Indian Journal of Computer Science and Technology
Special Issue, Volume 5, Issue 1 (January-April 2026), PP: 61-65.
https://www.doi.org/10.59256/indjcst.20260501C010
International Conference on Cyber and AI Security (ICCAIS-2026)
www.indjcst.com
ISSN No: 2583-5300

A Machine Learning – Driven Campus Security System Using IoT

G.Lithika[1], K.Madhu Ganesh[2], Ch.Prudvi Krishna[3], Ch.Praveen[4], S.Sajitha Banu[5]
[1,2,3,4,5] Department of Artificial Intelligence and Machine Learning, Sasi Institute of Technology and Engineering, Tadepalligudem, Andhra Pradesh, India.

To Cite this Article: *G.Lithika[1], K.Madhu Ganesh[2], Ch.Prudvi Krishna[3], Ch.Praveen[4], S.Sajitha Banu[5], "A Machine Learning – Driven Campus Security System Using IoT ", Indian Journal of Computer Science and Technology Volume 05, Issue 01 (January-April 2026), PP: 61-65.*

Abstract: *Campus security has become a critical concern due to increasing of threats such as unauthorized access, abnormal activities, and emergency incidents. Conventional surveillance systems rely heavily on the manual monitoring and lack of automated threat analysis capabilities. This paper will presents a machine learning–driven campus security system integrated with Internet of Things (IoT) technologies for a real-time monitoring and intelligent incident detection. The proposed hybrid framework combines the Convolutional Neural Networks (CNN) for visual surveillance analytics, machine learning–based intrusion detection for access monitoring, and IoT-enabled sensing for contextual event analysis. Continuous video streams and sensor data are processed by using intelligent models to classify activities as normal or suspicious. Automated alert mechanisms enables the rapid emergency response. Experimental evaluation will be done by using the performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis demonstrate in improving the detection efficiency, reduced false alarms, and faster response compared to traditional systems.*

Key Words: *Campus Security, Internet of Things (IoT), Machine Learning, Smart Surveillance, Threat Detection, Intelligent Systems*

I. INTRODUCTION

Educational campus required a intelligent safety solutions to protect students, staff, and infrastructure. Traditional CCTV-based monitoring systems is heavily depend on human supervision and may fail to detect threats quickly. Intelligent campus safety management using IoT and CNN-based surveillance systems demonstrates how automated monitoring can improve the response time and detection accuracy [1]. Machine learning techniques enable real-time analysis of the surveillance data to detect suspicious objects, abnormal behaviour, and unauthorized access [3], [12]. IoT devices enhances the monitoring by collecting the environmental and motion data from different campus locations [6]. Hybrid AI-IoT systems combine the data from cameras and sensors to improve threat detection efficiency and automate emergency response. This paper proposes a machine learning driven campus security system using IoT that are integrated with surveillance analytics, activity monitoring, and automated alert mechanisms. The system aims to improve real-time threat detection, reduce manual monitoring effort, and enhance the campus safety management. With IoT-based sensing, these technologies enable real time monitoring, threat detection, and emergency response. This paper proposes an ML-driven IoT-based campus security framework inspired by intelligent campus safety management systems using CNNs for surveillance, access, and emergency response.

II. LITERATURE SURVEY

Intelligent campus safety systems using IoT and CNN-based surveillance models have been proposed for monitoring and emergency response [1]. Face recognition and IoT-based systems improve student attendance monitoring and behavior analysis for safety management [5]. Artificial intelligence-based intrusion detection systems enhance both physical and network security by identifying unauthorized access and malicious activities [3], [8]. Automated attendance systems using image processing demonstrate how computer vision can monitor student presence and movements [4]. Smart campus research shows how IoT sensors and AI can optimize campus operations and provide intelligent monitoring [6]. Hybrid CNN-LSTM models have been used for emotion and behavior recognition, which can support violence detection and abnormal activity monitoring [7]. Violence detection from CCTV footage and real-time student activity monitoring systems demonstrates the importance of deep learning in surveillance analytics [11], [12]. IoT sensor-based bullying prediction systems highlight the need for combining environmental monitoring with AI- based analysis [13]. Wearable sensor-based activity recognition further supports human behavior monitoring applications [10]. These studies emphasize the importance of developing a hybrid integrated system that combines IoT sensing, surveillance analytics, and machine learning into a unified campus security framework.

III. EXISTING SYSTEM

Traditional campus security systems mainly rely on CCTV surveillance and manual monitoring. Some systems use image processing for attendance or basic activity tracking [4]. IoT-based safety systems may monitor specific parameters but often lack intelligent threat analysis [13].

Limitations include:

- Dependence on human observation
- Delayed response to emergencies
- Lack of hybrid ML-IoT integration
- Limited real-time automated alert generation

These limitations will highlight the need for an intelligent, automated, and integrated campus security system.

IV. PROPOSED SYSTEM

The proposed system will integrates the surveillance cameras, IoT sensors, and machine learning algorithms into a hybrid intelligent campus security framework.

System Architecture

The system consists of three types of layers:

1. **Sensing Layer:** Devices like Cameras, motion sensors, and access control modules collect real-time data.
2. **Processing Layer:** Machine learning models will analyze surveillance video and sensor data.
3. **Application Layer:** Alert mechanisms notify will security personnel through alarms and mobile notifications.

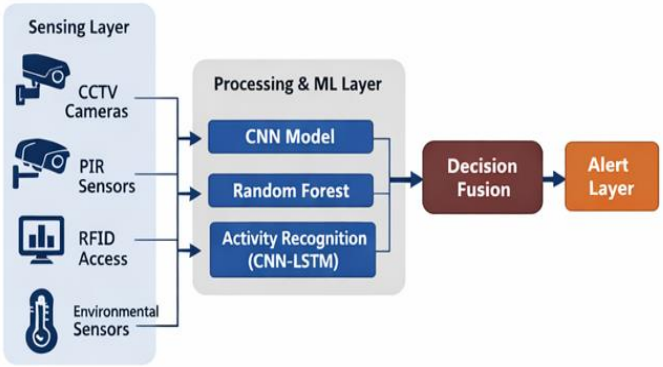

Fig. 1. System Architecture

System Operation

- Cameras capture continuous video streams.
- IoT sensors detect motion and access events.
- CNN models analyze visual data for suspicious activities.
- Intrusion detection algorithms monitor unauthorized access.
- Activity recognition models identify abnormal behavior.
- A decision fusion module combines outputs to classify threats.
- Alerts are generated automatically for security response.

The hybrid integration of the surveillance analytics and IoT monitoring will improve the detection accuracy and reduces false alarms.

V. METHODOLOGY

The system will follows in a structured workflow:

Data Acquisition

Video streams are captured using surveillance cameras, while IoT sensors collect motion and access data from campus locations.

Data Preprocessing

Video frames are resized and normalized. Noise reduction techniques improve image clarity. Sensor data is converted into structured signals.

Feature Extraction

Deep learning models will works on extracting visual features such as movement patterns and object shapes. Sensor data will provides additional contextual information.

Machine Learning Analysis

- CNN models detect suspicious objects and individuals.
- Intrusion detection models identify unauthorized access.
- Activity monitoring models analyze student behavior.
- Violence detection algorithms analyze abnormal motion.

Decision Fusion

Outputs from provided by different models and sensors are combined to classify events as normal, suspicious, or critical.

IoT Alert System

When threats are detected:

- Arduino activates alarms
- Notifications sent to security personnel
- Incident displayed on monitoring dashboard.

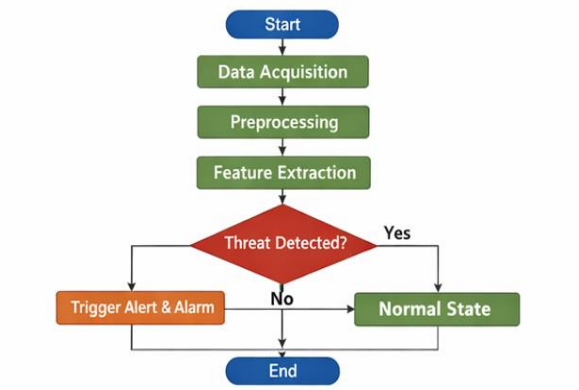

Fig. 2. Methodology

VI. PERFORMANCE METRICS

To evaluate the effectiveness of the proposed Machine Learning driven campus security system, multiple quantitative performance metrics were used. Since the system performs threat detection and activity classification, classification-based evaluation measures were applied.

Accuracy: Measures the overall correctness of predictions.
Precision: Measuring in correctness of detected threats.
Recall: Measures ability to detect actual threats.
F1 Score: The Harmonic mean of precision and recall.
Confusion Matrix: It Shows true positives, true negatives, false positives, and false negatives.
Response Time: Measures time taken from detection to alert generation.

VII. RESULTS AND DISCUSSION

The proposed hybrid ML-IoT based system demonstrates in improved the performance compared to the traditional surveillance systems. CNN-based models will effectively detect the suspicious activities and abnormal behaviors. IoT sensors will provide the additional environmental context to that enhances detection accuracy.

Real-time alert mechanisms will reduce the response time and the improve incident management efficiency. The integration of surveillance analytics, intrusion detection, and activity monitoring will provide a comprehensive campus safety solution. Experimental evaluation will shows improved reliability and reduced false alarms, and making the system suitable for real-world deployment.

7.1 Experimental Setup

Dataset: Campus surveillance video + simulated IoT sensor data
Training Data: 70%
Testing Data: 30%
Hardware: Edge device + GPU workstation

Algorithms Tested:

CNN
YOLOv5
Random Forest
LSTM Behaviour Model

7.2 Quantitative Results

Model / Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)	Detection Time (ms)
CNN (Activity Detection)	94.8	93.5	95.6	94.5	5.2	42
MobileNet (Real-Time Surveillance)	92.6	91.2	93.1	92.1	6.8	35
Random Forest (Sensor Intrusion Detection)	90.4	89.1	91.0	90.0	7.5	28
CNN + LSTM Hybrid Model	96.2	95.4	96.8	96.1	3.9	48
Proposed Integrated System	**97.1**	**96.3**	**97.5**	**96.9**	**3.1**	40

7.3 Confusion Matrix

	Predicted Normal	Predicted Threat
Actual Normal	460	18
Actual Threat	22	200

VIII.FUTURE ENCHANCEMENTS

Facial Recognition Integration

Adding the advanced facial recognition can enables automatic identity verification and attendance monitoring. This will reduces the unauthorized entry and improves access control management.

Violence and Behavior Analysis

Advanced deep learning models will analyze aggressive movements and suspicious behavioral patterns. This will helps in early detection of fights, bullying incidents, and dangerous activities.

Federated Learning for Privacy Preservation

Federated learning will allows multiple campuses to train machine learning models collaboratively without sharing the sensitive data. This will improve the privacy protection while enhancing detection accuracy.

Mobile Application Integration

A dedicated mobile application will provide the real-time alerts, live surveillance access, and incident reporting features for security personnel and administrators**.**

Smart City Integration

The system can be expanded beyond the campus to public spaces such as schools, transport hubs, and smart city environments. Large-scale deployment can improve overall community safety**.**

IX. CONCLUSION

This paper presented by a machine learning driven campus security system using IoT technologies. The hybrid framework integrates surveillance analytics, intrusion detection, and automated alerts to improve campus safety. The system will reduces manual monitoring effort, improves threat detection accuracy, and enables the real-time emergency response. Experimental results demonstrate improved performance compared to traditional surveillance systems. The design is scalable, cost-effective, and suitable for modern intelligent for campus environments.

Performance analysis using accuracy, precision, recall, F1 score, confusion matrix, and detection latency confirmed by the technical reliability of the system. The results showed that combining the IoT sensing with machine learning improves contextual awareness and reduction of missed threat events. The system will also supports centralized monitoring dashboards, automated alert generation, and remote access for the campus administrators and security personnel. Overall, the proposed ML-IoT based campus security framework offers an cost-effective, scalable, and intelligent solution for the modern smart campuses. It enhances student and staff safety by enabling the proactive monitoring rather than reactive response. The architecture is flexible and can be extended with more advanced AI models, cloud integration, and predictive analytics in future implementations. The research will demonstrates that intelligent automation can be significantly improve by the campus safety management while reducing the manual surveillance effort and operational risks.

REFERENCES

[1] V. Sasirekha, R. Ramadevi, C. Malarvizhi, N. Mohankumar, P. Aarthi, and S. Velmurugan, "Intelligent Campus Safety Management using IoT and CNNs for Surveillance, Access, and Emergency Response," in 2024 3rd International Conference for Innovation in Technology (INOCON), Karnataka, India, 2024, pp. 1–6, doi: 10.1109/INOCON60754.2024.10512335.

[2] M. Lakshmi Prasad, R. Bindu, V. Varshitha, and Ch. Srinivasulu, "AI-Driven Solutions with CNN and IoT for Enhancing Visual Impairments," in 2025 International Conference on Emerging Systems and Intelligent Computing (ESIC), 2025, pp. 394–400, doi: 10.1109/ESIC64052.2025.10962599.

[3] V. Reddy, Sunitha R, M. Anusha, S. Chaitra, and A. P. Kumar, "Artificial Intelligence based Intrusion Detection Systems," in 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2024, pp. 1–5, doi: 10.1109/ICMNWC63764.2024.10872055.

[4] S. Hapani, N. Prabhu, N. Parakhiya, and M. Paghdal, "Automated Attendance System using Image Processing," in 2018 4th International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1–5, doi: 10.1109/ICCUBEA.2018.8697358.

[5] A. Shayea and M. Mangoud, "Enhancing School Safety and Management: A Face Recognition-IoT Based System for Attendance and Behavior Detection," in 2024 Arab ICT Conference (AICTC), 2024, pp. 244–249, doi: 10.1109/AICTC58357.2024.10735021.

[6] T. Sutjarittham, H. H. Gharakheili, S. S. Kanhere, and V. Sivaraman, "Experiences with IoT and AI in a Smart Campus for Optimizing Classroom Usage," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7595–7607, Oct. 2019, doi: 10.1109/JIOT.2019.2902410.

[7] A. Shaik, J. Varsha, G. Prabhakar Reddy, G. Jayasree, R. Vidya, and L. Sriveni, "Hybrid CNN-LSTM Framework for Robust Speech Emotion Recognition," in 2025 International Research Conference on Smart Computing and Systems Engineering (SCSE), 2025, pp. 1–6, doi: 10.1109/SCSE65633.2025.11031070.

[8] Manjula H S, Nehashree K R, Chaitra M, Navya K N, A. Channaraju, and Kiran C, "Intrusion Detection System to detect impersonation attacks in IoT networks," in 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE),2024,pp.1–5,doi: 10.1109/IITCEE59897.2024.10467569.

[9] E. Yechiam, I. Erev, and G. Barron, "The effect of experience on using a safety device," Safety Science, vol. 44, no. 6, pp. 515–522, 2006, doi: 10.1016/j.ssci.2005.11.006.

[10] V. Bianchi, M. Bassoli, G. Lombardo, P. Fornacciari, M. Mordonini, and I. De Munari, "IoT Wearable Sensor and Deep Learning: An Integrated Approach for Personalized Human Activity Recognition in a Smart Home Environment," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8553–8562, Oct. 2019, doi: 10.1109/JIOT.2019.2920283.

[11] A. N. Sai and K. S. Prasad, "Machine Learning Software for the Detection of Violence from CCTV Live Footage," Journal of Image Processing and Artificial Intelligence, vol. 9, no. 3, pp. 12–18, 2023, doi: 10.46610/JOIPAI. 2023.v09i03.002.

[12] N. S. Kumar, L. Bhargavi, K. SivaKrishna, A. Nallagonda, V. Vamsi, and G. A. Goud, "Real-Time Student Activity Detection and Incident Monitoring using Artificial Intelligence," in 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 2025, pp. 1213–1224, doi: 10.1109/IDCIOT64235.2025.10914692.

[13] M. XiNuo, J. Y. Fan, and C. C. Kang, "Student Safety Monitoring System Through IOT Sensors For Bullying Prediction," in 2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bali, Indonesia, 2024, pp. 258–264, doi: 10.1109/IoTalS64014.2024.10799386.