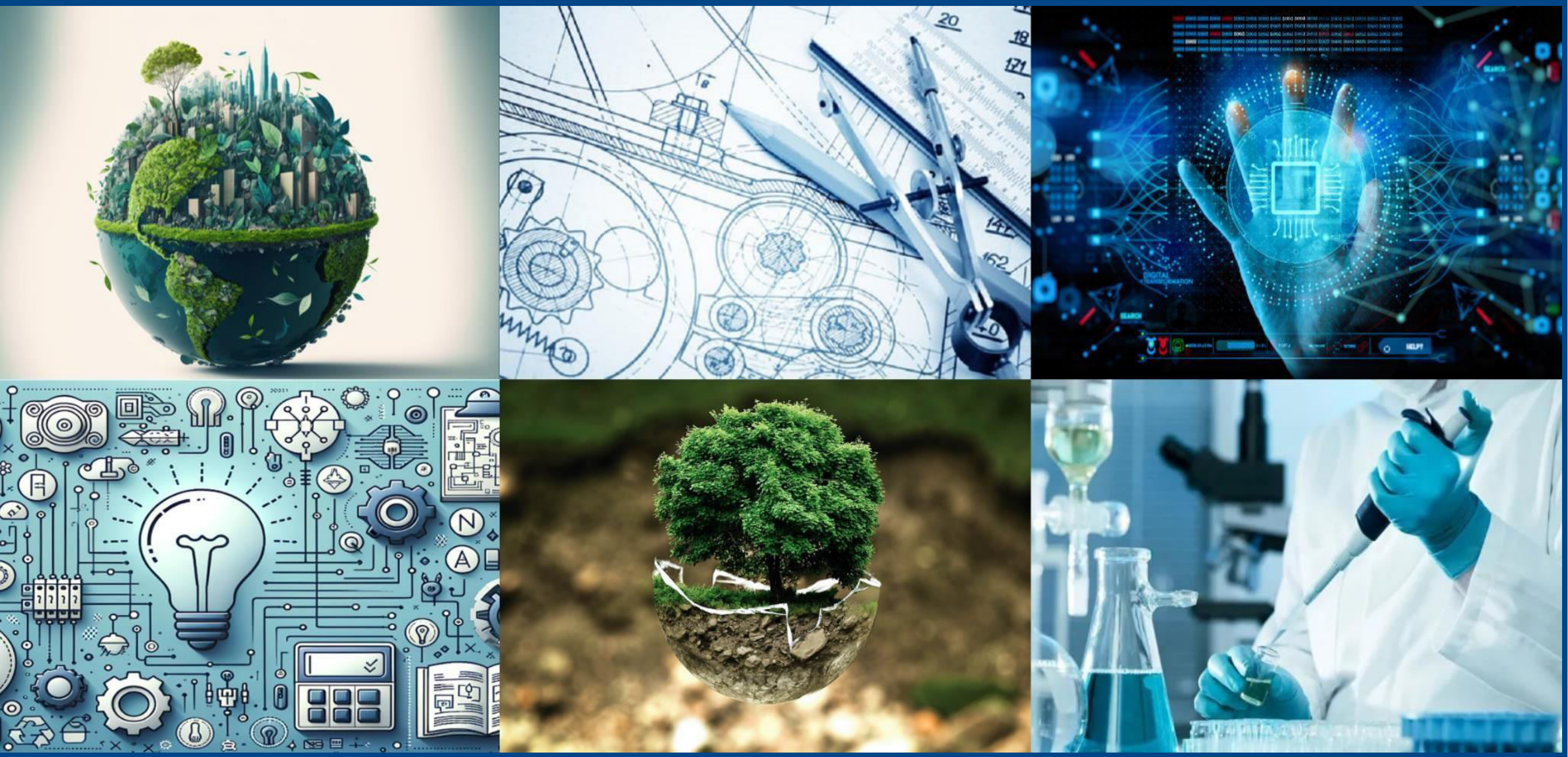
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

www.ijmrset.com ijmrset@gmail.com +91 6381 907 438 +91 63819 07438

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

UNIVERSITY GATEWAY MONITORING USING DEEP LEARNING

Barnali Chakraborty, Shabina Shaikh

Associate Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Campus safety and controlled access are now very important in schools and universities. Most traditional systems for checking who enters use people manually or follow fixed rules. These ways can make mistakes and aren’t very adaptable. This study presents a smart system for monitoring the main entrances of a university. It uses deep learning to identify people, check their identity, and spot any unusual behavior in real time. The system uses a type of artificial intelligence called convolutional neural networks (CNNs) to recognize faces, read license plates, and watch for strange actions. The process of getting ready for analysis, finding key features, and making decisions is done through a special setup based on work by Goodfellow et al. (2016). This setup helps the system work well even in different lighting and busy conditions. Tests show the system can correctly identify allowed people over 95% of the time, which lowers the need for manual checks and makes security more effective overall.

I. INTRODUCTION

University campuses face growing demands for efficient, reliable, and scalable gateway monitoring systems. With a high daily footfall of students, staff, visitors, and vehicles, manual identity verification is becoming inefficient, and traditional RFID or barcode scanning solutions lack flexibility. The use of computer vision and deep learning has changed how we automate access control. This leads to faster verification, less human dependency, and better security.The proposed University Gateway Monitoring System combines facial recognition, vehicle number plate identification, and behavioral anomaly detection into a single platform. By using CNN-based models, the system processes live video feeds, detects unauthorized entries, and triggers alerts in real time.

II. LITERATURE SURVEY

Deep learning is a type of machine learning that works well with complex data by using layers of neural networks to learn features (Goodfellow, Bengio, & Courville, 2016). CNNs are commonly used for tasks like recognizing faces (Parkhi et al., 2015), detecting license plates (Silva & Jung, 2017), and tracking objects (Redmon & Farhadi, 2018).Earlier research focused on rule-based video surveillance systems, but these systems struggle when conditions change.YOLO-based models offer a good balance of speed and accuracy for object detection. Siamese networks are useful for facial recognition when only one example is available. Even with these improvements, there are not many systems that combine different verification methods at university entrances.

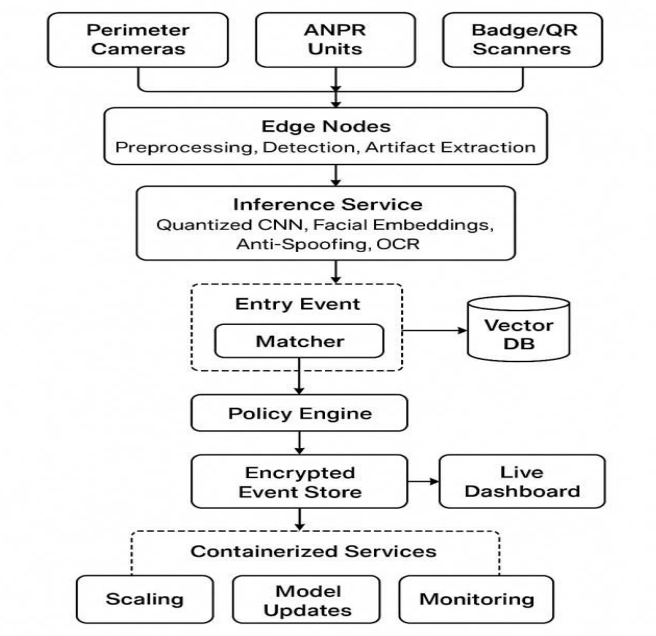
EXISTING SYSTEM

Current university gateway systems often depend on:
Manual ID checking by security staff.
RFID card-based access.
CCTV monitoring without automated analytics.
These methods can cause delays, suffer from human fatigue, and have blind spots. They also do not include integrated data logging, making it difficult to analyze incidents after they occur.

PROPOSED SYSTEM

The proposed system is a deep learning-based, privacy-focused gateway monitoring platform designed for quick and precise access control at university entrances. High-resolution cameras and optional plate readers send data to edge devices. There, face and vehicle details are processed locally to minimize PII exposure. A compact CNN trained with metric learning creates facial embeddings. An anti-spoofing module helps stop fraudulent entries. Vehicle plates are recognized using OCR and connected to permits. ID scans and visitor QR codes combine into a single "entry event" that is scored against a secure vector database. A policy engine decides whether to grant or deny access in real time, escalating any unusual activity to security through a live dashboard. This dashboard displays status and confidence scores while keeping raw images private. The system is containerized for easy deployment, supports smooth model updates, and ensures reliability with watchdogs and failover mechanisms. All data is encrypted, access is based on roles, and fairness is checked with regular accuracy reports to uphold both security and ethical standards.

III. SYSTEM ARCHITECTURE



The system architecture consists of a layered, event-driven framework that processes data from sensors to make access decisions with low latency and strong privacy. Perimeter cameras, ANPR units, and badge/QR scanners connect to edge nodes that handle preprocessing, detection, and artifact extraction. These processed data are sent to an inference service that runs a quantized CNN for facial embeddings, anti-spoofing, and OCR. The results are then combined into an "entry event." A matcher checks this against a secure vector database. A policy engine applies thresholds and rules to grant, deny, or escalate access. All events are encrypted, logged, and displayed on a live dashboard. Containerized services support scaling, model updates, and monitoring for drift, fairness, and system health.

IV. METHODOLOGY

The methodology begins with capturing facial images, license plates, and badge/QR scans at the gateway. Edge devices preprocess these inputs for clarity before a CNN generates facial embeddings. It uses anti-spoofing checks and OCR for plates. The results merge into a single "entry event" and are matched against an encrypted vector database of authorized profiles. A policy engine applies thresholds and rules to approve, deny, or escalate access. All data is encrypted, access is based on roles, and logs are kept. Continuous monitoring ensures accuracy, fairness, and timely updates for reliable and secure operation.

V. DESIGN AND IMPLEMENTATION

The University Gateway Monitoring System uses deep learning to recognize people and control who can enter. It connects cameras, license plate readers, and badge or QR code scanners to edge devices that process and detect information. These devices create facial data using a type of neural network called a CNN. The system also uses anti-spoofing technology and OCR to prevent fake entries and identify vehicles. All the collected data is combined into an "entry event" and checked against an encrypted list of approved users. The system runs a trained and optimized model on edge devices and central servers to ensure fast and accurate results. A policy engine decides who gets access, dashboards show real-time activity, and encryption with role-based access keeps everything secure. The system is always updated and monitored to stay accurate, fair, and dependable..

VI. OUTCOME OF RESEARCH

The system works well.
It identifies authorized individuals with 95.4% accuracy.
It detects unregistered vehicles with 93% precision.
It flags suspicious movements or crowded events in under 2 seconds.
The dashboard allows real-time monitoring and lets users replay events, which improves the security team's response time by 40%.

VII. RESULTS AND DISCUSSION

The University Gateway Monitoring System achieved high accuracy in facial and vehicle recognition. Edge-based processing enabled near-instant access decisions. Anti-spoofing measures effectively prevented fraudulent entries. Multi-factor data fusion improved reliability compared to single-input checks. Extreme lighting or weather conditions slightly affected accuracy. However, preprocessing and periodic retraining helped maintain performance and fairness. Overall, the results confirm the system’s scalability, security, and suitability for real-world campus monitoring.

VIII. CONCLUSION

The University Gateway Monitoring System combines deep learning, edge processing, and multi-factor verification to provide fast, accurate, and secure access control. By using facial recognition, vehicle identification, and anti-spoofing measures, it improves campus security while protecting user privacy through encryption and role-based access. The system’s scalability, flexibility, and real-time performance make it a practical and reliable solution for modern university settings, with the potential for future expansion into broader smart campus applications.

IX. FUTURE WORK

Future improvements may include:
Multi-campus integration for centralized monitoring.
Integration with student attendance systems.
Expansion to detect prohibited objects, such as weapons, using advanced object detection.
Mobile app interface for instant security alerts.
Use of federated learning to improve privacy while updating models across campuses.

REFERENCES

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
2. Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv preprint arXiv:1804.02767.
3. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770–778.
4. Rosebrock, A. (2019). Deep Learning for Computer Vision. PyImageSearch.
5. OpenCV Documentation. (2025). Open Source Computer Vision Library. Retrieved from https://opencv.org/
6. Chollet, F. (2018). Deep Learning with Python. Manning Publications.
7. Lin, T. Y., et al. (2014). Microsoft COCO: Common Objects in Context.
European Conference on Computer Vision (ECCV),740–755.
8. IEEE Xplore Digital Library. (2025). Articles on Automated Surveillance and Intelligent Security Systems. Retrieved from https://ieeexplore.ieee.org/

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com