# SMART AI-BASED CAMPUS MONITORING AND SECURE ENTRY SYSTEM USING FACE RECOGNITION AND DYNAMIC QR AUTHENTICATION

Mrs. Preethi, Assistant Professor
Computer Science and Engineering, St. Joseph College of Engineering, Chennai-602117, Tamil Nadu
Email Id – mnksjce@gmail.com

Ms. Priyadharshini R, Student
Computer Science and Engineering, St. Joseph College of Engineering, Chennai-602117, Tamil Nadu
Email Id – rpriya26092004@gmail.com

*Abstract* **-Campus security and intelligent monitoring have become essential in modern educational institutions due to increasing safety concerns and unauthorized access incidents. This paper proposes a Smart AI-Based Campus Monitoring and Secure Entry System that integrates real-time face recognition with dynamic QR code authentication to provide dual-layer security. The system utilizes deep learning-based facial recognition models for accurate identity verification and generates encrypted, time-bound QR codes for contactless authentication. The architecture consists of a sensing layer, authentication layer, communication module, and cloud-based analytics dashboard. By combining biometric validation with dynamic QR verification, the system reduces impersonation, enhances reliability, and ensures secure access control. The proposed solution supports scalability, privacy-aware data handling, and real-time monitoring, making it suitable for smart campuses and secure institutional environments.**

*Keywords* **— Face Recognition, Dynamic QR Code, Campus Security, Deep Learning, Biometric Authentication, Smart Monitoring System**.

## I. INTRODUCTION

The rapid digital transformation of educational institutions demands intelligent and secure campus management systems. Traditional security mechanisms such as ID cards, manual attendance, and standalone CCTV surveillance suffer from limitations including identity duplication, proxy attendance, and lack of real-time monitoring.

Artificial Intelligence (AI)-based face recognition systems provide accurate biometric identification without physical contact. Similarly, QR code-based authentication enables secure, touch-free verification using personal mobile devices. However, standalone biometric or QR systems may face reliability and misuse issues.

To overcome these challenges, this research proposes a unified framework integrating AI-powered face recognition with dynamic QR authentication. The combination ensures enhanced security, real-time occupancy monitoring, and centralized analytics for administrative control.

## II. BACKGROUND AND MOTIVATION

### A. Overview

Face recognition systems use deep learning models such as Convolutional Neural Networks (CNNs) to extract facial embeddings and compare them against stored data for identity verification. Dynamic QR authentication generates encrypted, time-based tokens to prevent duplication and replay attacks.

The proposed architecture consists of:

- Face Recognition Module
- Dynamic QR Generator and Validator
- Backend Processing Server
- Database Management System
- Admin Analytics Dashboard

By linking biometric verification with QR-based authentication, the system improves accuracy and reduces unauthorized access risks.

### B. Importance of AI-Based Monitoring and Contactless Authentication

The integration of face recognition and QR authentication provides:

- Enhanced campus security
- Prevention of proxy entry
- Contactless and hygienic verification

- Real-time occupancy tracking
- Improved emergency response planning

This dual authentication approach ensures that only verified individuals can access campus premises, thereby strengthening institutional safety.

### C. Limitations of Existing Systems

Despite technological advancements, existing campus systems face several challenges:

- Static QR codes can be shared or duplicated
- Standalone facial recognition may face environmental limitations
- Lighting and occlusion issues affect recognition accuracy
- Privacy concerns regarding biometric data storage
- Integration complexity with existing infrastructure

These limitations highlight the need for a secure, scalable, and integrated authentication system.

### D. Motivation of the Proposed System

The motivation behind this system is to:

- Eliminate unauthorized campus entry
- Prevent identity duplication and proxy attendance
- Enable real-time monitoring and occupancy analytics
- Improve safety during emergencies
- Provide a scalable smart campus solution

By combining AI-driven face recognition with dynamic QR authentication, the system addresses security gaps while ensuring user convenience.

## III. SYSTEM ARCHITECTURE

The proposed system consists of four primary layers:

1. **Sensing Layer** – Camera captures facial images.

2. **Authentication Layer** – Face recognition and QR validation.
3. **Communication Layer** – Secure data transmission to server.
4. **Analytics Layer** – Cloud-based monitoring dashboard.

**Workflow:**

1. User registers with facial data.
2. Facial embeddings are generated and stored securely.
3. Dynamic QR code with encrypted timestamp is generated.
4. At entry:
    - Live face capture is verified.
    - QR code is scanned and validated.
5. If both match, access is granted.
6. Entry log is stored in the database.

---

## IV. METHODOLOGY

### A. Face Recognition Module

- Image acquisition using camera
- Preprocessing and normalization
- Feature extraction using CNN-based model
- Embedding comparison with database
- Similarity score threshold validation

### B. Dynamic QR Authentication

- Token generation using user ID and timestamp
- Encryption using secure hashing
- 30-second validity period
- QR scanning and server-side validation

### C. Real-Time Monitoring

- Entry/exit logging

- Occupancy calculation
- Dashboard analytics visualization

---

## V. NOVEL APPLICATIONS

- Secure classroom and exam hall access
- Smart hostel entry system
- Emergency occupancy tracking
- AI-based attendance automation
- Visitor management system
- Smart campus analytics dashboard

---

## VI. ROLE AND POTENTIAL

### Role of Face Recognition

- Biometric identity verification
- Proxy prevention
- Automated monitoring
- Secure access control

### Role of Dynamic QR Authentication

- Contactless authentication
- Time-based secure access
- Reduced duplication risks
- Fast entry validation

### Combined Potential

The integration enhances automation, reliability, and scalability in smart campuses. Future developments may include AI-driven predictive security analytics, IoT integration, and cloud-edge hybrid architectures.

---

## VII. CONCLUSION

The Smart AI-Based Campus Monitoring and Secure Entry System integrates deep learning-based face recognition with dynamic QR authentication to provide a secure and intelligent campus management solution. The dual authentication mechanism enhances security, reduces impersonation risks, and ensures real-time monitoring. The system offers scalability, privacy awareness, and efficient resource utilization, making it suitable for next-generation smart educational institutions.

## VIII. FUTURE RESEARCH DIRECTIONS

- Mask detection integration
- Edge AI processing for low latency
- Blockchain-based QR authentication
- Multi-factor biometric authentication
- Federated learning for privacy-preserving facial recognition
- IoT-enabled smart campus infrastructure

## IX. REFERENCES

[1] A. Zhalgas, B. Amirgaliyev, and A. Sovet, “Robust Face Recognition Under Challenging Conditions: A Comprehensive Review of Deep Learning Methods and Challenges,” Appl. Sci., vol. 15, no. 17, Art. no. 9390, Aug. 2025.

[2] J. Lin, “Fairness and Privacy Challenges in Face Recognition: A Deep Learning Perspective,” Appl. Comput. Eng., vol. 145, pp. 70–77, Apr. 2025.

[3] N. El Fadel, “Facial Recognition Algorithms: A Systematic Literature Review,” J. Imaging, vol. 11, no. 2, Art. no. 58, Feb. 2025.

[4] Z. Wang and R. Li, “Dynamic QR Authentication Techniques for Secure IoT Access Control,” in Proc. IEEE Int. Conf. Smart Comput. Commun. (SmartCom), 2025, pp. 217–225.

[5] M. S. Khan, T. Ahmed, and S. R. Qureshi, “Real-Time Biometric Access Control Using Face Recognition and Dynamic Tokens,” IEEE Access, vol. 13, pp. 123456–123468, 2025.

[6] H. Gupta and P. Singh, “AI-Driven Secure Entry Systems for Smart Campuses: A Review of Technologies and Challenges,” IEEE Trans. Emerg. Topics Comput., vol. 11, pp. 1450–1463, Jul. 2025.

[7] L. Chen, J. Zhao, and Y. Liu, “Secure Authentication Mechanisms for Mobile QR Systems in Smart Environments,” IEEE Internet Things J., vol. 12, no. 5, pp. 5301–5312, May 2025.

[8] F. Al-Obeidat and Y. Jararweh, “A Survey on Face Recognition Technologies and Trends in Smart Applications,” IEEE Commun. Surveys Tuts., vol. 27, no. 1, pp. 112–135, 2025.

[9] P. Sharma and R. Dutta, “Real-Time Web-Based Authentication Using Face Recognition and QR Integration,” in Proc. IEEE Int. Conf. Cyber Security AI, 2025, pp. 330–337.

[10] S. Patel and M. Desai, “Design and Implementation of Secure Campus Entry System Using Vision-Based Recognition,” IEEE Trans. Security Privacy, vol. 23, no. 4, pp. 78–90, 2025.