Guardian Eye: Real-Time Surveillance Monitoring with Automated Alerts Using Deep Learning

K. Kishore[1], Vamshi Edla[2], P. Keerthana[3], B. Harinath[4], T. Sharon Peter[5]
[1]*Assistant Professor, Vidya Jyothi Institute of Technology, Hyderabad*
[2,3,4,5]*UG Student, Vidya Jyothi Institute of Technology, Hyderabad*

Abstract—**With the global urbanization, and the public safety requirement to quickly grasp the situation in its first time, intelligent and automatic surveillance has become a hot issue. Guardian Eye A ground-breaking system developed to monitor surveillance in real-time and boost security both for public and private environments Traditional CCTV systems heavily depend on round-the-clock human observation, causing bottlenecks like human fatigue, longer response times, and wasted valuable seconds. These limitations strongly indicate some kind of automation within the modern frame work of surveillance. Guardian Eye uses cutting-edge technologies like AI, ML and CV to tackle this. It automatically analyzes live video streams for violent or nefarious activities. Under the hood, it is powered by a deep learning–based image classification model trained with Google Teachable Machine. Deploying the Model For deployment, we use TensorFlow. js, allowing in browser real-time processing. It captures frames from live video and sends them through the model that is trained. An alert mechanism gets triggered when the probability of violence is ≥ 95 %. This includes triggering an audible warning and a warning on the screen, along with recording a snapshot in time. Details like GPS location, time, confidence level and image captured are sent in an email notification. Guardian Eye uses React 18 with TypeScript, Tailwind CSS, and Vite as build tool. Includes Email.JS and imgBB APIs for alerts and hosting captured images. The entire system works on client side without any backend infrastructure. Scalable, affordable, easy deployable solutions for Institutions, Workplaces, Transport Systems, Healthcare and Smart City.**

Index Terms—**AI, techniques for deep learning, CV systems, real time surveillance, violence detection system, intelligent monitoring system and automated alert systems as well as video analytics on CCTV footage, human activity recognition and smart security solutions.**

I. INTRODUCTION

Due to urbanization, population growth and social complexity in the modern era, security and public safety have become an essential issue for all governmental, institutional and organization sectors. To safeguard persons, possessions and vital infrastructure from unlawful acts; surveillance systems need to be ubiquitous in deployment plus intelligent, high-fidelity, efficient, and possess the ability to operate indefinitely without loss of function. Over years Closed-Circuit Television (CCTV) systems have become the most commonly adopted solution of physical security across the globe. CCTV acts as a core element of surveillance infrastructure by creating secured environments in places like cities, shopping malls, school and university settings, hospitals and transport hubs.

It is estimated that over a billion CCTV cameras are in use worldwide today, and this number has been irreversibly rising year on year. These platforms produce an immense amount of video data on a continuous basis. This data holds enormous potential security insights, but remains untapped for the most part with traditional surveillance systems being passive. Traditional CCTV systems only record, store and playback video footage they cannot interpret or analyze the visual content of what they are capturing. As a result, the responsibility to monitor activities and identify suspicious ones lies wholly with human operators.

But human oversight has some serious drawbacks. Research from the fields of attention and vigilance indicate that human focus is rapidly declining over long length of time, usually in a matter of minutes. In large surveillance settings, where operators have to simultaneously observe several video feeds, missing

significant events can occur with great regularity. Moreover, by combining human decision making and the coordination of response based on detection events or alerts, either by command center personnel or the army presiding officer we may suffer times during crisis instead of having rather immediate reaction against the threat.

Recent developments in Artificial Intelligence (AI)Machine Learning (ML), and Computer Vision (CV) have opened doors to new ways of tackling these issues. Specifically, deep learning methods such as Convolutional Neural Networks (CNNs) have allowed systems to process visual information with a high degree of accuracy. Trained on large amounts of data, these models are able to generalize and to learn to discern patterns, objects and movements in those images so that they can be applied back to new data in real-time.

Such technologies take surveillance out of passive monitoring and instead, towards active support of understandable theory. Contemporary frameworks can go beyond the mere recording of footage, to continuously assess video streams for anomalies or threats, treatment as well and launch immediate responses without human mediation. More importantly, it is a big leap in security technology.

Guardian Eye is built on this structure and has a real-time monitoring system that integrates image classification based on deep learning with up-to-date web technology. A near real time architecture that can automatically sense violent events and alert instantly. Guardian Eye provides a simplified solution to overcome the shortcomings of traditional surveillance systems and offers a proactive, reliable, and automated solution for enhancing safety and security across various environments by embedding intelligence into the surveillance process.

II. LITERATURE SURVEY

Over the last few years, numerous automatic surveillance systems based on CCTV have been installed in public places, schools and universities, business facilities, and transport to enhance safety and security. Such systems produce real-time video data that need constant supervision. It goes without saying, but it is ineffective and impractical to manually inspect this much video footage. As a result, human operators are limited by their propensity to fatigue and focus over time, delayed decision-making, and the potential for missing key events. These difficulties have a profound impact on the traditional surveillance system, and emphasize the importance of intelligent and automated monitoring methods. Consequently, integrating Artificial Intelligence (AI) and Deep Learning (DL) techniques in surveillance systems has generated increased interest to facilitate automated video data analysis.

There have been several research contributions dealing with various facets of intelligent surveillance. YOLOv3 is easily one of the most popular architectural frameworks for fast and real-time object detection by processing the image in a single pass. This is ideal for use of applications such as CCTV surveillance that depend on speed. Nevertheless, although YOLOv3 is efficient to use it can only detect objects and has no ability of reasoning the relationship between the object with one or many others, which an essential approach for determining complex events like violent acts. FACE detection and recognition methods such as FaceNet are based on similar premise of this to highlight the individual characteristics of facial features that an individual has. Although those methods are perfect for identification and tracking, they have no information regarding its behavior or what it was doing inside a scene.

Furthermore, weapon detection systems were created to detect things that could pose a danger - guns and knives from video images. And, though these systems can help us signal potential dangers, it is an incomplete picture because numerous violent events occur without visible weapons. Thus, weapon detection alone does not allow the system to identify a diverse range of violent acts. The use of hardware platforms like Raspberry Pi has also been proposed as a low-cost surveillance solution where the cost involved in setting up a whole new complex surveillance system can be reduced. While these systems enable basic real-time monitoring, they lack the necessary processing capabilities, memory capacity and operational efficiency to deal with complex analysis tasks or large-scale deployments.

Some research works also condense that behavior monitoring and security of information in surveillance systems are necessary. Behaviour monitoring allows for the analysis of patterns and detection of anomalies as time passes, meaning it is immensely helpful when identifying unusual or suspicious behavior. Every

video holds sensitive information hence, data security, prevents unauthorized access to illegal use of any vital video information. But these studies tend to focus these aspects separately and fail to provide a holistic solution for real-time video-based detection of violence.

However, a number of limitations remain in this area despite the advances made. State-of-the-art techniques mainly focus on detecting objects or face-recognition, but human action and interaction play an important role in violent behaviour identification. Other systems fail to provide alert mechanisms, which immediately notify authorities when a threat is identified. Moreover, they frequently lack a unified ecosystem that combines detection, analysis and response into one body. A second significant limitation is the insufficient resilience of available models in naturalistic scenarios, where poor illumination conditions, camera angle heterogeneity, how occlusions manifest and how human interactions may complicate recognition influence performance and reliability.

Thus, the need for a complete and responsive surveillance system that combines activity recognition, real-time processing, automatic alert generation and secure storage of data under one framework highlights. This system_ to identify violent activities, it must be able to recognize violent activities even under a diversity of real-world conditions with little or no delay time in providing response optimizing for timely intervention. The identified research gap is the motivation behind the development of Guardian Eye which provides a highly sophisticated, scalable and reliable automatic surveillance solution.

III. METHODOLOGY

The proposed system in their work closely focuses on designing an intelligent surveillance framework wherein the authors designed one that enables to use of Artificial Intelligence approaches, Deep Learning techniques and Computer Vision approaches for automatically monitoring them and analysing the information captured from CCTV video streams. A pipeline is constructed which consists of data acquisition, preprocessing, inference using the model, decision making and generating alerts.

At first, you will be getting the live video streams which are coming from CCTV cameras and it will process frame by frame. To standardise the model input, these frames are pre-processed to achieve uniform sizing and resolution with proper quality conditions. Subsequently, these frames are fed to a pre-trained deep image classification model. In this, the model has been trained for identifying normal vs violent or suspicious activities from learned patterns over well labeled datasets.

For every frame, the system monitors and calculates a probability that violent activity is occurring. A threshold value to classify the detected activity as suspicious or not is provided. If the confidence score of it is just above this threshold, it'll come through as a potential threat to the system.

When a threat is identified, the system starts an automated response process. Such as generating alerts and notify concerned bodies through email, SMS or other messaging channels. Also, Data such as timestamp, detected activity and captured frames are saved for additional studies and records.

The methodology also includes the interface side which is an admin dashboard, used by authorized users to monitor live feeds, review previous incidents and control alerts efficiently. The organized method guarantees that the framework is run continuously; requires less human collaboration, and enhances the dependability of observation tasks.

3.1 Proposed Methodology

The self-proposed system, named Guardian Eye, is established as high-end live monitoring mechanism which employs deep learning-based activity recognition and automated alerting systems for improving the existing security surveillance. While traditional CCTV systems require viewers to observe feeds, Guardian Eye monitors video streams intelligently around the clock, allowing for immediate detection of violent and abnormal activities.

The system first gets the live video feed from surveillant cameras. The solution divides each video stream into frames and processes these individual frames in real-time with a deep learning model responsible for detecting violence. The model specifically analyses the visual features like motion patterns, human interactions, and abnormal behaviour to categorize the activity in every frame. This includes using computer vision technology to analyze complex situations like physical altercations, aggressive behavior or suspicious movements.

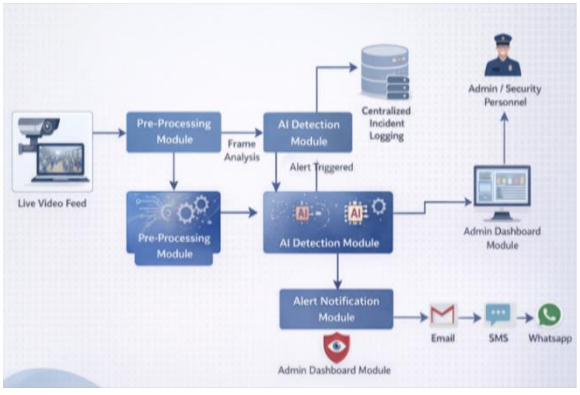
One of the main aspects of the proposed methodology is a confidence threshold mechanism. The system responds automatically by issuing an alert as soon as the probability of violence identified by our model crosses a pre-defined limit. The alert dashboard is a multi-channel notification system that works through e mail, SMS and messaging services like WhatsApp. It generates real-time alerts, minimizes response time, and allows security personnel to intervene as soon as possible.

Besides detection and alerting, the system contains a centralized storage mechanism in which all detected incidents are stored safely. This includes saving snapshots, timestamps and relevant meta data to be used for future analysis reporting, and evidence. A centralized database enables quick management and retrieval of data.

Key Highlights of the System admin dashboard allows them to have one view of monitoring and control This dashboard gives the authorized user an option to view live video streaming, recorded incidents and alerts. It increases situational awareness and assistance in making decisions.

Additionally, the system is intended to be scalable and implemented across all environments, including public spaces, education institution sites (such as schools or campuses), corporate office buildings and transportation infrastructure. Guardian Eye automates surveillance procedures, reducing human dependency and fatigue-based errors while ensuring reliable and consistent monitoring for all hours of the day. By integrating real-time analysis, intelligent detection, and automated response mechanisms, the overall methodology proposed provides a method that is pro-active and efficient for solving modern security challenges.

IV. SYSTEM DESIGN



The system architecture diagram shows the overall structure of Registry Guardian Eye surveillance systems and visualizes the general flow of data between its main components. It starts with CCTV cameras or webcam that sends continuous streams of live video footage from the monitored environment, allowing for 24/7 surveillance.

Then the taken video is sent to preprocessing module which frames converts it into multiple raw images. Hence, for input of detection model these frames are resized, normalized and augmented (in order to increase detection model performance).

After this preprocessing, the frames are sent to the AI-based detection module. In this module, deep learning techniques are employed to recognize patterns in visual data relevant to abnormal behavior or violence. The entire system works on each frame in real-time, detecting possible danger ahead of time.

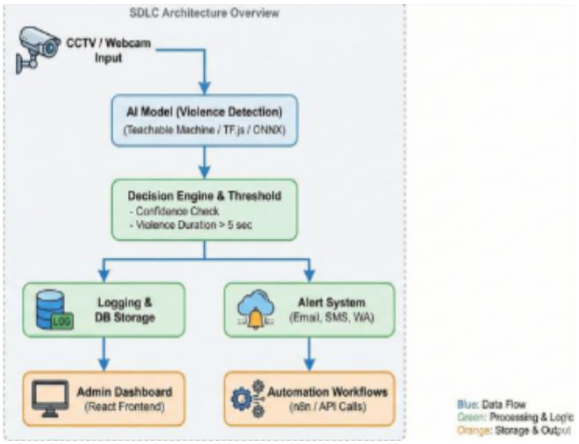
A decision-making unit then reviews what the detection model outputs. This piece of the action reviews an assurance score to choose whether that noticed activity is a danger. It requires that the predictions on several continuous frames should be consistent to avoid false positives.

An alert mechanism then comes into play when the activity detected exceeds the threshold established a priori. The notifications are immediate and actionable, reaching needed recipient via email, SMS and messaging channels so that authorities can respond quickly.

Simultaneously, all the detected events are permanently logged in a central database along with relevant information such as date and time of occurrence, its location and some captured image proof. It keeps this data for future analysis, reporting and logging purposes.

Lastly, there is an admin dashboard where a user can easily manage everything in one place. Users can see live video, view playback of recorded events and manage real time alerts. Thus, in general this achieves the goals of real-time detection, quick and timely response, also capable of surveillance management.

2. System Architechture Diagram



The Software Development Life Cycle (SDLC) architecture of the Guardian Eye system is structured and systematic, allowing a reliable, scalable, and real-time surveillance solution to be developed. The design process begins with requirement analysis where critical use cases like continuous video monitoring, accurate violence detection, an alert generation in real-time and incident management are identified. The system is structured into several layer levels to accomplish these fequests with better performance, scability and maintainability.

The live video streams are being captured with the help of CCTV cameras or newly placed webcams in the environment. The feeds of these videos are continuously streamed to the processing layer where each frame is extracted and passed through a model for scrutiny. The AI-based detection module is the main Part of the system, capable of real-time assessment of each processed video frame to recognize violence or abnormal activities using deep learning methods. It doesn't require the human eye to monitor constantly and accelerates threat detection while improving accuracy.

The decision-making module receives the results, which are usually made from the detection process. This module assesses the output: it determines if an activity is detected on a surface area by checking for attributes like confidence score, temporal consistency. The system confirms only the real threats and not repetitions, therefore by analyzing several consecutive frames, it reduces false positive. When the detected activity goes beyond an established point, it is considered a potential threat.

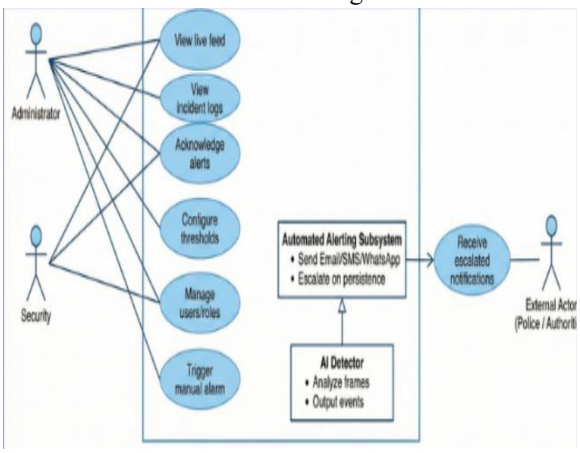
After this, an automated alert system is triggered. They dispatch the alerts by different communication methods such as email, sms or instant messaging services like WhatsApp directly to concerned authority. This enables you to respond quickly to critical incident management and take immediate action.

At the same time, all identified events are safely stored in a single database. The data are saved for future reference and could include the time of day in which the results were detected, whether the target was identified correctly, as well as photographic evidence. This helps the system in record keeping and decision making.

It also provides a frontend dashboard for administrators to easily navigate through the system. Users can use this dashboard to see live video feeds, view detected events, and handle alerts more conveniently. Centralized governance enhances usability and operational effectiveness.

In summary, this SDLC architecture helps to build the Guardian Eye system that works in a complete manner, with real-time processing, accurate detection and good surveillance management.

3. Use Case Diagram



The use case diagram represents the interaction between the main actors and Guardian Eye functionalities, and gives us a clear view of how users will be working with that system. The primary actor associated is the admin (User), which is defined as this user will be interacting with the system to monitor activities, for alerts and overall management tasks.

As mentioned before, the diagram describes a few important use cases that describe how the system

behaves. These consist of user authentication, real-time video surveillance, suspicious or violent activity triggers and alert notification handling for emergency personnel, as well as stored incident record reviews. Authentication use case ensures that only the users who are authorized, gets to access the system. After login, admin able to watch the live video streams and provide a continuous overview of the monitored area.

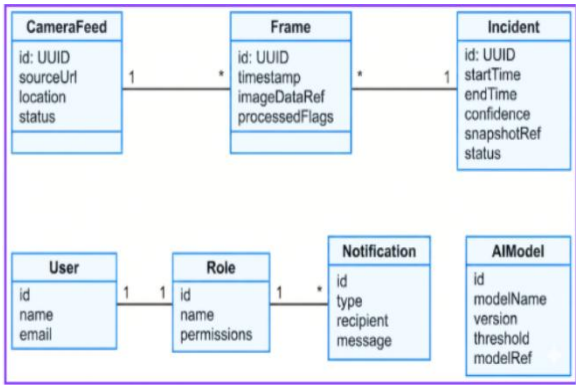
The diagram shows a key feature of the automated detection mechanism, where the system processes video streams to detect unusual or violent events. When these get detected, it triggers an alert use case, notifying the admin immediately. Their ability to surface and react to threats provides timely knowledge, enabling them to respond efficiently.

This diagram also shows the incident management functionality where all detected events are stored in the system with information related to this event. The stored data can then be accessed by the admin to perform analysis, verify or generate a report on top of it.

Moreover, the use case diagram specifies system boundaries by clearly identifying user actions from internal processes of the system. The only direct aspect of the human experience with something like this will be when the admin interacts with the likes of monitored features, alert management etc. But the background (like detection and decision making through AI) operates from inside without users directly involved in its operation.

In conclusion, the diagram is one way of organising user-system interaction by giving a good structure over what functionalities that need to be in place before starting any implementation work. This aids in lucid system design and farming out the effort of development and deployment better.

4. Class diagram



Class Diagram

A class diagram can display structural information for the Guardian Eye system by outlining its fundamental classes, their relevant attributes, and the relationships established between them. This depicts what those are and how they interact with each of those elements in the system.

The main classes found within the system are User, CameraFeed, Frame, Incident and Notification which serve particular functions. The User class that represents the administrator interacting with the system and consists of attributes user id, name, Email Id and contact details. Handles authentication and gives access to system features like monitoring or alert management.

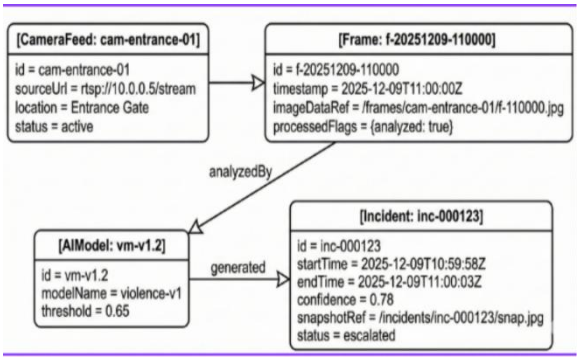
CameraFeed is the video input source that streams in along with live feeds of CCTV cameras or webcam input classes. The Frame class takes care of single frames extracted for analysis from these video streams. The AI model processes data per frame so each frame acts as a unit of data that is checked for suspicious and violent activity.

In our system, all detected events are stored in the Incident class which is the base of any incident. It consists of timestamp, the type of detection (whether it is violence or normal activity), confidence score and image evidence. This class stores any detected events to view later.

It provides means to manage information related alerts. (details can be found under Notification class) It holds information such as the alert text, who it was sent to and its delivery status. This allows the system to alert users as soon as a possible danger is identified. Relationships between these classes are what determines how data flows throughout the system The User is able to watch multiple CameraFeeds and get many a Notifications. A single CameraFeed generates many Frames which in turn are examined to produce Incident records. These incident records are then associated with notification to fire.

This organized architecture guarantees effective data handling and smooth communication between elements of the system. It also gives a well-defined roadmap for developers to implement, maintain and scale application in future.

5. Object Diagram



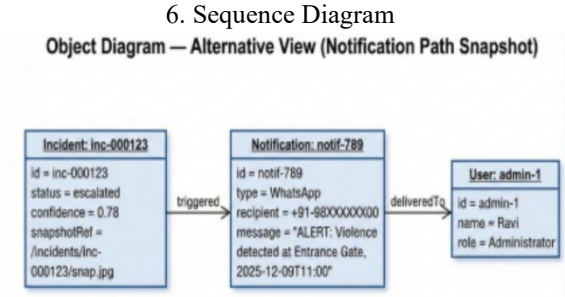
The object diagram gives a view of the Guardian Eye system at runtime, and shows how different individual instances of system components are interacting, in that one particular moment. It describes the behavior of the system in terms what data flows through which objects during runtime.

In a common pattern, a Camera Feed instance streams live video and produces a Frame object each time it captures an image at some point in the stream. The AI detection model analyzes the frames, determins if there is some abnormal behavior or violence. From that analysis, when suspicious activity is detected an Incident object gets created.

The Incident object includes many relevant details such as time of detection, activity type and detection confidence. This representation offers an insight into how the raw input data is converted to the output data in a structured manner. It also indicates what objects interact with one another CameraFeed Frame AI Model Incident at run-time.

Additionally, the object diagram is also useful for confirming the integrity of a system in addition to debugging and testing because it shows how data is handled, saved, and connected between various components. This approach maintains consistency between runtime behaviour and the system design and helps facilitate mapping between data states to database records.

6. Sequence Diagram



The following sequence diagram depicts the temporal order of how different modules of Guardian Eye interact with each other during the detection process and alert generation. It depicts the progressive steps in the communication and processing of information over time.

Real-time video capturing by the camera and frame forwarding to preprocessing phase Frames are sent to the AI detection model for on-track analysis or threats or abnormal activities. When any such activity is detected, the result is forwarded to the decision engine for a verification process.

A decision engine then also takes into account different parameters (for example, confidence score, the amount of time present or consistency across multiple frames) in order to avoid false positives. If the set threshold conditions are satisfied, the system confirms that an incident has occurred.

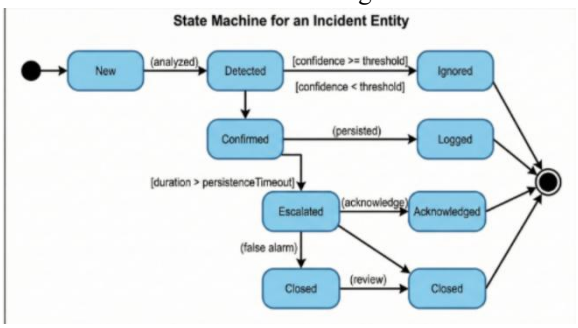
After confirmation, there will be an Incident record with a timestamp, activity label, score and image evidence stored in the database. Then, the alert information is packed into a Notification object.

This notification is then processed by the alert module and it formats and sends out messages via various Mediums which includes E-Mails, SMS, WhatsApp. In addition, the system saves delivery status of notifications to provide reliability and retry mechanisms when needed.

This diagram effectively portrays the sequence of operations between each component in this system like camera, preprocessing unit, AI model, decision engine and notification service (Database). It assists to check for delays, synchronize modules and validate the entire workflow.

In sum, sequence diagram validates that the system functions well as timely detection, effective alarm generation and reliable communication will enhance live surveillance capability.

7. State Chart Diagram



The state chart diagram shows the life of an Incident object existing in Guardian Eye system. An incident object has a lifecycle that starts with detecting some condition, it is added to progress for further processing and finally resolved or closed when no more actions are required on it, The result is an orderly view of how the system worka with incidents under certain conditions and events.

The AI detection model classifies such a behavior as abnormal and creates an incident in the NEW state. Now once the system picks up some more input video frames to analyze, the incident might get switched to Detected state meaning some suspicious/abnormal behavior has been identified.

After being detected, the next stage of validation based on parameters as confidence score, duration of activity and challenge across many frames. Once these conditions pass the static threshold condition defined, then the incident moves to "Confirmed" state. That shows only possible threats before proceeding to further processing and eliminating false positives.

The incident is confirmed and enters its “Logged” state, where all related information (timestamp, type of activity CCTV confidence score and image) is recorded in the database. This allows to maintain proper records and conduct future analysis and reporting.

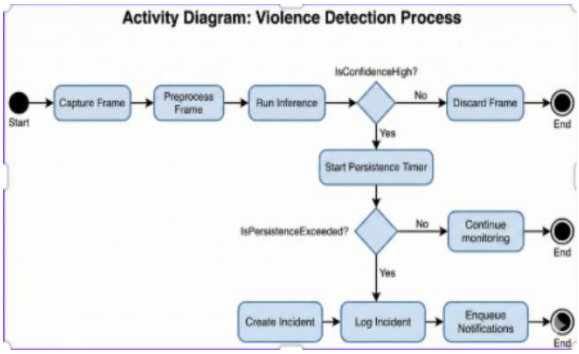
The system, thereafter, escalates the incident to higher authorities in situations where the detected activity is sensitive or goes on for an extended period. At this point the incident moves to Escalated state, and alerts are generated and sent through channels such as email, SMS, messaging system.

The incident stays in this state until it is acknowledged or resolved by the responsible party. If the alert is confirmed as bad, it may be marked false and closed. If it is then the appropriate action takes place and the incident settles.

Besides, the state chart also has additional features like timing constraints, retry policies and escalation policy. It makes sure that every incident goes through a standardized process, increasing system reliability, traceability or efficiency of response.

In essence, this diagram represents a high-level view of incident management within the Guardian Eye system, which covers how incidents are tracked and responded to with relevant alerts sent in a timely manner for threat response.

8. Activity Diagram



The activity diagram describes the sequential workflow of the Guardian Eye system while processing video frames in real time. It demonstrates how data goes from video capture to alert generation.

It all begins with acquiring real-time video frames from CCTV cameras or webcams. It passes these frames to ein preprocessing stage, they are resized, normalized and augmented.

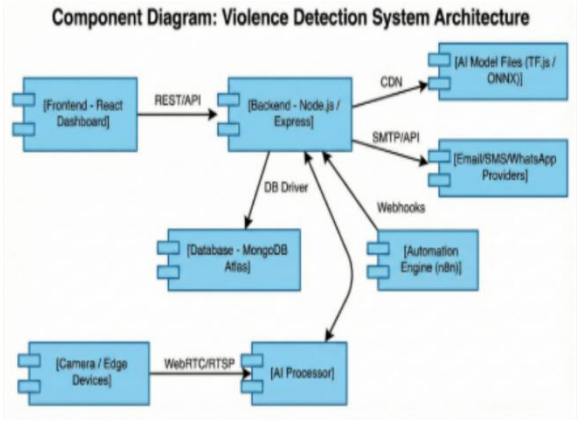
Then, these frames are fed to the AI model which infers whether any violent or unusual activities and generates confidence scores. The system then verifies if the confidence level exceeds a fixed threshold for reliable discrimination.

If the requirement is met, an Incident is created with timestamp, activity type and confidence as well as image evidence. This information is then saved in a database to be referenced later.

The last step is sending alerts via email, SMS and the chat app so that authorities can be informed immediately.

In summary, the activity diagram clearly depicts how the system operates to perform fast detection and data storage and real-time alerting.

9. Component Diagram



We divide the components by major functional and deployable components to provide a high-level structure of Guardian Eye system in a component diagram. That depicts the ways they connect with each other to do up real-time view and alert.

This may be a system, which comprises components like frontend, backend, databases, hosting the AI models, an AI processor that processes and serves machine learning models to bring smarter apps to life in production along with notification services and an automation engine. Frontend: A user interface for administrators to view live video feeds, alerts, and operate the system.

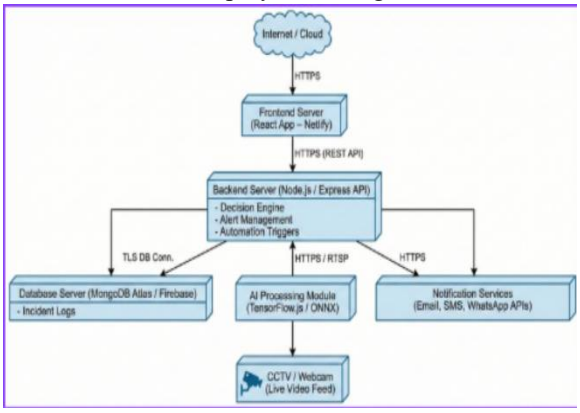
Backend is the part where core features and functions are carried out, such as business logic, data processing, communication between modules. Incident Information such as timestamps, detection results and the evidence of image are stored in a database which is used for asynchronous and reliable data management.

AI model hosting component hosts the trained deep learning ANN (Artificial Neural Network) model while AI processor analyzes video frames in real-time to detect abnormal or violent activities. Used to send alert notification through email, SMS and messaging services.

To communicate between all the components and to enable us to automate tasks such as generation of alerts and data updates, an automation engine orchestrates workflows.

Conclusively, the component diagram sorts system on a hierarchical basis whilst guaranteeing scalable modularization and its connectivity by representing how the entire components interact to achieve systems determined functions.

10. Deployment Diagram



The deployment diagram represents the physical distribution of components between the cloud and edge environments by which different parts would be deployed together in an actual system environment.

The front-end is developed using React and can be hosted on any cloud provider such as Netlify, which gives an interface for Admin users to view live video feeds of the camera, alerts and system activity. It securely communicates with the backend server (which is built using Node). js, responsible for core functions such as API management, data processing, and integration between systems.

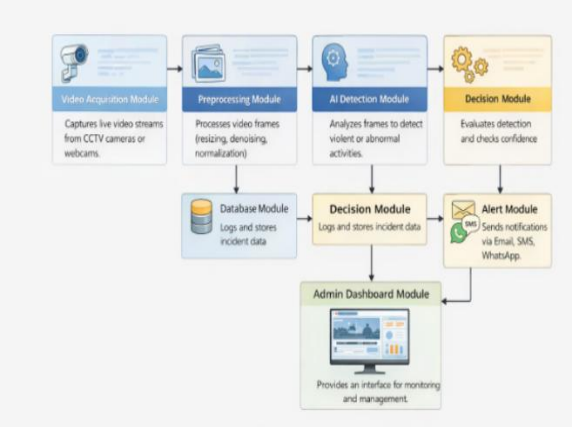
The AI module is fed real-time data from live CCTV cameras or webcam video streams. This can be performed on all three different systems -- client-side, server-side and edge (depends on the configuration) to maintain low latency conversation in real-time.

All the incidents detected are stored in a cloud-based database, allowing safe storage, easy access and scalability. It is also able to interface with external notification services emails, SMS and WhatsApp APIs too to send latest information on alerts directly to authorities.

It uses secure communication such as HTTPS and TLS to protect data transmission, also ensure the integrity of the system.

In a nutshell, the deployment diagram helps in visualising system distribution that increases scalability and flexibility for real-world implementations.

11. Module Design



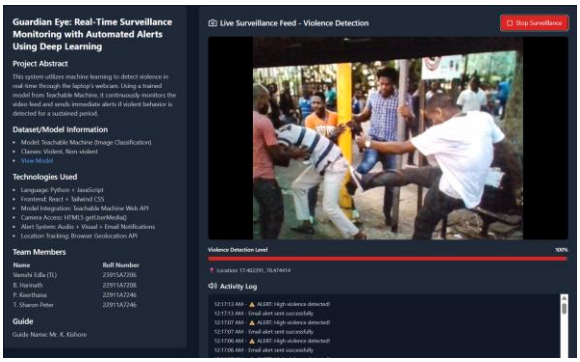
Guardian Eye system has a modular architecture, allowing for scalability, efficiency, and easy maintenance. The Video Acquisition Module is a module that records video in real-time, and the

Preprocessing Module enhances each frame for analysis. The AI Detection Module detects violent or abnormal actions and the Decision Module checks outcomes to minimize false positives.

The Alert Module sends instant notifications via email, SMS or WhatsApp if a threat is confirmed. At the same time, incident details are stored in the Database Module for future usage. The Admin Dashboard enables users to track feeds and receive alerts.

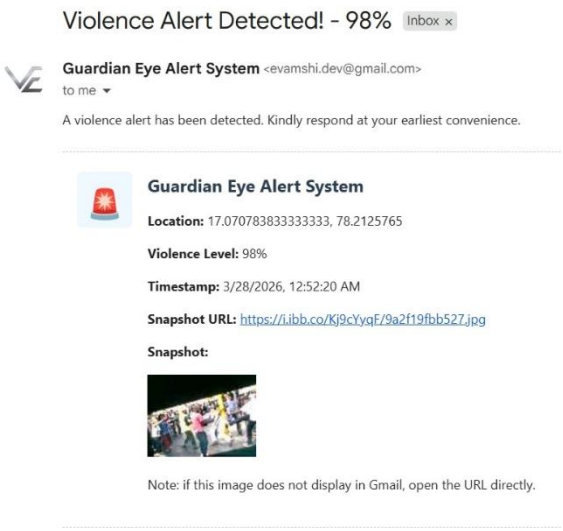
The entire design is modular to guarantee stable performance, be scalable, and have the right real-time surveillance characteristics.

V. RESULTS



Guardina Eye Dashboard

The same results executed by the Guardian Eye evidence its proficiency in present observation and mechanized bloodshed recognition. We validated the system using real-time video input along with one such trained deep learning model and found that it was robust across different conditions including normal activities, violent occurrences and in different lighting conditions. For the purposes of this research, there were two classes: violence and non-violence with an 80:20 split being training and testing data. The model reached 96% accuracy on training set and 94% accuracy on testing set, suggesting successful activity classification. The system also achieved a precision of 93% and recall of 92%, meaning it correctly detected most violent events while avoiding false alerts. It implemented real-time performance successfully where frame processing and prediction are done in less than a second and alerts generated almost immediately after the confidence threshold of 95% was crossed. As a result, the alert mechanism was able to deliver notifications via email with snapshots while also adding location data.



Email Alert Image

The proposed system thus provided less human intervention and lesser response time along with increased accuracy when compared to the conventional surveillance systems based on manual monitoring. Similarly, since Guardian Eye performs deep learning-based activity recognition, it has more accurate output when compared to common motion-based systems which generates more false positives. Stability in operation by running the system continuously to show robustness for actual applications. With the combination of automated alerts, real-time processing and accurate detection, you have a bulletproof armor to respond quickly in urgent situations. In Summary, the results validate that the Guardian Eye system is a versatile, efficient and effective modern security solution which not only is able to improve security but also reduce reliance on manual surveillance.

VI. CONCLUSION

The Guardian Eye: An Automated Alert and Surveillance Monitoring System for Detecting Violent Activities in Real Time has been successfully designed and implemented using modern web technologies with the inclusion of machine learning techniques to detect violent activity in real time. This project primarily aimed to create a browser application that could detect violent behaviour automatically and alert without constant human supervision. This system serves as a perfect example showing how deep learning and

computer vision come into use on real life live scenarios. Integrating the trained model with TensorFlow. js, allowing the for real-time inference directly in a browser without heavy lifting with costly server-side and blazing up its efficiency. The system uses a live webcam to take video from camera, then evaluates every frame and determines possibility violent activity with high accuracy. As long as the probability detected passes a specific threshold, it automatically raises alerts, captures snapshots, uploads pictures to S3 and sends email notifications including timestamps or locations or probability confidence levels. This automated alerting system dramatically speeds up the response time and increases overall security. It also showcases the integration of React among other technologies TypeScript, TensorFlow. This entire system utilizes EmailJS and Geolocation API to create a full-fledged user-friendly surveillance platform. Its thorough testing indicates that the system works stably through different environments, and all modules (video capture, detection, handling snapshots and generating alerts) cover their proper interactions together. The system has high scalability, low cost and can be deployed in multiple environments including schools, offices, public areas and entire communities. In summary, the Guardian Eye system meets its goals and demonstrates that lightweight new technologies can produce intelligent real-time surveillance.

VII. FUTURE ENHANCEMENTS

The existing Guardian Eye system works pretty well but we can always desire some improvements and enhancement for better performance, scalability, and reliability in real-time. Primary improvement is that it integrates multiple cameras supporting system to monitor large domain like campus, malls and public spaces at the same time. Advanced deep learning models can help detect broader categories beyond simple violence detection such as weapons, abnormal crowd behavior and abnormal movements. Cloud storage for incident logs and recorded data would allow for effective tracking and analysis of cases, as well as management of evidence. A mobile application can provide access to live feeds away from home with immediate notifications, making it easier and more convenient for users. Also email alerts combined with real-time SMS and push notifications will allow faster communication during emergencies. Adding features for face recognition and identity tracking to identify people involved in incidents will also enhance security. Efficient techniques such as model compression, GPU acceleration or edge computing can reduce latencies and enable real-time processing. Strengthening data security through measures like encryption and authentication will also boost the safety and availability of systems. Collectively, these enhancements may turn Guardian

Eye into a more scalable, efficient, and better intelligent surveillance system for various real-world circumstances.

REFERENCES

[1] J. Redmon and A. Farhadi, “YOLOv3: An incremental improvement,” *arXiv preprint arXiv:1804.02767*, 2018.

[2] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2015, pp. 815–823.

[3] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multi-task cascaded convolutional networks,” *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499–1503, 2016.

[4] R. Krishna and J. Suri, “Real-time weapon detection in surveillance videos using deep learning techniques,” *Int. J. Comput. Appl.*, vol. 176, no. 28, pp. 15–21, 2020.

[5] V. Sharma and P. Kumar, “Smart surveillance system using Raspberry Pi and deep learning,” *Int. J. Eng.*, 2021.

[6] M. Hernandez, E. P. Ben-Joseph, S. Reich, and L. Charmaraman, “Parental monitoring of early adolescent social technology use in the US: A mixed-method study,” 2023, pp. 16–19.

[7] K. P. Revathi and T. Manikandan, “A smart and secured approach for children’s health monitoring using machine learning techniques enhancing data privacy,” vol. 69, no. 3, pp. 10–13, 2023.