NEHRU INSTITUTE OF ENGINEERINGAND TECHNOLOGY
(AUTONOMOUS)
Thirumalayampalayam, Coimbatore-641 105
(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
An ISO 9001:2015 and ISO 14001:2015 Certified Institution
Re-Accredited by NAAC with A+ and Recognized by UGC with Section 2(f) and 12(B)
NBA Accredited UG Programmes :AERO | CSE | ECE | EEE | MECH | MCT | AI&DS

AI POWERED COLLEGE SECURITY MONITORING SYSTEM

Internal Guide : Ms.Kalpana G

Batch Member & Reg. No.:

Karthick B	-	721421243026
Dharun P	-	721421243016
Karun C	-	721421243027

Content

- Abstract
- Problem statement
- Objectives
- Existing Techniques
- Proposed Techniques
- Hardware Requirements
- Software Requirements
- Cost
- Algorithms used
- Block diagram
- Final result
- Conclusion and Future Work
- Reference

Abstract

The proposed AI-powered College Security surveillance Monitoring System aims to enhance the safety and security of college campuses by integrating advanced technologies to create a robust, real-time surveillance ecosystem. By combining high-definition cameras, motion detectors, AI-driven analytics, and centralized monitoring software, the system ensures continuous observation of critical areas such as entrances, classrooms, corridors, parking lots, and common spaces. It leverages smart technologies like facial recognition and automated threat analysis to detect unauthorized activities, prevent incidents such as vandalism, theft, and unauthorized access, and enable rapid response through real-time alerts via buzzers, mobile apps, and emails. The system incorporates IoT for seamless device connectivity, cloud-based storage for secure data management, and machine learning for proactive threat detection and behavioral analysis. This comprehensive approach not only minimizes human error and eliminates blind spots but also fosters a safe, trusting environment for students, faculty, and staff, setting a benchmark for modern, future-ready educational institutions.

Problem Statement

Ensuring the safety and security of students, faculty, staff, and campus property is a critical priority for colleges and universities in today's complex and dynamic environment. Traditional security measures, such as manual patrolling, limited CCTV systems, and isolated alarm systems, are inadequate for addressing the challenges of modern educational institutions. The vastness and complexity of college campuses, encompassing multiple buildings, libraries, laboratories, sports complexes, hostels, and open spaces, make consistent 24/7 surveillance difficult without a robust, integrated system. In emergencies like unauthorized access, theft, vandalism, violence, or health crises, delayed detection and response can significantly impact outcomes. The absence of centralized, intelligent surveillance monitoring further complicates maintaining a secure yet open campus environment. With advancements in technologies such as IoT, AI-based image analytics, and wireless networks, there is a significant opportunity to modernize campus security systems. The goal is to develop a smart, connected surveillance ecosystem that actively enhances security, protects valuable human and infrastructural assets, builds trust among students and parents, and establishes a standard for future-ready educational institutions.

Objectives

- Implement a real-time surveillance system for 24/7 monitoring of all critical areas across the college campus.
- Design a system that provides instant mobile or desktop alerts to security personnel during unauthorized activities or emergencies.
- Reduce dependency on manual surveillance through automated alert systems to improve reliability and consistency.
- Integrate AI-driven technologies such as facial recognition, and automated threat analysis for proactive monitoring.
- Promote a culture of safety awareness among students and staff by integrating real-time alerts and educational campaigns about surveillance system usage.
- Enhance safety compliance by implementing helmet identification systems at entry points to high-risk areas like workshops or bike parking zones.

Existing Techniques

- Relies on human observation to detect suspicious behavior or incidents like theft, vandalism, or unauthorized access.
- Primarily used for post-incident review rather than real-time monitoring, with footage stored locally.
- Involves security staff stationed at campus entry points to check identification and control access.

Dis-Advantages

- Manual surveillance and gatekeeping are prone to mistakes, such as overlooking suspicious activities or failing to respond promptly, reducing system reliability.
- Existing security measures are often not adaptable to campus expansions or evolving threats, requiring costly overhauls to meet modern safety demands.

Proposed Techniques

YOLO-based Object Detection: Utilizes YOLO algorithm for real-time identification and classification of objects in webcam video, enabling voice feedback for navigation.

Face Recognition: Identifies authorized students, staff, and visitors using AI to match facial features against a pre-registered database, denying access to unknowns.

Buzzer Alerts: Activates loud alarms for unauthorized entry or safety violations (e.g., no helmet in designated areas) to deter intruders and alert staff.

Weapon Detection: Identifies dangerous objects like guns or knives in real-time using computer vision, triggering immediate alerts to prevent violence.

Helmet Identification: Ensures safety compliance in high-risk areas (e.g., workshops, bike parking) by detecting helmet use at entry points.

Proposed Techniques

Advantages

AI-driven Real-time Monitoring: To analyze image feeds and sensor data for real-time detection of suspicious activities, unauthorized access, and threats.

Facial Recognition: Implements AI algorithms to identify individuals by matching facial features against a pre-registered database, granting or denying access and flagging unknowns.

Buzzer Alert System: Activates loud buzzers to deter intruders or signal safety violations (e.g., no helmet) when unauthorized access or non-compliance is detected, integrated with AI detection systems.

Real-time Alerts and Notifications: Generates instant notifications via buzzers, mobile apps, emails, or dashboards for suspicious activities or emergencies, ensuring rapid communication.

Cloud-based Data Management: Stores images footage, event logs, and reports in a secure cloud database with encryption and access controls for audits and evidence.

Proposed Techniques

IoT Notification via Blynk: Sends real-time emergency alerts with GPS coordinates using IoT connectivity over WiFi.

Image Processing with OpenCV: Enhances video frame analysis for object and emotion detection, optimizing AI performance.

Real-time Alerts and Notifications: Generates instant notifications through buzzers, emails, or centralized dashboards when suspicious activities or emergencies are detected.

Algorithms Used

Haar Cascade Algorithm:

In the proposed system, the Haar Cascade Algorithm is employed for face detection, a critical component for identifying individuals entering the campus. It detects faces in real-time image feeds from smart CCTV cameras, enabling subsequent facial recognition to determine if the individual is authorized.

Cascade Classifier

- The algorithm uses a cascade of classifiers, which are pre-trained models that sequentially evaluate regions of an image
- Each stage of the cascade checks if a region contains Haar-like features indicative of a face. If a region fails at any stage, it is discarded, reducing computation time. If it passes all stages, it is identified as a face.

Algorithms Used

YOLO

- **Purpose:** Real-time object detection to identify and classify objects (e.g., weapon, person).
- **Functionality:** Processes webcam image frames using a single neural network to predict bounding boxes and class probabilities

CNN

- **Purpose**: Emotion recognition to detect facial expressions
- **Functionality**: Analyzes facial features in image frames.

Algorithms Used

Deep Learning Algorithms :

- **Purpose:** To support complex pattern recognition and decision-making for proactive security management across diverse surveillance tasks.
- **Functionality:** Employs deep neural networks (DNNs) or recurrent neural networks (RNNs) to process sequential or spatial data from image feeds and sensors. Handles tasks like anomaly detection (identifying unusual patterns), facial recognition, and weapon detection by learning hierarchical features from large datasets.

Hardware Requirements

- ESP 32 Controller
- Buzzer
- Servo Motor
- Gate
- LCD Display
- Webcam

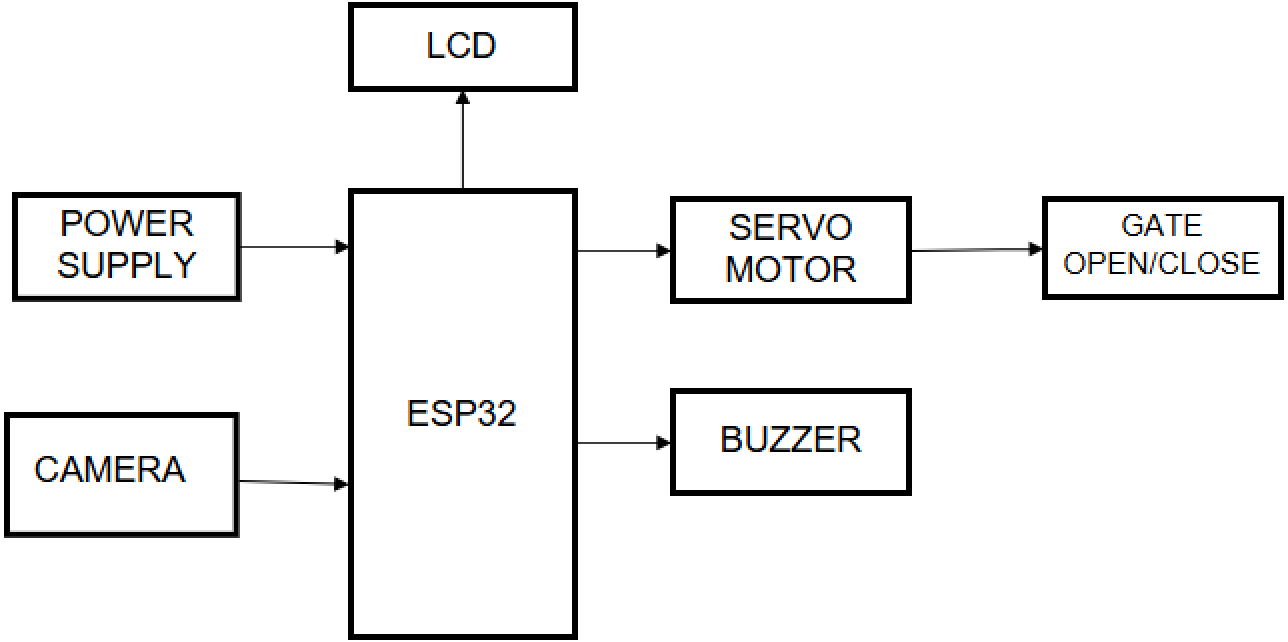
Software Requirements

- Programming –python
- OpenCV
- Tensorflow
- Blynk IOT platform

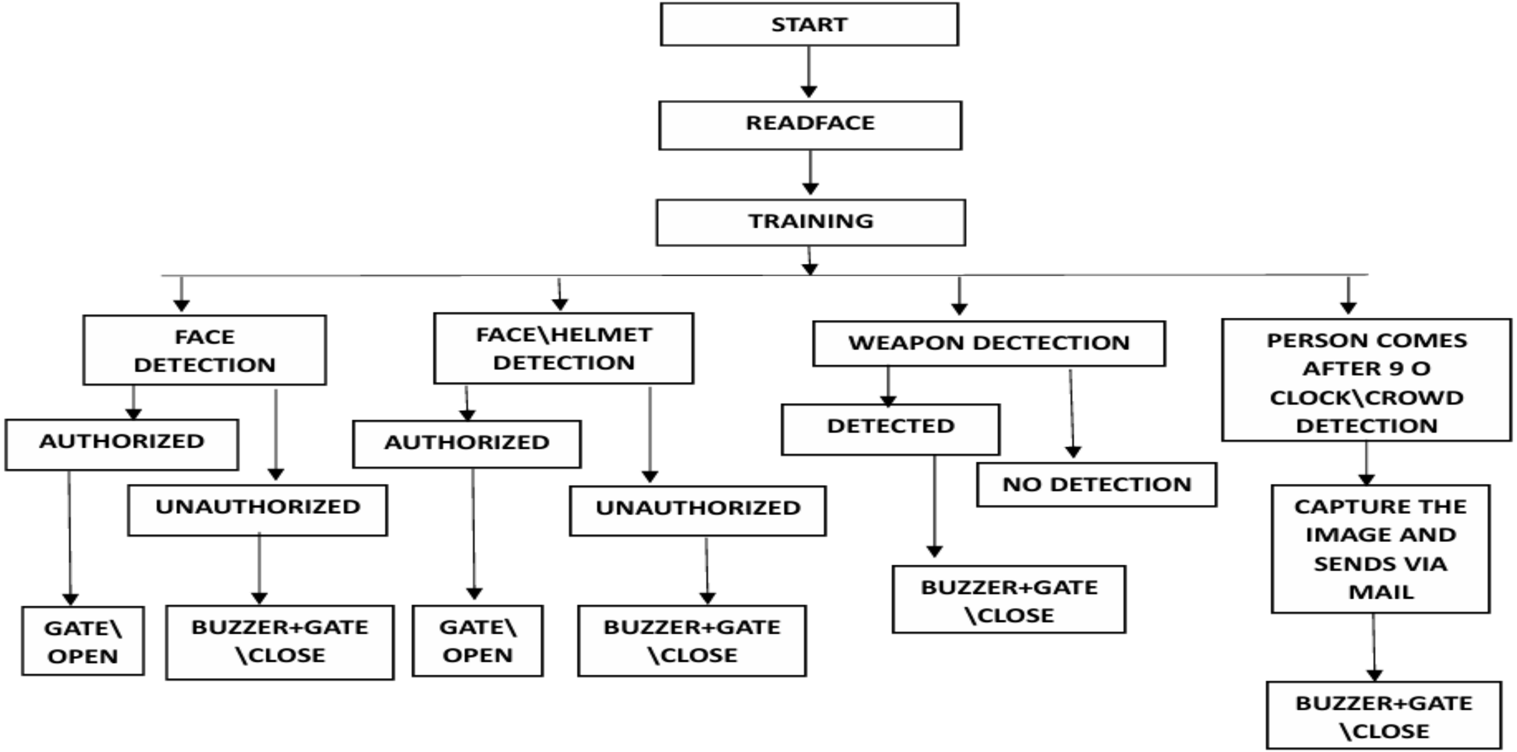
Cost

Requirements	Cost
ESP 32 Controller	₹ 5000
Buzzer	₹ 200
Servo Motor	₹ 800
Gate	₹ 200
LCD Display	₹ 400
Webcam	₹ 1200
0thers	₹ 1500

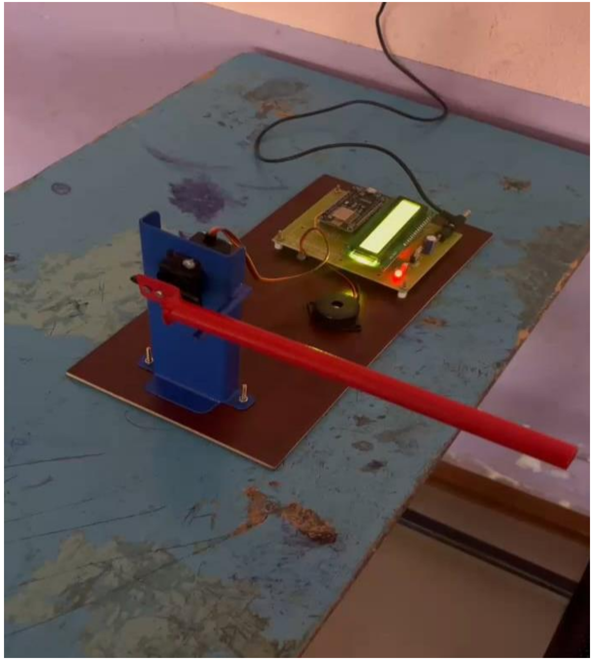
Block Diagram



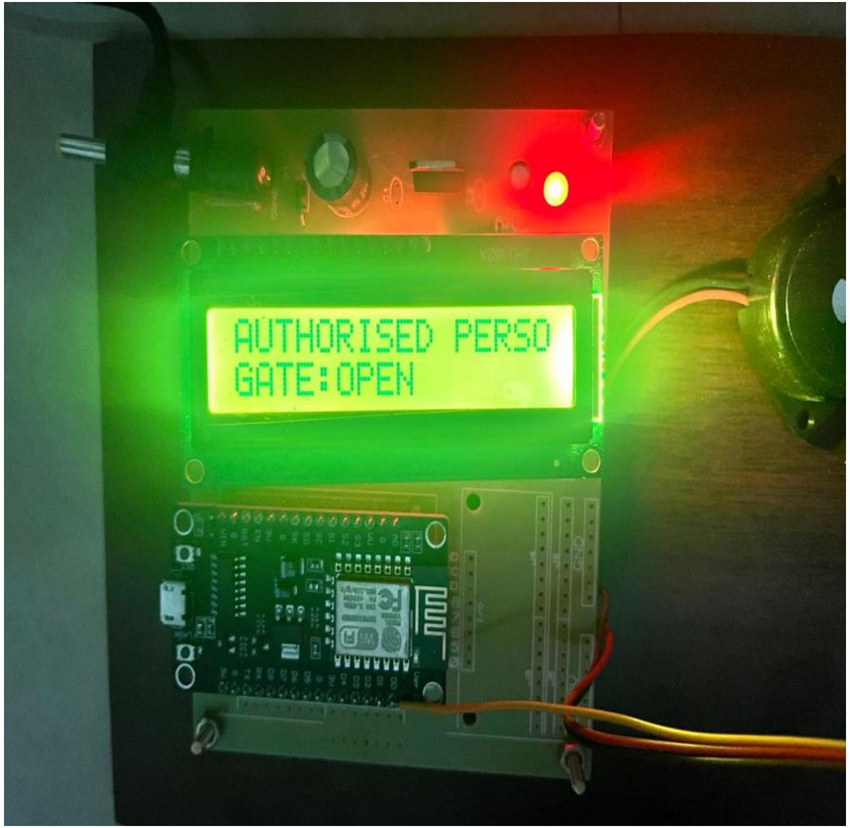
Flow Diagram



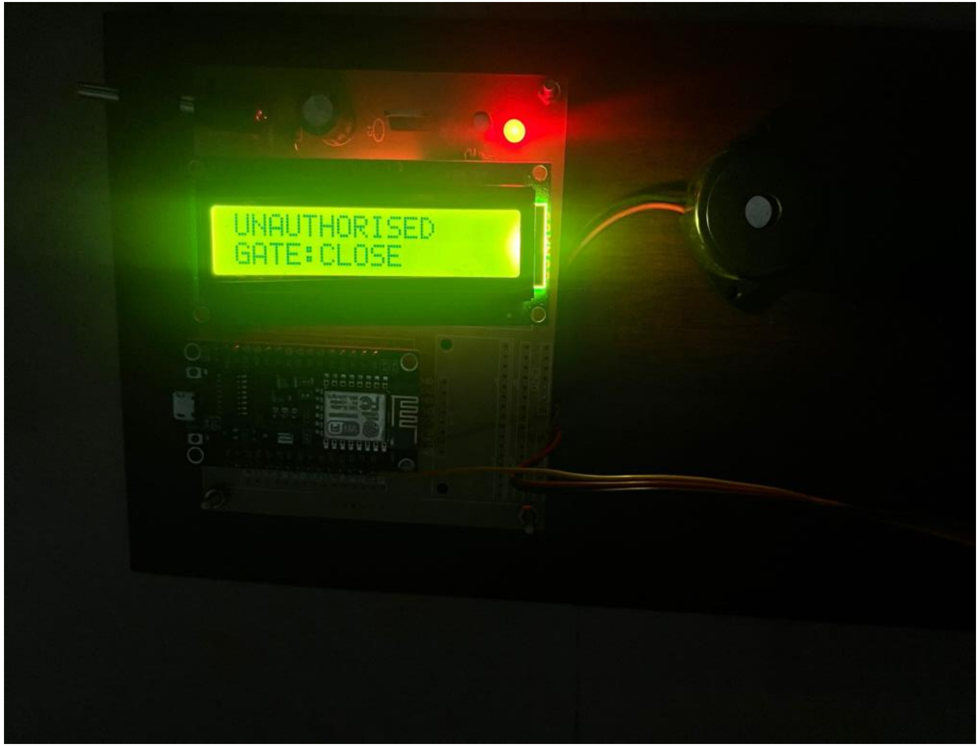
Prototype:



Final Result



Final Result



Conclusion

The AI-Powered College Security Monitoring System provides an efficient, automated, and intelligent approach to campus security. By leveraging AI-based face recognition, IoT for real-time alerts, and automated gate control, the system significantly enhances security while reducing manual intervention. The integration of ESP32, servo motor, buzzer, and LCD ensures seamless operation and efficient monitoring. This system can be further enhanced with cloud-based analytics and integration with law enforcement databases for better security management..

Future Scope

- AI models that can differentiate between faculty, students, visitors, and unauthorized persons with greater precision .
- Improved helmet and vehicle detection accuracy using deep learning models
- . Drone-based monitoring of parking areas, entry/exit points, and high-risk zones
- Detection of suspicious behavior patterns to prevent unauthorized access or misconduct
- Automated facial emotion recognition to identify distress situations and alert authorities

Reference

- S.S., etal. (2020). Helmet Detection System Using Deep Learning. Journal of Computer Vision and Applications, 12(3), 45-56.
- Singh, A. K., et al. (2019). Triple Detection System for Two-Wheelers Using Computer Vision. International Journal of Image Processing, 8(4), 123-134.
- Rao, R. R., et al. (2020). Unauthorized Entry Detection System Using Deep Learning. Proceedings of the International Conference on Artificial Intelligence and Security, 245-252.
- Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). Review on the Security Threats of Internet of Things. arXiv preprint arXiv:2101.05614.
- Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and challenges of cloud integrated IoMT. Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, 67-85.

Reference

- Patel, S., et al. (2020). "AI and Machine Learning in Campus Surveillance." Journal of Artificial Intelligence Research, 15(4), 101-112.
- Kumar, R., & Sharma, S. (2019). "IoT-Enabled Campus Security Systems." International Journal of IoT Applications, 5(1), 34-45.
- Chowdhury, M., & Hassan, S. (2018). "Facial Recognition in Campus Security." Journal of Biometric Systems, 6(4), 88-97.
- Verma, S., & Das, A. (2021). "Drone Surveillance for Campus Security." Aerial Systems Research, 6(1), 12-20.
- Hoque, K., Hossain, M. B., Sami, A., Das, D., Kadir, A., & Rahman, M. A. (2024). Technological trends in 5G networks for IoT-enabled smart healthcare: A review. International Journal of Science and Research Archive, 12(2), 1399-1410.

Thank
You