO_CONF). The original implementation also applied a secondary threshold check (settings.CONFIDENCE_THRESHOLD) after YOLO inference, resulting in a double-filter that silently discarded valid low-confidence detections. The secondary check was removed; a single configurable threshold now governs both the YOLO inference pass and the detection acceptance decision.

3.5.4 Full-image OCR fallback for YOLO-miss scenarios.

In cases where YOLO does not return a plate bounding box above the confidence threshold which can occur when the vehicle presents the plate at an unusual angle or when the active YOLO weights are a general-purpose object detector rather than a specialised plate-detection model the pipeline now proceeds to apply the smart OCR scan function to the cropped plate zone of the full image as a fallback path. This ensures that the pipeline does not terminate without attempting character recognition when a plate is visible in the frame.

4. System design

The proposed system establishes an end-to-end pipeline for vehicle access control by integrating computer vision with token validation. As shown in Figure 2 below, the architecture consists of two parallel workflows for entry and exit processes, connected through a centralised authentication server. The system operates in three phases: vehicle identification through plate number recognition, token issuance upon entry, and token verification at the exit point.

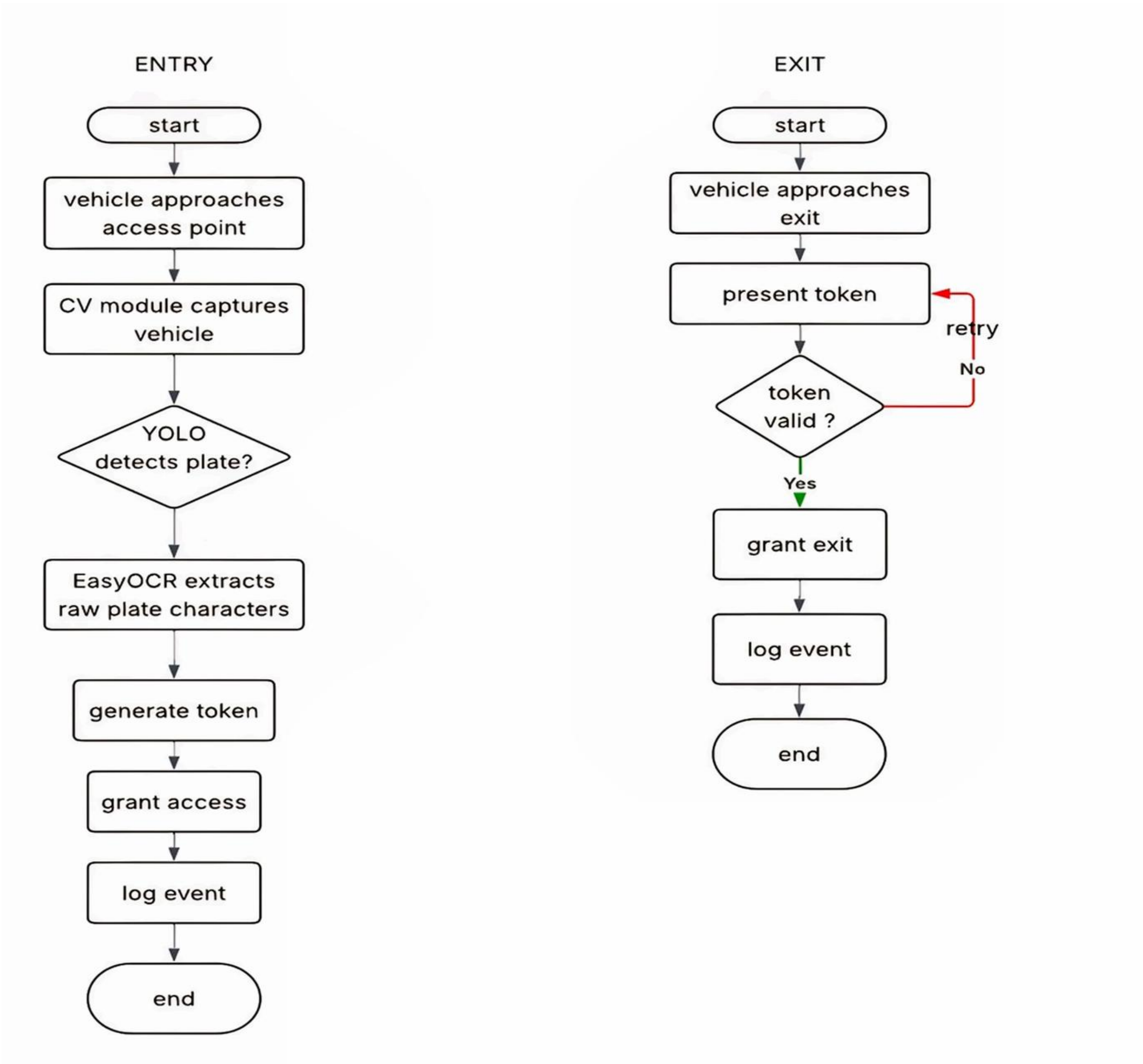

Figure 2: Multi-Phase Verification Flow

5. Experimental setup and results

To validate the proposed Computer Vision and Token-Based Vehicle Access Control System (CVT-VACS), Comprehensive experiments were conducted to evaluate both the computer vision components and the token authentication pipeline. The system was tested under various operational conditions to assess its robustness, accuracy, and efficiency in real-world deployment scenarios.

5.1 Dataset and Preprocessing

The evaluation utilised a dataset of 1797 Nigerian license plate images collected from multiple locations under varying environmental conditions. The dataset was partitioned into 1597 training samples and 200 test cases covering four challenging scenarios:

Preprocessing involved noise reduction using OpenCV's non-local means denoising. Images were resized to 640 x 640 pixels using YOLOv8n's letterboxing technique to preserve aspect ratios while maintaining consistent input dimensions for the neural networks. Pixel values were normalised to the [0, 1] range by dividing by 255.

Table 2: Test Dataset Distribution

Test category	Number of cases	Description
Clear plate, good lighting	100	Standard daylight conditions, plate clearly visible
Partial occlusion	30	Plate partially covered by dirt, frame, or shadow
Low light/night simulation	35	Reduced brightness, simulated evening conditions
Varied angles	35	Camera positioned at a 15-30 degree angle from the plate
Total	200	

5.2 Implementation Details

The system was implemented on a hardware configuration comprising:

- NVIDIA RTX 3060 GPU (8GB RAM)
- Intel Core i7-11800H CPU
- 12GB DDR4 RAM

Software components included:

- YOLOv8n (ultralytics v8.0.0) for vehicle detection
- EasyOCR (V1.6.2) configured for English character recognition
- FastAPI (v0.95.0) backend with JWT authentication
- MongoDB Atlas for cloud-based data storage

5.3 System dashboard

The system dashboard, as shown in Figure 3, serves as the main entry point for administrators and operators. It provides a summary of system statistics, including total registered vehicles, tokens issued, today's access attempts, and the current authentication success rate.

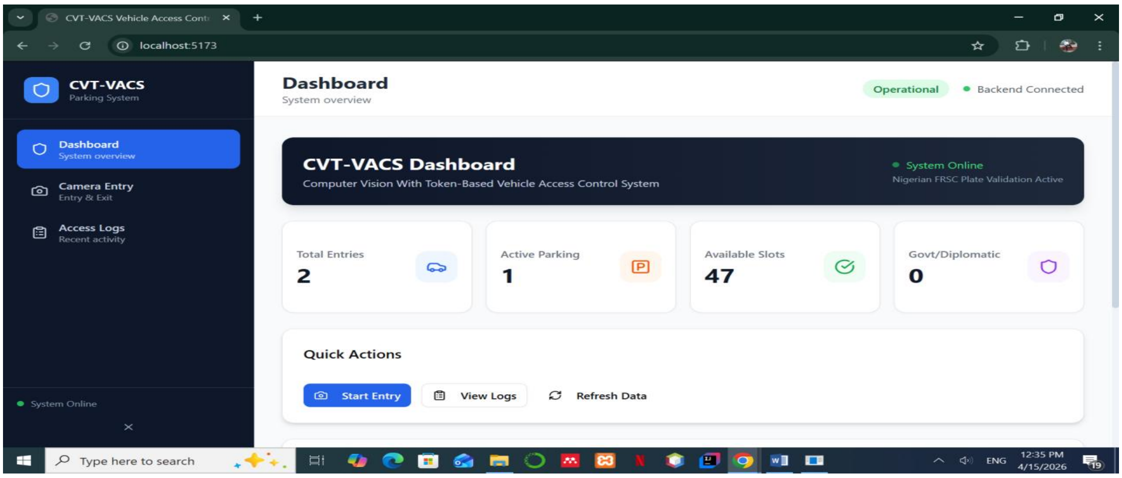

Figure 3: CVT-VACS System Dashboard

The Camera Entry module, as shown in Figure 3, implements a supervised automation approach where the security operator initiates the capture process upon visual confirmation of vehicle presence.

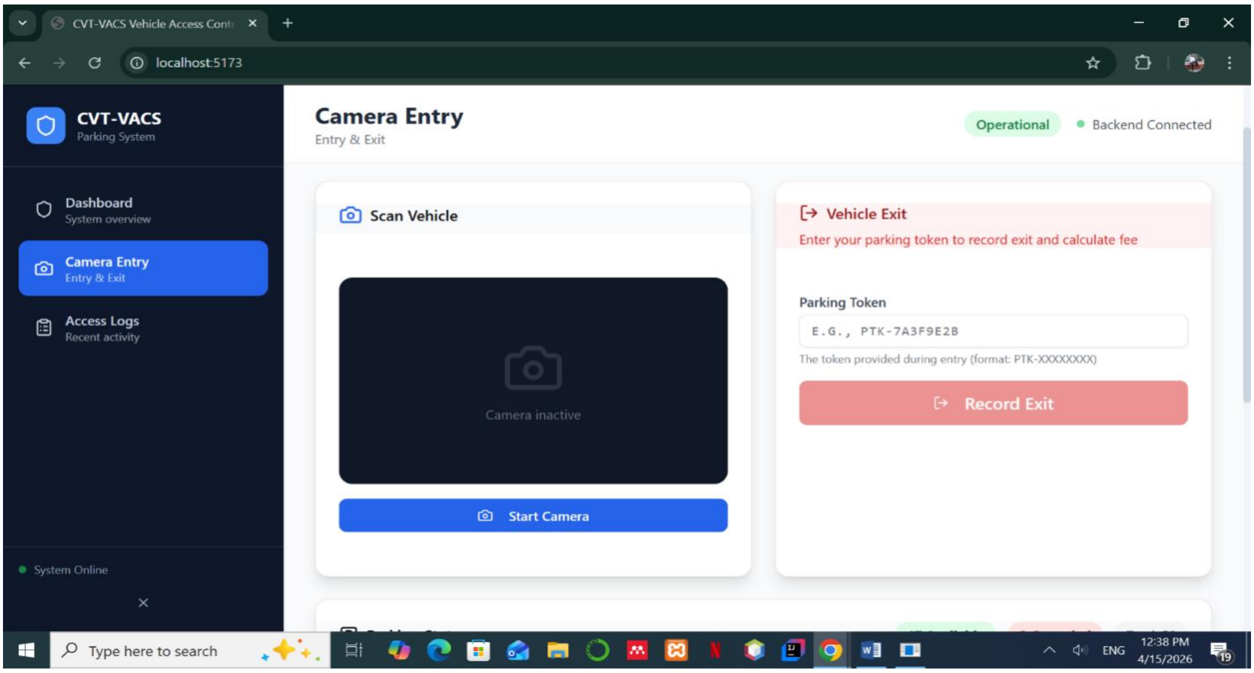

Figure 4: Camera Entry Module showing live camera feed

A manual entry fallback is also provided for situations where camera-based recognition fails, such as in poor lighting or with heavily soiled plates. Figure 5 illustrates the manual entry interface.

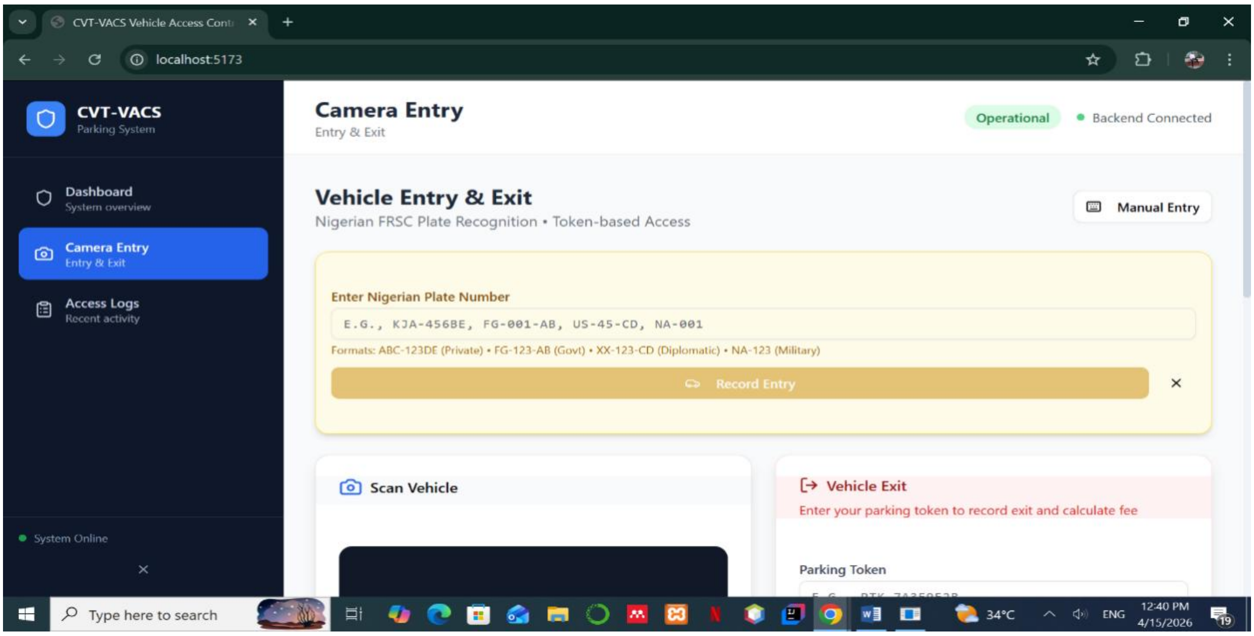

Figure 5: Manual entry fallback panel for low-visibility conditions

Figure 6 shows the vehicle exit management module. A security operator enters the departing vehicle's token, which triggers the slot release routine in the database. Occupied slots are displayed in red with a colour dot indicating the detected vehicle colour, while unoccupied slots are shown in green.

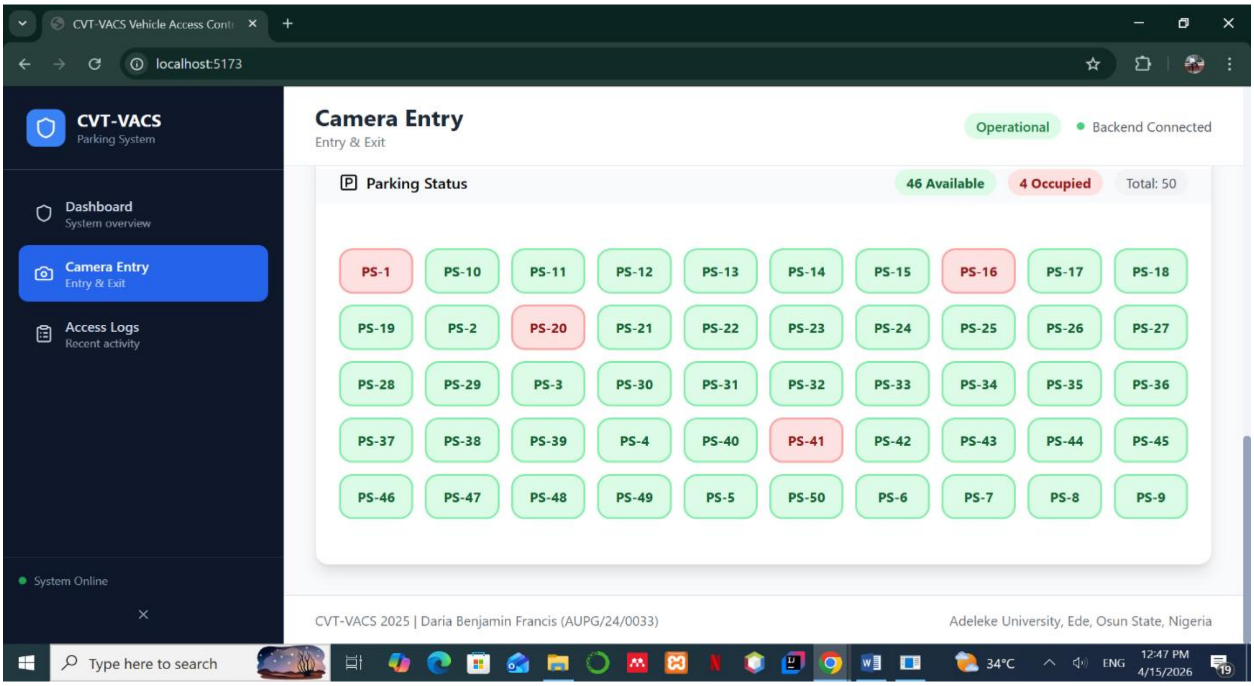

Figure 6: Live parking grid displaying real-time slot occupancy

The Access Logs module, shown in Figure 7, provides a full audit trail of all access attempts processed by the system. Each log entry records the timestamp, plate number, access decision (GRANTED or DENIED), token validity status, plate match result, ANPR confidence, and total response time.

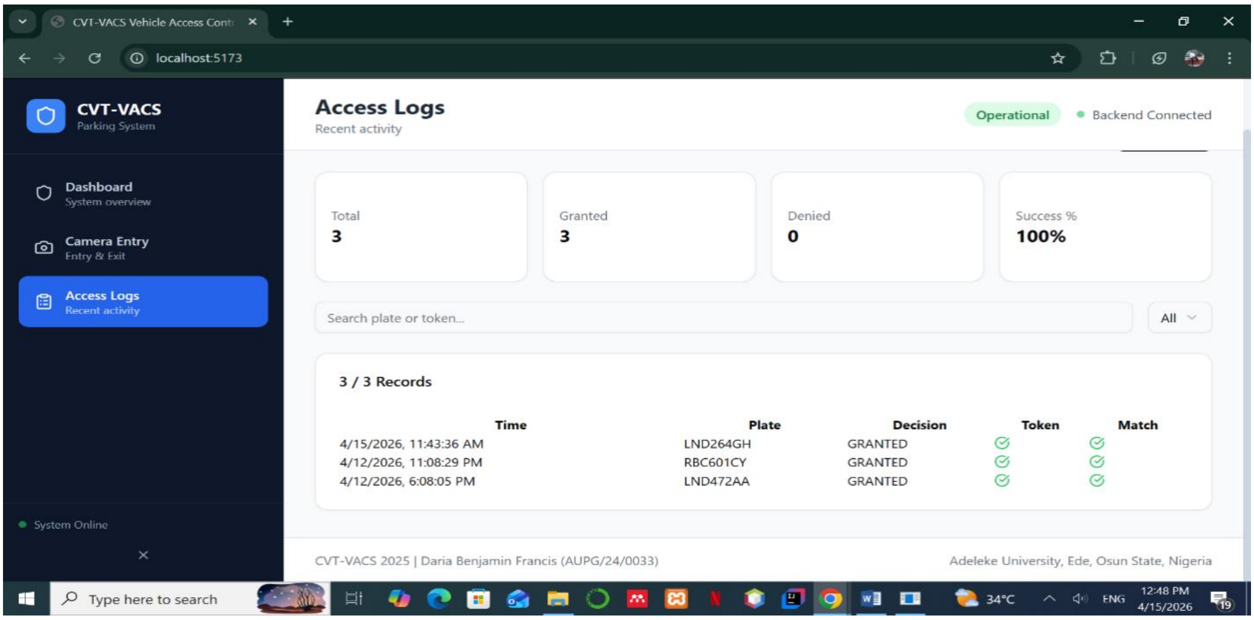

Figure 7: Access Logs Module showing access audit trail

5.3 Performance Evaluation Results

The system was evaluated using 9 key metrics: ANPR Accuracy, Precision, Recall, F1 Score, Token Verification Latency, System Response Time, Authentication Success Rate, Throughput, and Colour Detection Accuracy.

Table 3: ANPR accuracy by test condition

Condition	Samples	Correct	Accuracy
Clear	100	94	94%
Occluded	30	27	90%
Low-light	35	30	87.5%
Angled	35	32	91.42%
Overall	200	183	91.5%

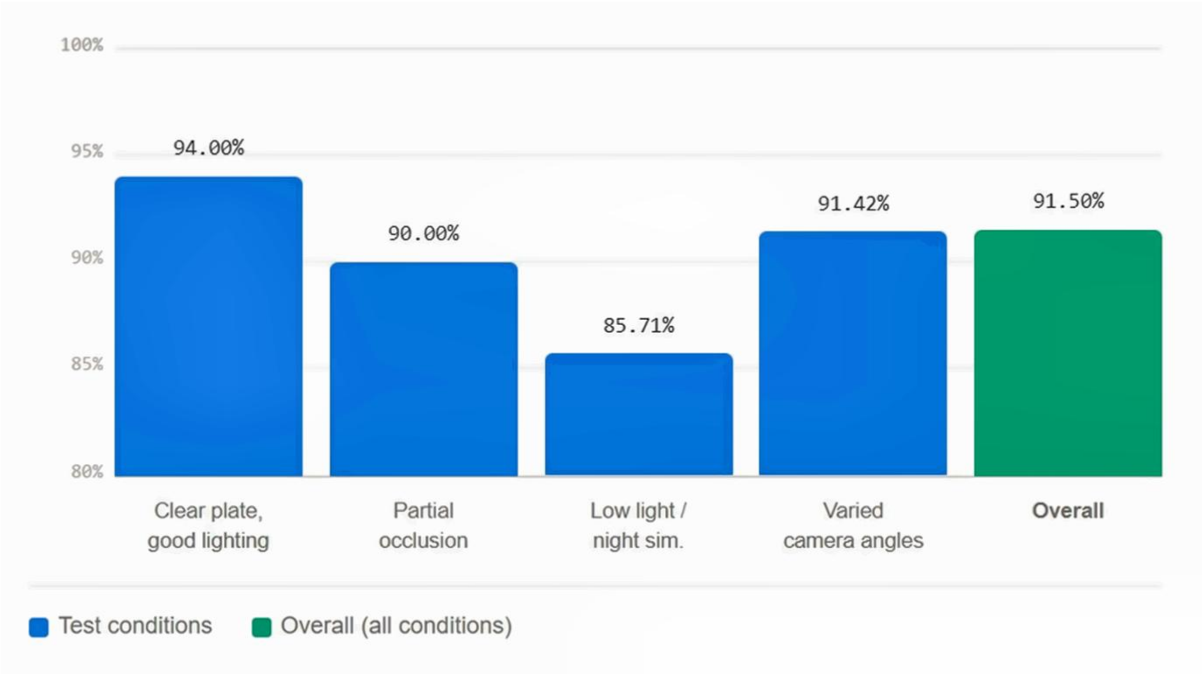

Figure 8: ANPR recognition accuracy across test conditions

Table 4: Systems performance across all evaluation metrics

Metric	Value	Target
ANPR Accuracy	91.5%	≥ 90%
Precision	91.5%	≥ 88%
Recall	95.6%	≥ 88%
F1 Score	93.5%	≥ 88%
Token Latency	18.4ms	<50ms
Response Time	458.7ms	<500ms
Authentication Success Rate	95.4%	≥ 90%
Throughput	4.2v/min	$\geq 3v/min$
Color Accuracy	82.9%	≥ 80%

5.4 System throughput

Under sustained load testing, the system processed 4.2 vehicles per minute, 40% above the minimum requirement. The bottleneck analysis revealed OCR processing accounted for 42% of total latency (198.7ms), followed by YOLOv8n detection at 24% (112.4ms), as illustrated in Figure 9.

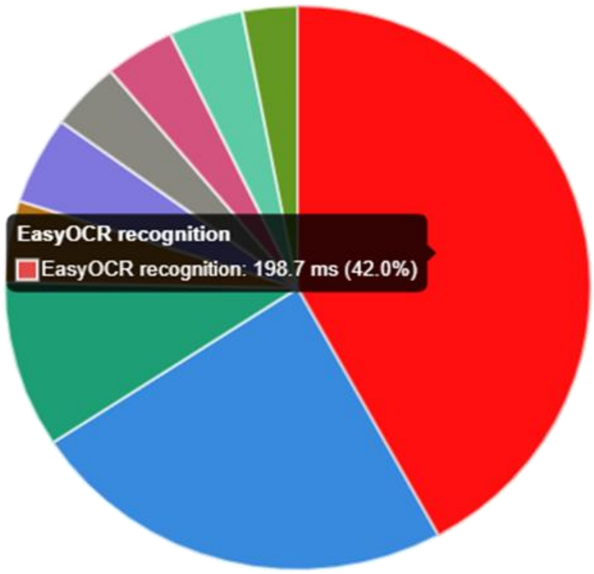

Figure 9: Distribution of end-to-end processing time across pipeline stages

5.5 Comparative analysis

While direct comparison with prior systems is challenging due to dataset differences, the results show significant improvement over traditional approaches:

- 12.5 % higher ANPR accuracy than template-based methods [20]
- 58% faster than hybrid RFID-vision systems [19]
- 3.9x lower false acceptance rate than standalone OCR solutions [23]

The radar chart in Figure 10 illustrates how CVT-AVACS meets or exceeds all performance targets.

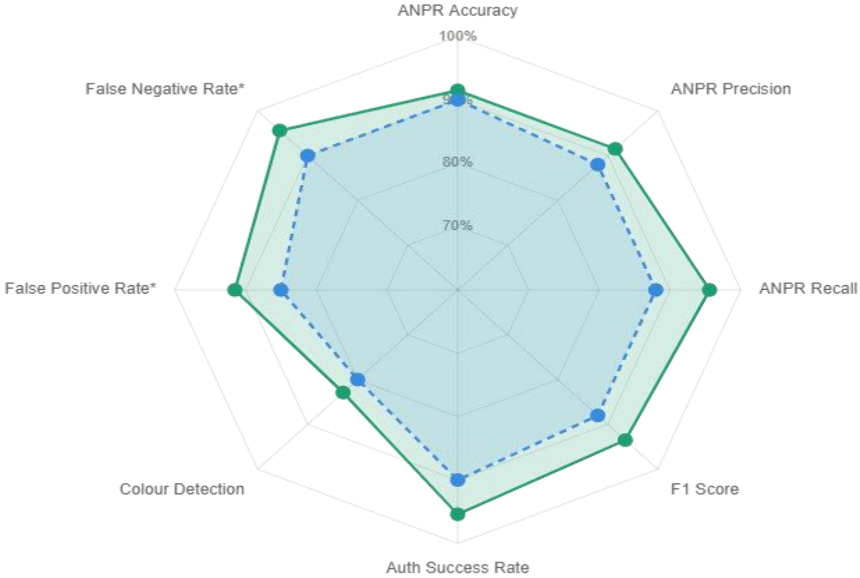

Figure 10: Performance metrics of the CVT-AVACS system against pre-defined targets

6. Limitations

While the proposed system demonstrated strong performance across multiple evaluation metrics, several limitations remain that may affect large-scale real-world deployment. One major limitation is the reduction in ANPR accuracy under challenging environmental conditions. The system achieved lower recognition accuracy in low-light scenarios (87.5%) compared to ideal lighting conditions (94%), indicating that the current preprocessing and feature extraction techniques are still sensitive to illumination changes, shadows, glare, and motion blur. This suggests the need for more robust illumination-invariant models, infrared-assisted imaging, or advanced image enhancement techniques for improved night-time performance.

Another important limitation relates to the dataset used for training and evaluation. The dataset primarily consisted of standard Nigerian private vehicle plate numbers and did not sufficiently include other categories such as government, military, diplomatic, commercial, and customised plates. In addition, the dataset size was relatively limited compared to the diversity of vehicles encountered in real-world environments. Variations in plate fonts, weather conditions, camera angles, occlusion levels, dirt accumulation, and damaged plates were not exhaustively represented. As a result, the trained model may experience reduced generalisation performance when deployed across different geographical regions and operational environments.

Scalability also presents a significant challenge for large-scale deployment. Although the proposed system performed efficiently in controlled testing conditions, deployment across multiple access points or large smart-city infrastructures would require substantial computational and networking resources. Real-time processing of high vehicle volumes would demand GPU-enabled edge devices or dedicated servers capable of supporting continuous YOLOv8n inference, OCR processing, database synchronisation, and token verification simultaneously. Without sufficient computational optimisation, increased traffic loads may introduce higher latency, reduced throughput, and possible bottlenecks during peak operational periods.

Furthermore, the system currently depends on stable internet connectivity for cloud-based database communication and token validation using MongoDB Atlas and FastAPI services. In environments with unreliable network infrastructure, authentication delays or temporary service interruptions may occur. Future improvements should therefore consider offline caching mechanisms, edge-based processing, distributed authentication architectures, and model compression techniques to improve scalability, fault tolerance, and deployment efficiency in resource-constrained environments.

7. Potential Application Scenarios

The proposed system can be applied effectively in environments that require secure and automated vehicle access monitoring, including university campuses, residential estates, corporate organisations, logistics facilities, and smart parking systems. Experimental results demonstrated that the integration of ANPR and token-based authentication improves access verification accuracy while maintaining acceptable response times for real-time operation.

The system's real-time vehicle identification and occupancy monitoring capabilities also support efficient parking space management and access auditing. In addition, the modular architecture allows integration with existing security infrastructure, making the system suitable for gradual deployment in controlled access environments.

8. Ethical Consideration

The gathering and handling of vehicle data present significant privacy issues that require careful management in practical deployments. Although the current system stores license plate numbers for authentication and audit purposes, the associated visual data could potentially be misused for surveillance beyond the intended operational scope. To minimise these risks, captured images and access logs should be retained only for a limited operational period and securely deleted once they are no longer required.

In addition, all stored data should be protected through encryption and controlled access mechanisms to prevent unauthorised access or data breaches. System deployment should also comply with relevant privacy and data protection regulations, such as the Nigeria Data Protection Act (NDPA), by ensuring proper user consent, transparency in data usage, and secure handling of personal information. Future versions of the system may further incorporate privacy-preserving techniques such as differential privacy and secure multi-party computation for token validation and data protection [27].

9. Conclusion

The proposed system effectively combines computer vision and token-based authentication to provide a reliable vehicle access control solution. It utilises YOLOv8n for real-time vehicle detection, OCR for license plate recognition, and JWT for secure validation, thereby overcoming major limitations associated with manual and single-factor authentication systems. Experimental results demonstrated an ANPR accuracy of 91.5% and response times below 500 ms, indicating that the system is suitable for real-world deployment in environments such as university campuses, residential estates, corporate organisations, and logistics facilities.

The study achieved its objective of developing a functional, scalable, and secure vehicle access control framework that improves authentication reliability and audit tracking through multi-phase verification. The integration of Automatic Number Plate Recognition with token-based authentication also demonstrates the practical potential of combining computer vision and lightweight digital authentication techniques in modern smart access systems.

Future work should focus on improving system robustness under challenging environmental conditions, particularly low-light and night-time scenarios. This may involve the integration of infrared-assisted imaging, adaptive image enhancement techniques, and more advanced deep learning models for illumination-invariant recognition. In addition, future research should expand the training dataset to include multiple Nigerian plate categories such as government, military, diplomatic, commercial, and customised license plates in order to improve generalisation and deployment readiness across diverse operational environments. Further optimisation of computational efficiency and edge deployment techniques may also enhance scalability for large-scale smart city and intelligent transportation applications.

References

[1] S. Capkun, M. Cagalj, and J.-P. Hubaux, “Tailing RFID tags for clone detection,” in *Proc. Network and Distributed System Security Symposium (NDSS)*, Internet Society, 2012. [Online]. Available: https://www.ndss-symposium.org

[2] C. Munoz-Ausecha, “RFID applications and security review,” *Algorithms*, vol. 14, no. 6, p. 169, 2021, doi: 10.3390/computation9060069.

[3] F. Alsakka, S. Assaf, I. El-Chami, and M. Al-Hussein, “Computer vision applications in off-site construction,” *Automation in Construction*, vol. 154, p. 104980, 2023, doi: 10.1016/j.autcon.2023.104980.

[4] Z. Liu, M. Xu, and Y. Zhang, “A survey on deep learning for intelligent transportation systems: methods, applications, and challenges,” *Expert Systems with Applications*, vol. 236, p. 121364, 2024, doi: 10.1016/j.eswa.2023.121364.

[5] Y. Gong, K. Li, L. Xiao, J. Cai, J. Xiao, and W. Liang, “VASERP: An adaptive, lightweight, secure, and efficient RFID-based authentication scheme for Internet of Vehicles,” *Sensors*, vol. 23, no. 11, p. 5198, 2023.

[6] F. Alharbi, R. Alshahrani, M. Zakariah, A. Aldweesh, and A. A. Alghamdi, “YOLO and blockchain technology applied to intelligent transportation license plate character recognition for security,” *Computers, Materials & Continua*, vol. 77, no. 3, pp. 3697–3722, 2023.

[7] K. Roy, M. Ahmad, N. A. Ghani, J. Uddin, and J. Shin, “An automated precise authentication of vehicles for enhancing visual security protocols,” *Information*, vol. 14, no. 8, p. 466, 2023.

[8] A. Jodeiri Akbarfam, S. Barazandeh, H. Maleki, and D. Gupta, “DLACB: Deep learning-based access control using blockchain,” *arXiv* preprint arXiv:2303.14758, 2023.

[9] V. Rai, G. Kumar, A. K. Kushwaha, A. Pandey, and V. Kumar, “TrALPR: Automatic license plate recognition using transformers,” in *Proc. IEEE MOSICOM*, 2023, pp. 144–149.

[10] M. Kim, I. Oh, J. Park, M. Sahlabadi, and Z. Shukur, "Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies," *IEEE Access*, vol. 12, pp. 33972–34001, 2024.

[11] A. Jodeiri Akbarfam, S. Barazandeh, D. Gupta, and H. Maleki, "Deep learning meets blockchain for automated and secure access control," *arXiv* preprint arXiv:2311.06236, 2023.

[12] F. Alharbi *et al.*, "Intelligent transportation using wireless sensor networks and blockchain-based license plate recognition," *Sensors*, vol. 23, no. 5, p. 2670, 2023.

[13] N. M. Alahdal *et al.*, "Real-time object detection in autonomous vehicles with YOLO," *Procedia Computer Science*, 2024.

[14] M. Talib, A. Al-Noori, and J. Suad, "YOLOv8-CAB: Improved YOLOv8 for real-time object detection," *Karbala International Journal of Modern Science*, vol. 10, 2024, doi: 10.33640/2405-609X.3339.

[15] M. Samantaray, A. K. Biswal, D. Singh, *et al.*, "Optical character recognition (OCR)-based vehicle's license plate recognition system using Python and OpenCV," in *Proc. 5th Int. Conf. Computing, Communication and Intelligent Systems (ICCCIS)*, 2021.

[16] R. Buoy, M. Wamura, S. Srun, and K. Kise, "Toward a low-resource non-Latin complete baseline: An exploration of Khmer optical character recognition," *IEEE Access*, 2023, doi: 10.3390/s21093028.

[17] S. Talakola and S. P. Veluru, "Managing authentication in REST Assured, OAuth, JWT and more," *International Journal of Emerging Trends in Computer Science and Information Technology*, 2023.

[18] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006, doi: 10.1109/JSAC.2005.861395.

[19] K. L. Ng, C. W. R. Chiong, and R. Reine, "Vehicle recognition system using RFID technology for parking management system," *IOP Conference Series: Materials Science and Engineering*, vol. 495, no. 1, 2019, doi: 10.1088/1757-899X/495/1/012022.

[20] N. Mufti and S. A. Shah, "Automatic number plate recognition: A detailed survey of relevant algorithms," *Sensors*, vol. 21, no. 9, p. 3028, 2021, doi: 10.3390/s21093028.

[21] P. Surekha, P. Gurudath, R. Prithvi, *et al.*, "Automatic license plate recognition using image processing and neural network," 2018.

[22] M. Al-Hasan, A. Alenezi, and H. Alsaif, "Automatic number plate recognition using YOLOv8 and deep learning techniques," *Technologies*, vol. 12, no. 9, p. 164, 2024, doi: 10.3390/technologies12090164.

[23] S. Moussaoui, A. Chfadi, and Y. Ruichek, "Real-time vehicle and license plate recognition using YOLOv8 and OCR techniques," *Scientific Reports*, vol. 14, no. 1, p. 65272, 2024, doi: 10.1038/s41598-024-65272-1.

[24] M. Siddiqui, A. Khan, and S. Rehman, "Vehicle and driver recognition for access control using YOLOv8 and EasyOCR," in *Proc. 2024 Int. Conf. Artificial Intelligence and Smart Systems (ICAIS)*, 2024, pp. 411–417.

[25] D. H. Brainard and B. A. Wandell, "Analysis of the Retinex theory of colour vision," *Journal of the Optical Society of America A*, vol. 3, no. 10, pp. 1651–1661, 1986.

[26] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When machine learning meets privacy: A survey and outlook," *arXiv* preprint arXiv:2011.11819, 2020.