

AI POWERED SMART SURVEILLANCE FOR CAMPUS SECURITY AND MONITORING

Kumuda D P

Computer Science and Engineering (Artificial
Intelligence and Machine Learning)
Malnad College of Engineering
Hassan-573202, India
dpkumuda12@gmail.com

Harshitha B V

Computer Science and Engineering (Artificial
Intelligence and Machine Learning)
Malnad College of Engineering Hassan-573202, India
harshithabv2004@gmail.com

Manikya K

Computer Science and Engineering (Artificial
Intelligence and Machine Learning)
Malnad College of Engineering
Hassan-573202, India
manikya682@gmail.com

Dhavan H S

Computer Science and Engineering (Artificial
Intelligence and Machine Learning)
Malnad College of Engineering
Hassan-573202, India
limitsno886@gmail.com

Ankita

Computer Science and Engineering (Artificial Intelligence and Machine
Learning)
Malnad College of Engineering
Hassan-573202, India
ankitamawanti@gmail.com

Swathi H Y

Computer Science and Engineering (Artificial
Intelligence and Machine Learning)
Malnad College of Engineering
Hassan-573202, India
hys@mcehassan.ac.in

Abstract: As the need for improved campus safety grows, intelligent surveillance systems that can monitor and determine potential risks in real-time are being developed. This is particularly relevant for surveillance in large areas, as traditional methods are manual, which is bound to produce both inefficiency and oversight. This paper proposes an AI based intelligent surveillance system to help monitor and improve campus safety. The system being developed will utilize the You Only Look Once (YOLO) framework to provide real-time detection of people and vehicles. Detected people will undergo face detection using the Haar Cascade Classifier, and then the

detection and/or recognition of the face will be determined using the Local Binary Pattern Histogram (LBPH). Detected cars will have their license plates determined from using OCR. Because of this, the system will have an interactive database that provides the logs of the in and out of people and cars. There will be real-time notifications regarding people of concern, and responding to the repeated suspicious behaviour is managed by the system. The results of the system are the reduction in the need for human monitoring and the increased campus safety, as the system will have the ability to complete the tasks of an individual. This system is extendable, and a smart campus system is being developed for the system to be implemented in an economically careful way.

Keywords: Artificial Intelligence, YOLO, LBPH, OCR, Smart Surveillance, Face Recognition, License Plate Recognition, Campus Security

I. INTRODUCTION

All There are rising concerns about unauthorized access, theft, and vandalism to school property. These concerns have driven the importance of security on school campuses. Traditional security systems that rely on closed-circuit television (CCTV) rely on human operators. This is labour intensive, and operators are prone to miss things and react to things very slowly and inefficiently. Campuses are getting larger and more complex, and it is clear that human operators are not as productive as how fast (or slow) a human can react.

Artificial Intelligences (AI) and Computer Vision (CV) are able to automate the monitoring and analysis of surveillance video which is able to greatly increase and speed up security measures of surveillance systems. These systems are able to self-respond to security issues and threats with no or very little human intervention.

This paper proposes a security and monitoring surveillance system for school campuses using computer vision and integrating several techniques or tools within a unified framework. This system is sketched out using the computer vision tool called You Only Look Once (YOLO) which is used to detect people and vehicles in the surveillance video. Once people are detected, the system analyzes the videos further to detect faces using a classifier called Haar Cascade, and once a face is detected, the system recognizes the identity of the person with the Local Binary Patterns Histogram (LBPH) method. When a vehicle is detected, the system uses Optical Character Recognition (OCR) to monitor vehicle license plates.

The system keeps track of the campus entry and exit records for people and cars. There is also an alerting system to find unknown people and identify suspicious behavior, such as people entering and exiting the campus multiple times. This lets security personnel Intercept the campus to prevent a security breach.

The most notable parts of the project were:

- 1) Made AI-based multi-layer detection, recognition, and monitoring surveillance.
- 2) Made an automated entry and exit record log system for people and cars.
- 3) Made alerts for people and detection of irregular behavior.

The expected outcome of the project is to increase security for educational facilities with an automated, efficient, and scalable system that saves money.

II. LITERATURE SURVEY

A literature review has been conducted on multiple AI-powered surveillance systems that incorporate object detection, face identification, and Optical Character Recognition (OCR). The review examines methods including You Only Look Once (YOLO) and Local Binary Patterns Histogram (LBPH) aimed at enhancing safety and surveillance efficacy.

A campus surveillance system was designed to track individuals using face recognition and pre-registered databases. It enabled efficient monitoring of entry and exit activities within the campus. However, the lack of performance metrics and dependence on registered users limit its scalability and practical application[1].

A system was developed to automate attendance using real-time surveillance and face recognition techniques. It achieved very high accuracy under controlled conditions, showing its effectiveness. However, issues like poor lighting, pose variations, limited data, and privacy concerns affect its use in real-world scenarios[2].

A smart surveillance system was developed using real-time CCTV and object detection techniques to enhance campus security. It automated monitoring and alert generation through integrated technologies. However, continuous surveillance raises concerns related to privacy and data protection[3].

A system was developed to detect violent activities in campus environments by analyzing surveillance video sequences over time. It used action recognition techniques to identify suspicious behavior effectively. However, challenges such as real-time processing and false detections need to be addressed for practical use[4].

A study explored the ethical, societal, and legal aspects of facial recognition technologies, highlighting the need for proper regulations and accountability. It focused on real-world usage by organizations but did not include technical experiments or data analysis. The lack of practical validation limits its contribution to system performance evaluation[5].

A facial recognition system was developed to automate attendance using CCTV and deep learning techniques. It efficiently extracted key activities from video footage, making monitoring more effective. However, its reliance on a specific dataset and the need for retraining limit its adaptability to different environments[6].

A low-cost face recognition system was developed using embedded hardware and deep learning techniques. It combined multiple feature extraction and recognition methods to improve performance in practical setups. However, real-time efficiency can be affected by hardware limitations and processing delays[7].

A face recognition system was developed to handle masked faces in real-time using a custom deep learning model. It achieved good accuracy and worked well for single-face detection, making it suitable for practical applications.

However, performance dropped in multi-face situations and with variations such as non-frontal angles and children's faces[8].

A face recognition system was developed using a custom dataset collected under different lighting and angle conditions. The approach showed promising results by combining traditional and learning-based methods. However, the limited dataset size and lack of diversity may affect its performance in larger real-world applications[9].

A comparative study evaluated different face recognition models for attendance systems using standard preprocessing techniques. The results showed that deep learning models achieved higher accuracy than traditional methods, though performance depended on dataset size and computational requirements. The models were also affected by occlusions and varying lighting conditions, limiting real-world reliability[10].

A real-time facial recognition system was developed using deep learning and CCTV integration for surveillance. It performed well in identifying individuals from live video streams. However, its accuracy was affected by low-light conditions and changes in facial orientation[11].

A system was developed to improve facial recognition in low-resolution surveillance scenarios using advanced feature extraction and classification models. It showed good accuracy across different image qualities, but struggled with pose variations and limited dataset diversity. These factors reduce its effectiveness in real-world conditions[12].

A facial recognition system was developed using feature optimization techniques along with preprocessing and classification methods to improve suspect identification. The model achieved high accuracy on standard datasets but relied mainly on controlled, static images. This limits its effectiveness in real-world surveillance scenarios with dynamic and unpredictable conditions[13].

A facial recognition system was developed using face detection and recognition techniques to assist law enforcement. It performed well in controlled conditions with high accuracy. However, its performance dropped in low-light environments and with limited dataset diversity, affecting its reliability in real-world use[14].

A smart surveillance system was developed by combining multiple face recognition and feature extraction techniques. It used various methods to improve detection and recognition performance in campus environments. However, its effectiveness in real-world scenarios depends on computational efficiency and changing environmental conditions[15].

A campus surveillance model applied to the JMI-UCF dataset used prospected data from CCTV and UCF-Crime. JCF used I3D, C3D, and TSA Vision Transformer Hybrid. It achieved 96.26% precision and 95.9% accuracy. However, they are high GPU power thirsty, and low-quality and low-resolution videos caused I3D and C3D to malfunction while processing[16].

Another computer-based library surveillance system deployed YOLOv7 for object detection. Using a convolutional neural network (CNN), it performed face recognition on a library of images with a dataset of more than 7,000 images and achieved approximately 90.4% accuracy despite challenges with image quality, small or co-occluded objects[17].

A library CCTV system implemented YOLOv4 with CSPDarknet53 to achieve approximately 91% performance in real-time anomaly detection. However, it addressed issues with delayed processing, privacy, and inconsistent lighting[18].

Using FaceNet and YOLOv8, an artificial intelligence-based surveillance system achieved approximately 92% accuracy in detecting falls and 97.1% in detecting face recognition. However, it struggled with poor light conditions, occlusions, and raised privacy concerns with biometrics[19].

A surveillance system with an edge deployed Internet of Things (IoT) devices both to AI-powered monitor and reduce false positives, and to provide motion-activated monitoring. However, privacy issues and minimal performance metrics emerged with system calibration[20].

The studies reviewed show that with the use of the You Only Look Once (YOLO) and Deep Learning Model (DLM) approaches, AI-powered surveillance systems can achieve high accuracy in detection and recognition. Nevertheless, there are still issues, including high computational needs, sensitivity to lighting and image quality, and privacy issues. Thus, there is the need for an integrated and efficient real-time surveillance system, taking into account these shortcomings.

III. METHODOLOGY

An AI surveillance tool optimizes monitoring by streamlining the analysis of videos from multiple cameras. This tool can identify individuals and vehicles to log activities and track people of interest. The purpose of this system design is to perform automated surveillance.

Real-time object recognition through the YOLO algorithm involves the use of overlapping boxes around detected people and vehicles in each frame. YOLO is a fast and accurate process that objectively determines areas of interest. YOLO is then classified as a tool that is appropriate for surveillance.

Haar Cascade Classifier is then utilized to identify the presence of a face and draw the corresponding bounding box around each detected human. It extracts the specified images and thus further optimizes the process of identification through the use of recognition.

LBPH analyzes faces by comparing them to saved data. Users are classified as authorized when there is a match and unknown when there is not. This aids access control and identifies potential unauthorized users.

The OCR system is able to analyze and extract data from images of number plates. This data is converted to text and associated with the respective number plate. This allows for the tracking and monitoring of vehicle access to a number of areas.

A full record of this data is stored in a database for a number of purposes. This database enables the analysis of data related to the number of times an individual has entered/exited a specific location.

The data also allows for the auditing of security in the areas monitored by this system.

The system has a mechanism to identify potential threats. Alerts are generated when an unknown person is detected. Alerts are also generated when unusual patterns, such as entry and exit of a person or vehicle are observed. These alerts are communicated to management or security personnel. This enables intervention and prevents possible security incidents.

The proposed methodology combines computer vision techniques into a framework. By integrating detection, recognition, logging and behavioral analysis the system provides a solution for campus surveillance. It addresses the limitations of monitoring systems. The system provides an automated solution, for campus surveillance.

IV. SYSTEM ARCHITECTURE

The design of the AI-based smart surveillance system aims for modular design, real-time processing, and smooth data transfer for different components. The design infers a layered structure where each layer executes a specific task. This helps achieve scalability, flexibility, and easy system implementation for campus integrations. The system captures video, processes it through several AI-based modules, and produces outputs as identification, logging, and alert notifications.

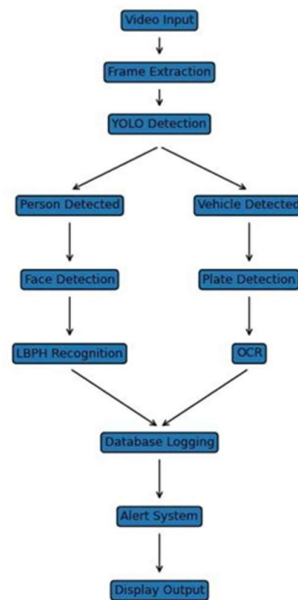


Fig. 1: Overall System Flow Diagram

As shown in Fig. 1, during the input stage, several surveillance cameras are placed around campus to stream several videos. The videos are segmented into single frames and sent to the processing layer. The processing layer computer vision frames to check the alignment of the frames and ensure compatibility of the frames to the models for detection and recognition. The basic system functions operate at the detection and recognition layer. In this layer, detection occurs through the You Only Look Once (YOLO) method to identify persons and vehicles. Depending on the type of the detected object, the data is streamed through either of the two parallel processing paths.

The Human Processing Path:

In this path, detected persons are first processed through Haar Cascade to locate the facial contours. The framed face is sent to LBPH where identity is

recognized and the system outputs the person's identity as either Authorized or as Unknown.

Path of Processing Vehicles:

Detected vehicles are processed with OCR to obtain license plates. OCR text facilitates unique identification to track vehicles entering and exiting campus.

The outputs of each path of processing are sent to the data management layer. This layer is responsible for packing information into a properly structured database. The database includes recorded identities, vehicle registration, and timestamps for the enter/exit events. This structured logging provides the means for perpetually active monitoring and analyses of campus activity.

To provide the system with advanced capabilities, an alert and monitoring module, sits on top of the data management layer. This module provides the functionality for analyzing incoming data, as well as stored logs, to identify probable security threats.

Alerts are generated under the following conditions:

- 1) Detection of an unknown individual not present in the database
 - 2) Frequent or repeated entry and exit of a person or vehicle within a short time window
 - 3) Unusual or suspicious movement patterns over a given time period
- These alerts notify management or security personnel to improve the ability of the system to manage and handle the risk.

The processed results are laid out and visually presented in the output layer. This includes the ability to provide alerts, detected system objects, real-time recognition, and license plate retrieval. The architecture consists of a stacked and modular design which balances system reliability with inter-component communication efficiency. It also provides system scalability.

V. IMPLEMENTATION DETAILS

Have introduced a smart surveillance system using artificial intelligence that efficiently processes real-time video streams using the Python programming language. OpenCV is an essential library that will help in the capture and preprocessing of video where the video will undergo resizing, grayscale, and removal of noise. This surveillance system will help in monitoring the activities that occur in various places of the campus.

Detecting, labeling, and tracking objects (and people) in a video stream using the You Only Look Once (YOLO) framework occurs in real time. This framework draws bounding boxes around objects it detected while classifying the detected objects. To help with the large numbers of processed object classes, class-based filtering helps with the load and improves the system's efficiency.

Training the detection framework to perform refined classification of the detected objects is done using a Haar Cascade classification method. This framework helps in real time analysis and classifying of several objects that can help in detection for monitoring the various tasks in a campus.

Haar Cascade improves image detection by converting images to grayscale and normalizing them. Detection performance is enhanced and activity tracking across the campus is made more reliable.

LBPH provides classification and verification of detected objects in real time. It analyzes the confidence scores of various activities. Based on these scores the system classifies activities as either monitored or restricted.

Once captured, the area containing the vehicle for the automated license plate capture (ALPC) process is cropped to contain only the vehicle and some background. The image is altered by correcting the geometry of the image and the background. After the image is processed, it is dropped to the Optical Character Recognition (OCR) system. These detection systems are deliberately used to track vehicles on campus automatically.

The system has a database module to store and analyze surveillance data. The database can analyze and store surveillance data on detected objects, and conduct real-time and retroactive surveillance analysis. The stored data would include:

- 1) User identity (authenticated/unauthenticated)
- 2) Detected vehicle plate number
- 3) Detected vehicle entry/exit duration

The analysis module improves the system's security by providing a set of alerts in chronological order. The module obtains surveillance data to analyze and evaluate possible threats. Alerts are issued in the following cases:

- 1) Detection of a new user while an individual outside of the supervised learning data is detected
- 2) Monotonous entry-exit of people/vehicles within a specific time threshold
- 3) Activities classified as potentially threatening based on recorded data analysis

These alerts are communicated to campus management/security personnel to take the appropriate action.

The system aims for the optimal balance between modularity, flexibility, simplicity, and speed. The system has rapid adaptability to different environments, allowing for a range of different campus uses.

VI. RESULTS AND DISCUSSION

Analyzed the performance of our AI-powered smart surveillance system using real-time video feeds that mimic the video surveillance conditions present on a campus, including varying levels of movement, illumination, etc. The performance of the system was analyzed based on the level of accuracy in detection, efficiency of recognition, reliability of the alerts, and the speed of processing.

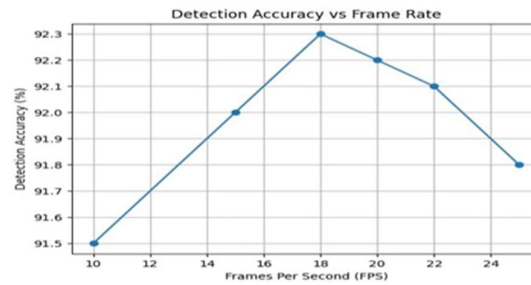


Fig. 2: Detection Accuracy vs Frame Rate

The surveillance system based on the You Only Look Once (YOLO) architecture for the purpose of detecting and tracking objects was seen to achieve good performance in real time. The average processing performance was calculated to be 92.3% for the detection of people and vehicles. The processing speed was observed to be around 18–22 frames per second (FPS), ensuring smooth real-time monitoring. As shown in Fig. 2, detection accuracy shows that the model was able to achieve a good detection accuracy with high frames per second.

The system performing facial detection and recognition using the Haar Cascade and LBPH for face recognition achieved an accuracy of approximately 87.5% under normal light conditions, while for dim light conditions, the accuracy was between 80-82%. The system is sensitive and adaptive with changing conditions of illumination as shown in Fig. 3.

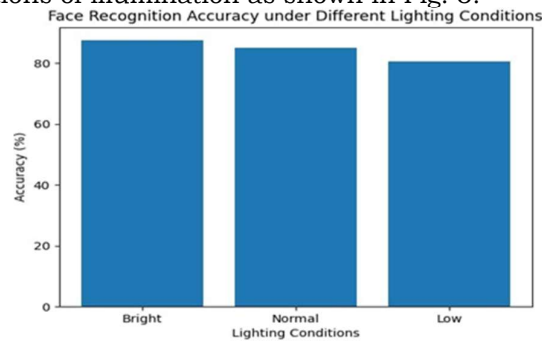


Fig. 3: Face Recognition under Different Lighting Conditions.

The accuracy of the optical character recognition system assigned to the recognition of vehicle number plates was 85.2% and 75-78% for images of clearer and more blurred images, respectively. The effect of the blur condition of the images on the performance of the optical character recognition system is shown in the Fig. 4.

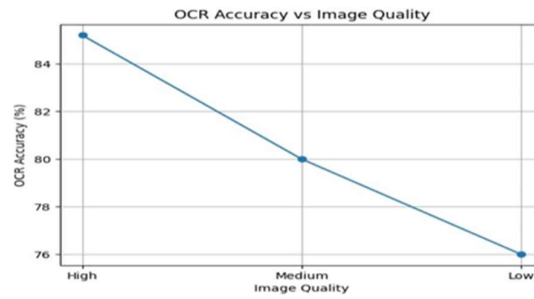


Fig. 4: OCR Accuracy vs Image Quality

The logging and alert module of the system achieved 100% accuracy of the recording of the entry and exit events. As shown in Fig. 5, the alerts that were mostly sent to the monitoring operator were based on the detection of unknown people, while the entry and exit alerts were mostly sent to the operator for the repetitive detection of people.

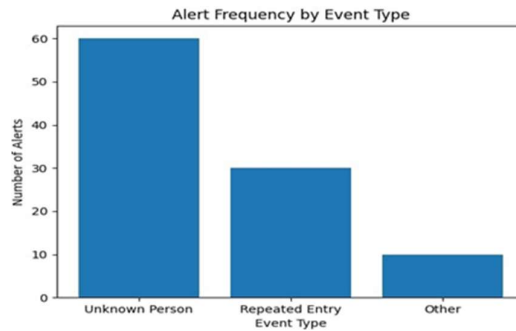


Fig. 5: Alert Frequency by Event Type

To evaluate the effectiveness of individual components in the system, a quantitative comparison of model accuracy is presented in Table 1.

Table 1: Accuracy comparison of models used in the proposed system

Model	Task	Accuracy (Normal Condition)	Accuracy (Challenging Condition)
YOLO	Object Detection	92.3%	89–90%
Haar Cascade	Face Detection	90.1%	85–87%
LBPH	Face Recognition	87.5%	80–82%
OCR	Number Plate Recognition	85.2%	75–78%

The YOLO model demonstrates the best results for accuracy compared to all other model components, underlining the model's suitability for real-time applications. The Haar Cascade classifier provides efficient, accurate results for locating faces, and LBPH provides moderate accuracy for recognition. The performance of OCR compares poorly to the others under suboptimal conditions as it is more dependent on the quality of the input image.

The combination of detection, recognition, and monitoring provides detailed tracking of the campus activities. The system is both accurate and dependable under the conditions of the evaluation.

Some barriers are also evident. LBPH performance is also influenced by Lighting, quality of the image as well as the environmental conditions. Although YOLO detection accuracy is very high, all the other system components are also dependent on the performance of the other components working in the detection pipeline.

In summary, the system is flexible enough to allow the balancing of the accuracy and real-time issues. This makes the system appropriate for implementing in campus environments. Further functioning of the system may also be improved by implementing several advanced deep learning strategies.

VII. CONCLUSION AND FUTURE WORK

In this study, we developed an AI-driven surveillance system designed to monitor campuses and automatically spot potential threats in real time. By bringing together YOLO for object detection, LBPH for facial recognition, and standard OCR, our setup successfully tracks both people and vehicles. We also tied in automated logging and alert systems to quickly flag unfamiliar faces or suspicious behavior.

Our tests showed that the system runs smoothly in real time, offering a solid alternative to having security staff manually watch camera feeds around the clock. However, we did run into a few hurdles: the OCR and face recognition modules still struggle when the lighting is poor or the video quality drops.

Moving forward, we plan to upgrade the facial recognition to a more robust CNN-based model to handle those environmental issues better. We're also looking at shifting the system to cloud or edge platforms to improve scalability, and adding predictive analytics to our alerts to catch threats even earlier.

In conclusion, the AI-based surveillance system described in this proposal meets the modern campus security system requirements and integrates real-time detection, identification, and intelligent surveillance in a single system..

REFERENCES

- [1]. Sarikonda, P., & Bhutada, S. (2020). Customized campus surveillance system.
- [2]. Sreekantha, B., Vijayalakshmi, S. A., Prasad, H. B., Hrithik, C., Nagajyothi, M. S., & Rakshitha, . (2021). Face-based CCTV attendance monitoring system using deep face recognition.
- [3]. Junaid, N., Khalid, M., Saunshi, N., Mehta, P., & Thippeswamy, M. N. (2021). Smart College Camera Security System using IOT. In Lecture notes in electrical engineering (pp. 295–309).
- [4]. Ye, L., Liu, T., Han, T., Ferdinando, H., Seppänen, T., & Alasaarela, E. (2021). Campus violence detection based on artificial intelligent interpretation of surveillance video sequences.
- [5]. Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology.
- [6]. Kagona, E. (2022). Facial recognition attendance scheme on CCTV cameras using Open Computer Vision and deep learning: A case study of International University of East Africa (IUEA).
- [7]. Zamir, M., Ali, N., Naseem, A., Frasteen, A. A., Zafar, B., Assam, M., Othman, M., & Attia, E A. (2022). Face detection & recognition from images & videos based on CNN & Raspberry Pi.
- [8]. Golwalkar, R., & Mehendale, N. (2022). Masked-face recognition using deep metric learning and FaceMaskNet-21.
- [9]. Nurpeisova, A., Shaushenova, A., Mutalova, Z., Zulpykhar, Z., Ongarbayeva, M., Niyazbekova, S., Semenov, A., & Maisigova, L. (2022). The study of mathematical models and algorithms for face recognition in images using Python in proctoring system.
- [10]. Budiman, A., Fabian, F., Yaputera, R. A., Achmad, S., & Kurniawan, A. (2022). Student attendance with face recognition (LBPH or CNN): Systematic literature review.
- [11]. Irfan, E., Jacob, C., & Resmi, R. (2024). Facial recognition and CCTV integration for enhanced security using deep learning techniques.
- [12]. Surantha, N., Yose, E., & Isa, S. M. (2024). Low-Resolution face recognition for CCTV and EdgePowered smart attendance systems.
- [13]. Sari, S. A., & Sulistiyo, M. D. (2024). Suspect Identification Based on Facial Recognition from CCTV Using Hybrid Bat Algorithm.
- [14]. Chittibomma, S. S., Surapaneni, R. K., & Maruboina, A. (2024). Facial Recognition System for Law Enforcement: An Integrated Approach Using Haar Cascade Classifier and LBPH Algorithm.
- [15]. Keerthana, P., Prasath, S., Tamilmani, S., & Veeragokulraj, S. (2024). Enhancing campus security through smart surveillance system.
- [16]. Mishra, S., & Jabin, S. (2024). Enhancing campus surveillance using temporal self attention.
- [17]. Deepalakshmi, R., Murugan, K. R. S., Arunnachalam, R. S., & Asif, M. B. (2024). Campus surveillance: Deep learning-based rules violation detection.
- [18]. Olorunyomi, G. T., Babalola, D. A., Tihamiyu, A. T., Aliyu, B. A., & Ojajuni, D. (2025). Exploring the integration of deep learning in CCTV systems for enhanced security measures in academic libraries.
- [19]. Anand, P. D., Umasankaran, R., Joshi, N., & Mamtha, K. R. (2025). Optimized CCTV monitoring using biometrics and AI-driven surveillance.
- [20]. Chahande, M., Yadav, L., & Wadhibhasme, B. (2025). Creation of an automated video surveillance system using IoT and AI systems.