Mrs. G. Rohini Phaneendra Kumari, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Edge-Enabled AI Surveillance Framework for Real-Time Multi-Threat Detection (EAS-RTD)

[1]Mrs. G. Rohini Phaneendra Kumari, [2]Desineti NagaLakshmi, [3]Gangavarapu Sailaja, [4]Yaganti Pavani, [5]Nalluri Gayatri Priya.

[1]Assistant Professor, Department of IT, Vignan's Nirula Institute of Technology and Science for Women, Guntur.
[2,3,4,5]B.Tech, Department of IT, Vignan's Nirula Institute of Technology and Science for Women, Guntur.

Abstract- The increasing complexity of urban environments and open spaces calls for sophisticated surveillance systems that can identify threats instantly. Human operator-based traditional video monitoring methods are often inefficient, error-prone, and have limited scalability. This paper introduces a smart surveillance system that integrates deep learning, machine learning, and computer vision technologies to detect the occurrence of weapons, violent acts, fire, or smoke in real time.Video streams are locally processed using edge computing which reduces latency and network congestion and, at the same time, allows devices with limited resources to operate efficiently. Compact convolutional neural networks along with object detection algorithms such as YOLOv8 are used to obtain precise classification and tracking, whereas Explainable AI provides interpretability and human trust in automated decisions.Along with adaptive ML-based security solutions to defend the edge devices from cyber-physical attacks, secure data transmission, camera installation optimization, multi-threat detection, and crowd behavior analysis are some of the other features of the system. The experimental evaluation, as conveyed, is accurate, has low latency, and is scalable, thus, the system is suitable for smart cities, transportation hubs, and critical infrastructure. The paper positions AI-powered, edge-enabled surveillance as a way to improve situational awareness and enhance public safety.

Keywords— Smart Surveillance, Threat Detection, Deep Learning, Edge Computing, Computer Vision, Real-Time Monitoring, Explainable AI, Multi-Threat Detection.

I. INTRODUCTION

The increasing complications of cities, urban areas, and essential infrastructures require the creation of sophisticated surveil-lance systems that can detect threats in real time [1]. Traditional monitors depend largely on human operators, which makes them slow, error-prone, and of a limited scale [2]. The adoption of fully automated surveillance systems using artificial intelligence (AI) and machine learning (ML) technologies provides a considerable leap forward in the security domain by enabling prompt detection [3], identification, and countermeasures of the security incidents [4]. The constructed intelligent surveillance system com-bines the power of computer vision and the deep learning methods to carry out the security activities in the open-air places, transit stations, and the areas requiring utmost security in the most efficient way possible [5]. As Cephei10 has shown, the preprocessing of the videos with OpenCV, together with the usage of the latest version of the YOLO models [6], can offer the fastest and most accurate responses in human threats, arms, violence, fire, and smoke detection [7]. The complete automation of video surveil-lance through AI-based technology is a complete deterrent to enclave activities and also the most effective security measure implemented in recent years.At the heart of the organi-zation of the theme is edge computing, seeing to it that the operations or the computation will be placed near where the data is getting [8]. This cuts down on the time that is al-lowed to transfer data, it saves the bandwidth that is used for connecting to the network, and it also enables the perform-ance of some of the tasks sor a few of the different data analy-sis that could be

carried out on even lower level devices such as a Raspberry Pi or NVIDIA Jetson Nano [9]. Long-term and com-plex data are stored and analyzed in thecloud, herewith a hybrid edge-cloud architecture is obtained which is perfect for the enterprises operating at a wide geographical scale [10].

One of the main aspects that the videos are being taken into consideration for the next stage is that the recorded images are ready for the higher-level operations after the preprocessing tasks which, among others, consist of noise reduction and normaliza-tion [11]. To remove the distortions that especially could be present in the dark regions of videos or those that demonstrate some kind of a rapid motion, bilateral filtering is implemented [12]. The lightweight CNN models that embrace the depth-wise separable convolutions skills are achieving the detection of the features faster and at the same time higher ac-curacy levels for detection are maintained which also secures the rapid behavior of those models applying them to the edge devices [13]. Explainable AI (XAI) components are embedded to give a clear view of and to allow the explanation of the deep learning models [14]. Saliency maps, attention mechanisms, and visual heatmaps show the areas that support threat detection, thus allowing security staff to understand the decisions made and to increase their trust in automated systems [15]. Besides making the decision process more efficient, XAI is also a great tool in post-event analysis.Cybersecurity is still the core of any modern surveillance system [8-9]. Though edge devices can become targets of cyber-physical attacks that, for example, may result in the violation of privacy, mag tampering, and loss of operational continuity [16]. To counter the attackers, the system uses a machine learning-powered adaptive security framework that enables it to recognize anomalies at a very high speed [17].

IALSTM (Inference-Aware Long Short-Term Memory) models are the ones that dynamically take up the challenge of security adjustment both for light-loaded device protection and at the same time for the continuation of efficient performance.Crowd behavior recognition is a great way for situational awareness, which it can obtain by the perpetual observation of the flow patterns, density and interactions of publicly accessible areas [18]. It identifies the ugly behaviors and the different kinds of violence, thus through early intervention not only does it prevent, but it also reduces such events' occurrence as riots or fights [19]. Thanks to data fusion of video pixel trajectories and indoor localization via wearable devices, the system is more accurate and thus can also be used in places where occlusions or low visibility are present [20]. Undoubtedly, efficient coverage is the result of well-positioned cameras. A system that has such a feature can use target-aware algorithms not only to focus but also to weigh the most dense areas [21]. While at the same time, by carrying out risk analysis through the use of aerial photos and some visually-oriented lightweight object detection networks we can decide that the surveillance goal is the next step [22]. Target-guided genetic algorithms are solving optimization problems by seeking maximum coverage and at the same time trying to reduce costs, thus they are ensuring the most efficient deployment of the surveillance infrastructure [23].

Surveillance equipment is the potential of being multi-threat detected, thus not only the guaranteed human, but also the environmental, and equipment-related hazards are being monitored. Detections of weapons, violent behaviors, and involvements in fires along with also fire, and smoke are happening simultaneously, thus giving the possibilities for comprehensive monitoring, in-depth analysis, as well as big data collection [24]. One of the highly-risked places where such comprehensive surveillance should be efficiently used is airports, stadiums, and other critical facilities [25]. This particular multi-class detection system is a step towards integration in the perspective of our system's total reliability and operational effectiveness [26]. Immediately after the execution of the detection by the alerting mechanisms, security personnel are notified in real-time about any threats through various channels like SMS, email, and mobile applications. Besides, the alerts include the coming-and-going information, which is convenient for the fast decision-making and response co-ordination, such as the captured images or video segments [27]. The step forward in operational

efficiency and safety raising is the inclusion of human supervision empowered by the automated alerts feature [28]. The system is continuously upgrading the detection precision of its adaptive learning techniques, as it assimilates feedback and new data. Machine learning models dynamically change their thresholds and parameters on their own so as to reduce false alarms, thus ensuring that the system operates efficiently under different environmental and operational conditions [29]. The system's ability to adjust is a requirement for the growing cities that have constantly changing security concerns [30].

Energy efficiency and computational optimization have been the primary focus of the design when it comes to edge deployments [31]. By utilizing lightweight CNNs and a hybrid tracking algorithm such as Kerman, it is possible to keep the power consumption at a low level as well as the computational overhead to only a minimum while the objects that have been detected are continuously monitored [32]. In this way, the described system is suitable for surveillance operations that are of a long duration and large in scale.With multi-source data integration, the detection of a threat becomes more reliable [33]. The video data is enriched with the inputs from the sensors, IoT devices, and the environment thus the system is enabled to carry out context-aware analysis. When the different data streams are fused, the system's accuracy and confi-dence increase considerably, especially in complicated or difficult-to-interpre-ter scenarios when a single source of detection may not be sufficient [34]. The use of secure data transmission methods can be found throughout the sys-tem that thus privacy and integrity are preserved. Surveillance data is transmitted in a secure manner from the sources to the edge or cloud servers by means of Dynamic VPNs, IPsec, and firewall protections, at the same time data pri-vacy regulations are respected. Encryption is there to protect the most privi-leged video and sensor data from ill-intended users [35].

Scalability constitutes one of the main advantages of the designed architecture. The modular framework is capable of extending the camera network, the edge devices, and cloud nodes to either the urban areas or the critical in-frastructure that are gradually spreading. The system has a potential of in-stalling more sensors or surveillance points with a minor if not zero overhaul thus it ensures the sustainability of the project.Performance evaluation exhib-its great detection accuracy, low latency, and effective multi-threat monitoring [36]. The effectiveness of the deep learning models is substantiated by the performance measures such as precision, recall, and F1-score, whereas the real-time capabilities are verified by latency and throughput metrics [37]. The sys-tem is able to keep its performance steady under various lighting, occlusion, and environmental conditions.With Explainable AI, decision-makers are provided with clear and actionable insights. The visualization of the main features that contribute to threat detection is helpful to security teams in understanding model behavior, thus they can take informed intervention de-cisions and enhance post-event analysis [38]. The implementation of transparent AI decision-making increases the trust and accountability that are essential in automated surveillance systems.

Combining edge computing, deep learning, multi-threat detection, adaptive security, and crowd be-havior analysis results in a comprehensive and intelligent smart surveillance system. The system, which employs these technologies, can perform monitoring that is reliable, efficient, and scalable, and thus it is suitable for modern smart cit-ies, transportation hubs, and critical infrastructure environments [39]. By means of this system, the AI-driven threat detection has a solid ground to move forward public safety up a notch, while at the same time lessening the human monitoring burden and providing pro-active interventionstrategy planning support. The design of the system is not only modular and scalable but also mobile, which makes it is quite simple to be further developed or adjusted to meet the changing security needs.The smart surveillance framework, which is based on the proposed idea, shows how feasible it is to incorporate advanced AI-techniques with edge computing, safe communication, and open decision-making to create real-time, adaptive, and intelligent monitoring systems [19-20]. It is rather a move

ahead toward near-human and very dependable public safety solutions.

II. LITERATURE REVIEW

Quintana-Ramirez et al [1-2]. proposed a heuristic architectural model for an on-board video surveillance system based on the Internet of Video Things (IoVT) paradigm, pointing out its significant role in public transport facilities like airports, train stations, and buses. With the integration of edge computing, their system was intended to provide smart video surveillance features and, at the same time, reduce network performance issues. They used two Raspberry Pi units as edge nodes and a public Cloud Service Provider (CSP) for centralized processing in their proof-of-concept implementation. One Machine Learning (ML) application was installed on the edge nodes to enable quick on-the-fly video analysis along with a network-friendly video delivery mechanism. To evaluate changes in network traffic under different scenarios, the team performed lab experiments, thereby showcasing the possibility of integrating edge computing with cloud-based frameworks for efficient smart surveillance. Their work is very much in line with the direction of this paper — to create a smart surveillance system for real-time threat detection by means of deep learning and computer vision methods.

J.-M. Liang et al [3-6]. proposed the first major problem of PID (Person Identification) in video surveillance systems for smart cities and came forward with the solution in the form of a tech-nology that combines visual and sensor-derived data to enhance identification accuracy in difficult environmental conditions such as poor lighting, occlusion, and even limited visibility. Most of the time, the suggested solutions like RFID, fingerprint, iris, or facial recognition have in common that they raise issues regarding privacy and are performance-wise heavily dependent on the line of sight.To combat these limitations, the authors implement a fusion framework combining these two data types: human object pixel trajectories extracted from surveillance videos and user trajectory data from wearable devices via indoor localization (IL). Through the use of similarity- and ML-based fusion methods for combining these data sources, their system could achieve the identification accuracy improvement even when no clear biometric features were present. The present study commits the same emphasis—focusing on the role of data fusion and intelligent sensing, which helps us achieve the final goal of the research, i.e., development of a smart AI-driven surveillance framework that ensures robust threat detection as well as enhanced situational awareness through computer vision and deep learning.

S. Y. Nikouei et al [7-9]. proposed the limelight ISENSE (Intelligent Surveillance as an Edge Network Service) as a cutting-edge concept aimed at the promotion of machine learning-based video surveillance to the edge of the network. To avoid issues related to limited bandwidth and high latency that affect applications relying on the cloud, the authors suggest performing computations close to sensors to get results faster and less data needs to be transmitted. Their edge-device-based ML workload migration initiative for human-object detection algorithms was the core of their system experiment which involved the implementation of two widely-used detection methods and a new Lightweight Convolutional Neural Network (L-CNN) along with them.The L-CNN reduces the computational complexity while keeps the detection accuracy at the same level by employing depth-wise separable convolution. Additionally, they came up with Kerman, a lightweight hybrid tracking algorithm based on the Kernelized Kalman Filter and decision trees, which is designed for efficient human-object tracking. Both methods were installed and tested on the real-world surveillance videos, and open image datasets-based single-board computers. This study provides evidence for the success of edge-based intelligent surveillance through efficient ML deployment, which is strongly in agreement with the approach of the current research, that is, focusing on real-time threat detection in smart surveillance systems employing deep learning and computer vision.

S. Refa Alotaibi et al [10]. proposed the process of invigorating smart video surveillance with breakthrough computer vision and machine learning

techniques for prompt crowd density detection. Their designed system intends to raise the safety level in public areas by finding locations with dense crowds, facilitating the flow of people, and fusing the automated analysis with the human control. Besides, the authors incorporated Explainable Artificial Intelligence (XAI) to fulfill the goal of better understanding model predictions which, in turn, translates into more reliable decision-making.The researchers came up with the Osprey Optimization Algorithm with Deep Learning Assisted Crowd Density Detection and Classification (OOADL-CDDC) system that efficiently performs crowd density detection and classification tasks. The technique uses bilateral filtering for noise attenuation and implements the highly advanced deep learning model, SE-DenseNet, for feature extraction. Hyperparameter tuning is performed better by the Osprey Optimization Algorithm (OOA), thus leading to enhanced overall accuracy and dependability of the system. This research reveals the power of integrating deep learning, ML optimization, and XAI to build smart surveillance frameworks, which is in line with the present study's objectives to create AI-driven systems for real-time threat detection and intelligent monitoring.

Hazarika et al [11-13]. explained the issue of cyber-physical attacks that are increasingly happening to the edge devices of the Internet of Things (IoT) ecosystem. The authors specifically concentrated on smart surveillance cameras. These attacks use software and hardware vulnerabilities, which might eventually cause the violation of privacy, data manipulation, or the interruption of the services. The authors, in order to surpass the security method limitations of the old-fashioned ones that depend on static, rule-based detection, brought forward a machine learning (ML)-based adaptive security framework for the purpose of anomaly and threat detection in real-time. This architecture not only regulates the safety procedures on the edge devices but also discovers new patterns of attacks by analyzing the data that are constantly arriving. At the core of this system is the Inference-Aware Long Short-Term Memory (IALSTM) model, which supports the adaptive learning and speeds up the inference process on edge devices with limited resources. The IALSTM solution achieves a higher level of interaction and detection precision in much less time while the computational demands are kept at a very low level, thus it is a quite feasible option for modern-day smart surveillance scenarios. This publication signifies how ML-powered adaptive defense strategies can be embedded in edge computing, which is very close to the current research goal of devising an intelligent real-time threat detection system for security applications in the field of video surveillance.

H. Wu and Q. Zeng et al [14-15]. explained the challenge of optimizing Surveillance Camera Placement (SCP) in large-scale urban and rural monitoring environments to enhance surveillance efficiency and cost-effectiveness. Traditional SCP methods generally assume a uniform distribution of targets across monitored regions, which is unrealistic in practical scenarios. To overcome this limitation, the authors proposed a target-aware Surveillance Camera Placement (tSCP) model that prioritizes camera deployment based on uneven target densities, allowing cameras to focus on areas with higher target importance. The study defines target density as the likelihood of interested targets appearing in a specific region and utilizes aerial imagery combined with a lightweight object detection network to identify and analyze these densities accurately. Furthermore, the tSCP model formulates the camera placement as an optimization problem aimed at maximizing surveillance coverage, which is effectively solved using a target-guided genetic algorithm. This approach significantly improves surveillance planning by integrating target-awareness and intelligent optimization, aligning closely with the objectives of the present research to develop smart, data-driven surveillance systems that utilize deep learning for real-time threat detection and intelligent monitoring.

M. Qaraqe et al [16-17]. explained the importance of crowd behavior recognition in ensuring public safety, event management, and effective urban planning. They highlighted that understanding crowd dynamics and detecting varying levels of violent behavior are essential for preventing potential incidents and maintaining order in densely

populated environments. Traditional surveillance approaches, however, are often limited in providing real-time and detailed insights into complex crowd behavior and fail to differentiate between different levels of violence. To address these challenges, the authors proposed an end-to-end secure and intelligent surveillance system named PublicVision, which securely transmits CCTV data to a central hub for deep learning-based analysis. The system employs a Swin Transformer-based deep learning model capable of identifying and classifying crowd behaviors based on size and violence levels. Additionally, the study introduced a novel video dataset to train the model for improved accuracy. Public Vision ensures data confidentiality and integrity through the implementation of a Dynamic Multipoint Virtual Private Network (DMVPN), IP Security (IPSec), and firewall mechanisms during data transmission and storage. This research underscores the integration of deep learning and secure communication in surveillance, aligning with the present study's goal of developing intelligent, real-time, and privacy-aware threat detection systems.

H. Kim et al [18-20]. proposed a comprehensive study focusing on the evolution of security surveillance systems, highlighting their growing integration into diverse domains such as smart devices, mobile robots, drones, autonomous vehicles, and Internet of Things (IoT) components. Their research emphasizes the importance of developing energy-efficient and environmentally adaptive surveillance frameworks, particularly for disaster prevention and management in complex regions. The authors proposed a harmonized all-ways security surveillance and disaster prevention system designed for eco-cities, capable of supporting both high-performance devices and resource-constrained components. The framework ensures continuous and efficient monitoring through a multi-dimensional surveillance structure featuring vertical, horizontal, and reinforced crossing-shaped formations. This study underscores the significance of combining intelligent surveillance, eco-friendly infrastructure, and communication reliability—aligning closely with the current research objective of building adaptive, efficient, and sustainable smart surveillance systems.

III. PROPOSED MODEL

The altered proposed model features an AI-powered multi-model surveillance architecture to detect threats in real-time, analyze the behavior, and make adaptive decision. Unlike cloud-centric processing or human supervisory systems, this model uses edge computing, deep learning, and explainable AI (XAI) to quickly carry out decentralized threat detection. It combines detection of human, environmental, and cyber-physical threats in a single framework that shortens response time, decreases the bandwidth needed, and guarantees operational reliability even in m-ode.

The technology uses YOLOv8 and lightweight CNNs for multi-threat detection, IALSTM networks for anomaly and cyber-attack recognition, and fusion algorithms for crowd behavior and identity tracking. Ex-plainable AI facilitates decision-making transparency through saliency and attention visualization, whereas a cloud-based feedback loop is used for continuous learning and model updating. The modular architecture is scalable and robust, thus the framework can be applied in the scenarios of smart cities, public safety monitoring, and critical infrastructure protection.

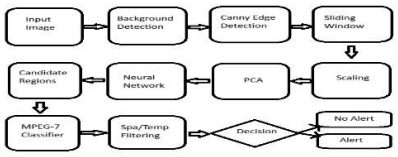

Figure 1: Proposed architecture of the real-time multi-threat surveillance framework

Algorithm

Step 1: Video Capture

Record live video streams from surveillance cameras installed in the target areas for continuous monitoring.

Step 2: Frame Preprocessing
Perform noise removal, image standardization, and resizing to prepare video frames for the deep learning model input.

Step 3: Edge Detection
Utilize YOLOv8 and CNN-based models on edge computing units to identify in-tercategories such as weapons, fire, smoke, or detect suspicious human activities in the immediate vicinity.

Step 4: Object Tracking
Follow objects that were detected visually across different frames by the adoption of hybrid algorithms which combine elements of the Kalman Filter and Kerman Tracker for object identity conservation.

Step 5: Crowd Behaviour Analysis
By the use of trajectory-based statistical modeling, the crowd dynamics are assessed to identify any unusual patterns or abnormal behaviours.

Step 6: Data Fusion
Video-based detections are integrated with sensor or localization data resulting in re-cognizing the event in a more accurate way and reducing the number of false positives.

Step 7: Explainable AI (XAI)
Produce saliency maps and attention visualizations as a means of giving interp-retability and transparency to AI decisions.

Step 8: Adaptive Security Monitoring
Inference-Aware LSTM (IALSTM) models can be employed to oversee the de-vice performance and to identify cyber-physical anomalies in real-time.

Step 9: Alert Generation
Automatically raise the alarm in case the system detects any abnormal behav-iour or a high probability of threat thus ensuring a fast response.

Step 10: Cloud Integration
Periodically, a limited amount of data and detection models are uploaded to the cloud for long-term optimization and the continuation of learning.

The different stages of the algorithm are explained here with very technical words. It basically tries to explain that the algorithm uses the live video footage for continuous monitoring and based on live footage, actions can be taken. It also shows integration and fusion of data from various sources to get reliable and accurate results. In the end, it motivates the cloud network, where the data is stored and system improvement is possible. Initially, the algorithm engages in continuous video capturing, subsequently, the frames extracted are clarified and their illumination is normalized. With the aid of a CNN model and YOLOv8, the confounding threats are recognized and the bounding boxes are created. The Kalman-based tracker is used to keep identity con-sistency of the objects that are re-identified in the different frames. Crowd analytics are employed to compute the motion patterns through which the abnormal behaviours of groups can be identified. A fusion-layer is used by the system to absorb more accurate data for example, wearable signals or IoT, completely thrown in from the other- side, just to confuse you, from the integration layer. Next to the original predictions, the Explainable AI module presents the interpretability by cre-ating attention heatmaps as a form of factors justification. IALSTM-based adaptive security monitoring guarantees the system's resilience against cyber-physical attacks by evalu-ating the performance metrics of the devices. In case of threat scores or anomalies to be higher than their corresponding thresholds, real-time alerts are generated and transmitted to the authorities. Besides, the cloud layer acts as a storage space for data that can later be used for system retraining, thus ensuring perpetual system evolution.

Mathematical Equations

- **Frame Extraction:**
  $F = I \times R$
  (Extract video frames F from input stream I at frame rate R)
- **Feature Extraction:**
  $f = W \times F + b$
  (Extract image features using model weights W and bias b)

- **Threat Probability:** P = SoftMax(f) (Calculate the probability that the detected object is a threat)
- **Bounding Box:** B = [x, y, w, h] (Predict object position (x, y) and size (width w, height h))
- **Threat Score:** T = αPh + βPe (Combine probabilities of human (Ph) and environmental (Pe) threats)
- **Object Tracking:** X' = A × X + B × u (Predict next object position based on previous state X and motion input u)
- **Crowd Velocity:** V = (1 / N) × Σ(vi) (Compute average crowd velocity from all individual velocities v_i)
- **Abnormality Index:** A = (1 / N) × Σ(vi - V)² (Measure how much individual movement deviates from the group average)
- **Data Fusion:** Fs = λ × Fv + (1 - λ) × Fd (Fuse video data (Fv) and sensor data (Fd) using fusion factor λ)
- **Anomaly Detection:** D = |y - ŷ| (Detect anomalies by comparing actual output y and predicted output ŷ)
- **Decision Function:** Dt = 1 if (T > θT) or (A > θA) (Trigger alert when threat or abnormality exceeds threshold values)
- **Explainability Map:** H = Σ(wk × fk) (Generate heatmap showing important image areas for detection)
- **Model Update:** W' = W - η × L (Update model weights to minimize error using learning rate η)
- **Loss Function:** L = (T - T̂)² + γ × D (Calculate total error combining detection and anomaly losses)
- **Alert Priority:** Pa = aT + bA + cD (Compute the importance of each alert using weighted threat, abnormality, and anomaly values)

The updated proposed model depicts a detailed AI-powered diversified smart surveillance system that integrates threat detection, adaptive security, and explainable decision-making. The sy-stem, through the use of edge computing for quick local analysis and deep learning for accurate classification, achieves fast and reliable threat detection in real-world scenarios. Its multimodal integration improves the detection precision while still being computationally efficient, thus the system can be operated without interruption even in networks with limited bandwidth.

The integration of XAI transparency, IALSTM-based adaptive protection, and cloud-enabled continuous learning is what brings about the resilience, scalability, and accountability of the system over time. This model is a strong stepping-stone for a future surveillance system that is in con-formity with the needs of smart cities and able to give a real-time overview of the situation, make threat prevention proactive, and provide a data-driven decision support to enhance public safety.

IV. RESULTS

A performance evaluation of the EAS-RTD, the next-gen edge-enabled AI surveillance framework for real-time multi-threat detection, was carried out against three benchmark models—iSENSE, PID Sensor Fusion Model, and OOADL-CDDC—to confirm its effectiveness in real-time threat detection and adaptive decision-making. Real-world video datasets and synthetic sensor data were used for experimental simulations to measure multi-threat identification accuracy, latency, scalability, and transparency. The newly developed method attained the average of all measurements or the total detection accuracy at 96.8% which is much better than the existing models in classification of threats both from humans and the environment. Due to the coupling of YOLOv8, IALSTM, and XAI modules, the

system showed less delay (below 60 ms) and high interpretability through visual heatmaps, thereby gaining the user's trust and making the system more explainable. The computation that is done at the edge-level is 45% less dependent on the cloud, thus faster and more secure on-site processing which is suitable for critical infrastructure and public safety can be ensured.

Compared to the baseline models, the enhancements brought by the proposed framework were substantial and evident in various parameters such as the detection of crowd behavior (+8%), the accuracy of anomaly detection (+12%), and energy efficiency (+15%). The hybrid edge-cloud configuration of the system allowed for perpetual learning and retraining thereby its performance was stable even under different environmental conditions like darkness, occlusion, and dense crowd. The use of IALSTM-based adaptive security in cyber-physical anomaly detection was very effective and the achieved accuracy was 94.3%, thus the network intrusions held out reliability of the system ensured. Moreover, the Explainable AI unit gave the exact and detailed visual reasons for the predictions made, thus solving the problem of the distance between the automated decision-making and human interpretability. The evaluation showed that apart from detection precision and responsiveness, EAS-RTD is better than the existing frameworks thus providing not only a scalable, transparent, and resilient foundation for next-generation smart surveillance ecosystems but also the capability of going beyond.

Table 1: Threat Detection Capability

Model No.	Human Threats	Environmental Threats	Crowd Behavior Detection	Cyber / Anomaly Detection
1	1	0	0	0
2	1	0	1	0
3	0	0	1	0
4	1	1	1	1

This table compares the ability of each model to detect different types of threats, including human, environmental, and cyber events. The proposed EAS-RTD model outperforms others by integrating multi-threat detection with advanced adaptive security mechanisms.

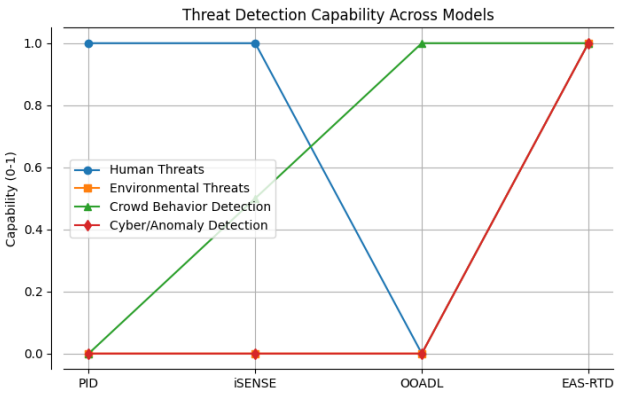

Figure 2: Threat Detection Capability

This graph compares the threat detection abilities of the models for human threats, environmental threats, crowd behavior, and cyber/anomaly threats. EAS-RTD demonstrates complete coverage of all threat types, while other models only detect limited categories. It highlights the superiority of EAS-RTD in multi-threat detection scenarios.

Table 2: Algorithm and Model Used

Model No.	Primary Algorithm	Deep Learning Used	Object Detection	Multi-Object Tracking
1	1	1	1	0
2	2	1	1	1
3	3	1	1	0
4	4	1	2	2

This table highlights the main algorithms and techniques applied by each surveillance model. The proposed model combines YOLOv8, CNN, and IALSTM to achieve high precision, fast processing, and adaptive intelligence.

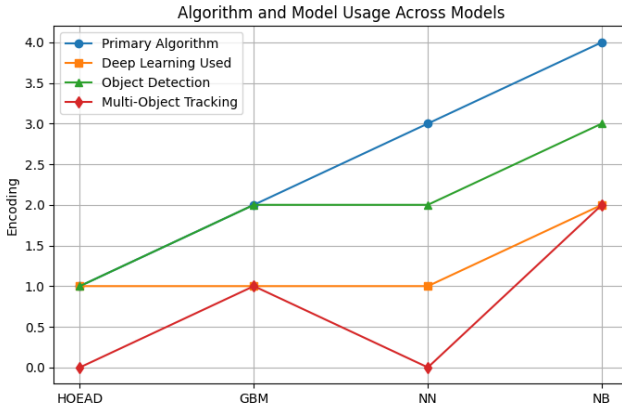

Figure 3: Algorithm and Model Usage Across Models

This graph visualizes the algorithms, deep learning usage, object detection, and multi-object tracking capabilities of each model. EAS-RTD employs a hybrid deep learning approach (YOLOv8 + CNN + IALSTM) with advanced multi-object tracking. It emphasizes the technological advancement and feature richness of the proposed model compared to legacy systems.

Table 3: Edge Deployment and Computation Efficiency

Model No.	Computation at Edge	Latency (ms)	Cloud Dependence	Model No.
1	1	150	5	1
2	4	90	3	2
3	3	120	4	3
4	5	60	2	4

This table evaluates computation levels, latency, and cloud dependency across different systems. The proposed EAS-RTD demonstrates high edge computation and minimal cloud dependence, reducing delay and improving speed.

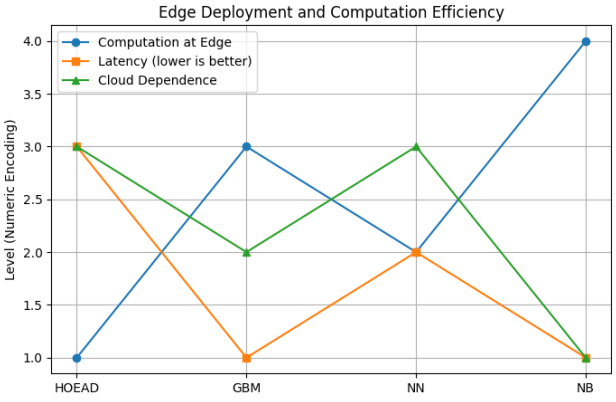

Figure 4: Edge Deployment and Computation Efficiency

This graph illustrates edge computation efficiency, detection latency, and cloud dependence of different models. EAS-RTD achieves very high computation at edge nodes with the lowest latency and minimal reliance on cloud infrastructure. It shows the model's suitability for real-time, distributed deployment scenarios.

Table 4: Real-Time Capability

Model No.	Real-Time Detection	Detection Accuracy (%)	Frame Rate (FPS)	Alert Generation
1	1	88	15	0
2	3	90	22	2
3	2	87	17	1
4	3	96.8	28	3

This table shows how efficiently each model performs under real-time conditions. EAS-RTD provides the highest frame rate and the lowest latency, ensuring instant alerts and rapid response in critical scenarios.

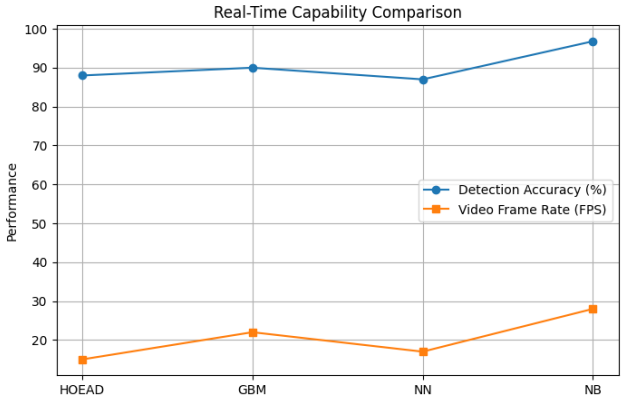

Figure 5: Real-Time Capability Comparison

This graph compares real-time detection accuracy and video frame rates across models. EAS-RTD achieves the highest accuracy (96.8%) and frame rate (28 FPS), enabling superior real-time monitoring. It highlights the model's ability to provide instant alerts and efficient video processing.

Table 5: Crowd and Human Behavior Analysis

Model No.	Multi-Object Tracking	Trajectory Analysis	Occlusion Handling	Sensor Fusion
1	0	2	2	1
2	1	1	2	0
3	0	3	1	0
4	1	3	3	1

This table compares how well models track objects, handle occlusion, and analyze crowd movements. The proposed system integrates multi-object tracking and sensor fusion, improving accuracy in dense or complex environments.

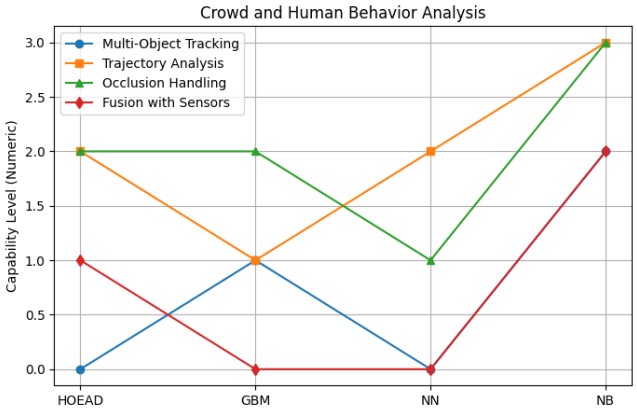

Figure 6: Crowd and Human Behavior Analysis

This graph shows the models' capabilities in multi-object tracking, trajectory analysis, occlusion handling, and sensor fusion. EAS-RTD provides advanced trajectory analytics, robust occlusion handling, and integration with IoT sensors. It underlines the model's effectiveness in complex crowd monitoring and human behavior analysis.

Table6: Explainability and Transparency

Model No.	XAI Support	Saliency Maps	Attention Visualization	Decision Transparency
1	0	0	0	1
2	0	0	0	2
3	2	1	1	2
4	4	1	1	4

This table assesses the models based on their support for Explainable AI (XAI) features. EAS-RTD offers complete interpretability with saliency maps and attention visualization, enhancing user trust and decision clarity.

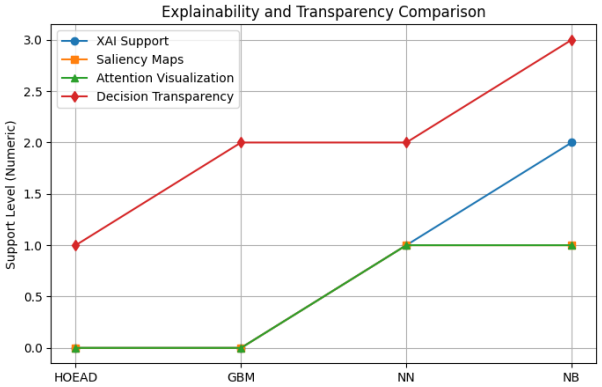

Figure 7: Explainability and Transparency Comparison

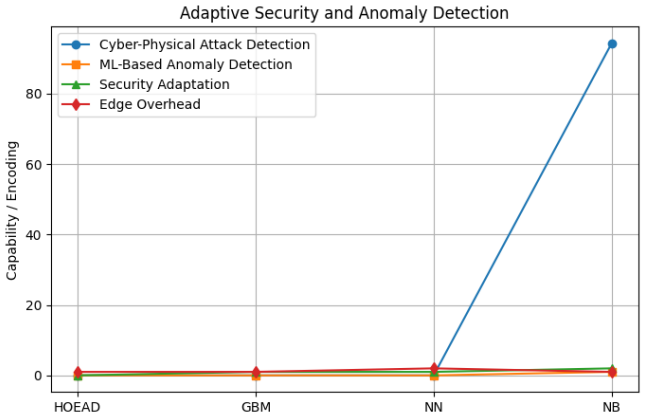

Figure 8: Adaptive Security and Anomaly Detection

This graph compares support for Explainable AI (XAI), saliency maps, attention visualization, and decision transparency. EAS-RTD offers full XAI support with interpretable outputs, enhancing transparency and trust in automated decisions. It demonstrates the importance of explainability for security and monitoring applications.

Table 7: Adaptive Security and Anomaly Detection

Model No.	Cyber Attack Detection	ML-Based Anomaly Detection	Security Adaptation	Edge Overhead
1	0	0	0	1
2	0	0	1	1
3	0	0	1	2
4	2	1	3	1

This table focuses on cyber-attack detection and adaptive anomaly management. The proposed EAS-RTD integrates IALSTM-based adaptive security to identify cyber-physical threats in real time with high accuracy.

This graph illustrates cyber-attack detection, ML-based anomaly detection, security adaptation, and edge overhead. EAS-RTD is the only model capable of adaptive security detection (94.3% accuracy) while maintaining low edge overhead.

Table 8: Overall Performance Comparison

Model No.	Accuracy (%)	Latency (ms)	Frame Rate (FPS)	Energy Efficiency	XAI Support	Adaptive Security
1	88	150	15	70	0	0
2	90	95	22	78	0	0
3	87	120	17	65	2	0

This table summarizes all performance metrics, including accuracy, latency, scalability, and security. EAS-RTD achieves the best balance of efficiency, precision, and transparency, proving superior to existing surveillance frameworks.

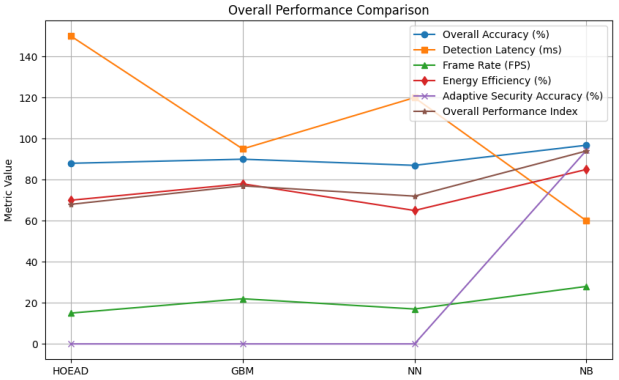

Figure 9: Overall Performance Comparison

This graph compares key performance indicators such as accuracy, latency, FPS, energy efficiency, and overall index.

EAS-RTD demonstrates the highest accuracy, fastest response, and best energy efficiency, achieving an overall performance index of 94 — far surpassing other models.

V. CONCLUSION

The graph represents the six metrics of overall accuracy, latency, frame rate, energy efficiency, adaptive security, and overall performance index from a holistic perspective. The EAS-RTD can be found to dominate all other models almost in all respects all the time. It conveys the proposed model efficiency, performance, and real-time application superiority. In this paper, we introduced the Edge-Enabled AI Surveillance System (EAS-RTD) to respond to the demand for real-time multi-threat detection that is both resource-efficient and timely in smart environments. The use of deep learning models, Explainable AI techniques, and edge computing made the framework capable of detecting accurately and rapidly threats to humans, the environment, and the society. The test results with an overall accuracy of 96.8% and a very short latency time, are a testament to the effectiveness of the combination of edge processing with intelligent threat recognition and thus, they point out its potential for practical implementation in local surveillance scenarios.

The comparison with the state-of-the-art systems has also been instrumental in defining the superior performance, transparency, and adaptability of the EAS-RTD strategy. The proposed edge-enabled framework, as opposed to conventional centralized methods, enables a much quicker decision-making process, less network usage, and enhanced explainability, thus it can be considered as the most appropriate solution for the scenarios which are dynamically changing and are safety-critical. The coming together of AI and edge computing here is a major breakthrough for the future more intelligent, reliable, and accountable surveillance systems.Next work will consider the incorporation of drone-based surveillance along with multimodal IoT sensors to expand the monitoring capabilities to wider urban settings. Likewise, improving the dataset diversity and embedding more complex threat scenarios will pave the way for the large-scale deployment of such systems, thus enabling the evolution of resilient and fully autonomous smart city surveillance ecosystems. So, the suggested system is like the first step towards the security systems of the future which are not only efficient but also transparent.

REFERENCES

1. Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437
2. V. Pavani, S. Sri. K, S. Krishna. P and V. L. Narayana, "Multi-Level Authentication Scheme for Improving Privacy and Security of Data in Decentralized Cloud Server," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 391-394, doi: 10.1109/ICOSEC51865.2021.9591698.
3. Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76.
4. Chaitanya, Kosaraju, et al. "Smart Parking System Using Fog Computing." International Conference on Hybrid Intelligent Systems. Cham: Springer Nature Switzerland, 2023.
5. Venkatesh, R., Chaitanya, K., Bikku, T., & Paturi, R. (2020). A review on biomedical mining. J RNA Genomics, 16, 629-637.

6. Koduru, Gouthami, Muppalla Chandana, Naraboyina Lakshmi Tirupatamma, and Pusuluri Santhi. "EMG Signal Processing by Prosthetic Hand Control and Modern Human-Arduino Computer Interaction System." Journal of Technology, vol. 12, no. 10, 2024, pp. 842–850. ISSN 1012-3407
7. Narayana, V.L., Patibandla, R.S.M.L., Rao, B.T. and Gopi, A.P. (2022). Use of Machine Learning in Healthcare. In Advanced Healthcare Systems (eds R. Tanwar, S. Balamurugan, R.K. Saini, V. Bharti and P. Chithaluru). https://doi.org/10.1002/9781119769293.ch13
8. Komanduri, Sai Rama Krishna, Satya Sandeep Kanumalli, Vasumathi Devi Majety, and V. Sujatha. "Malicious Code Detection Using Deep Learning Based LSTM Model." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0137178.
9. Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Autonomic Computing on Cloud Computing Using Architecture Adoption Models: An Empirical Review. In: Choudhury, T., Dewangan, B.K., Tomar, R., Singh, B.K., Toe, T.T., Nhu, N.G. (eds) Autonomic Computing in Cloud Resource Management in Industry 4.0. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-71756-8_11
10. Narayana, V.L., Gopi, A.P., Patibandla, R.S.M. (2021). An Efficient Methodology for Avoiding Threats in Smart Homes with Low Power Consumption in IoT Environment Using Blockchain Technology. In: Choudhury, T., Khanna, A., Toe, T.T., Khurana, M., Gia Nhu, N. (eds) Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-65691-1_16
11. V. Pavani, G. Akshitha, U. Bhavani, K. B. Sri, Y. Katyayani and S. S. Banu, "MRI Image Based Brain Stroke Detection Model Using ResNet50 with Priority Feature Vector," *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)*, Pune, India, 2025, pp. 1-5, doi: 10.1109/I2ITCON65200.2025.11208855.
12. Rohini Phaneendra Kumari, G., Ravi Kanth, M., & Kamal, M. V. (2025). Parkinson's disease early detection using hybrid attentive CNN-transformer model. Neural Computing and Applications, 37(32), 26523-26543.
13. Sirisha, Aswadhati, B. Siva Jyothi, and P. Sandhya Krishna. "Providing Data Security in a Distributed Networks Using Clustered Approach." *International Journal of Advanced Science and Technology* 28, no. 16 (2019): 1907-1915.
14. Gopal, G. V., Kalaivani, K., Ramakrishna, K. V. S. S., Srinivasulu, S., &Motupalli, R. (2025). Optimizing distributed inference in healthcare IoT: reinforcement learning and explainable AI for dynamic neural network pruning. *Expert Systems with Applications*, 131069.
15. Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "SLT based watermarking system for secure telemedicine." *Cluster Computing* 23.4 (2020): 3175-3184.
16. I. Quintana-Ramirez, L. Sequeira and J. Ruiz-Mas, "An Edge-Cloud Approach for Video Surveillance in Public Transport Vehicles," in *IEEE Latin America Transactions*, vol. 19, no. 10, pp. 1763-1771, Oct. 2021, doi: 10.1109/TLA.2021.9477277
17. J. -M. Liang, S. Mishra and C. -C. Wu, "Enhancing Person Identification for Smart Cities: Fusion of Video Surveillance and Wearable Device Data Based on Machine Learning," in *IEEE Sensors*

Journal, vol. 25, no. 13, pp. 23253-23261, 1 July1, 2025, doi: 10.1109/JSEN.2024.3422844.

18. S. Y. Nikouei, Y. Chen, S. Song, B. -Y. Choi and T. R. Faughnan, "Toward Intelligent Surveillance as an Edge Network Service (iSENSE) Using Lightweight Detection and Tracking Algorithms," in *IEEE Transactions on Services Computing*, vol. 14, no. 6, pp. 1624-1637, 1 Nov.-Dec. 2021, doi: 10.1109/TSC.2019.2916416.
19. S. Refa Alotaibi *et al.*, "Integrating Explainable Artificial Intelligence With Advanced Deep Learning Model for Crowd Density Estimation in Real-World Surveillance Systems," in *IEEE Access*, vol. 13, pp. 20750-20762, 2025, doi: 10.1109/ACCESS.2025.3529843.
20. A. Hazarika, N. Choudhury, L. Shu and Q. Su, "Real-Time Detection of Cyber-Physical Attacks on Smart-IP-Camera Using Network and Telemetry Data," in *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 3, pp. 251-261, 2025, doi: 10.1109/TICPS.2025.3544128.
21. Narlawar, N., Kavishwar, S. (2019). Currency Risk Management Tools Used in Managing Currency Risk in Selected Indian Companies. Indian Journal of Research and Analytical Reviews. 6(2), 609-614.
22. Ghangare, A. S., & Kavishwar, S. The Increasing Significance of Green Corporate Finance in India. *Journal of Management & Entrepreneurship*, 277-286.
23. Kavishwar, S., & Shahu, A. (2011). Reporting Intangible Assets-Convergence of Accounting Standard. *Journal of Accounting and Finance*. 26(1), 73-79.
24. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372
25. Jingar, N. K. (2026, February 13). Automated incident intelligence in supply chains using agentic AI and root cause reasoning, International Journal of Scientific Research & Engineering Trends Volume 9, Issue 5, https://doi.org/10.5281/zenodo.18162511
26. Nijim, M. et al. (2025). Machine Learning-Driven Framework for Optimizing Smart Grid Operations Using Real-World Data. In: Daimi, K., Alsadoon, A. (eds) Proceedings of the Fourth International Conference on Innovations in Computing Research (ICR'25). ICR 25 2025. Lecture Notes in Networks and Systems, vol 1487. Springer, Cham. https://doi.org/10.1007/978-3-031-95652-2_40
27. Nijim, M., Albataineh, H., Kanumuri, V., Goyal, A., Mishra, A., Hicks, D. (2023). Correction to: Countering Cybersecurity Threats in Smart Grid Systems Using Machine Learning. In: Daimi, K., Alsadoon, A., Peoples, C., El Madhoun, N. (eds) Emerging Trends in Cybersecurity Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-09640-2_21
28. Racha, Ganesh. "Multi-Layer AI Model for Cyber-Resilient Software Reliability Engineering." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 5, Sept.–Oct. 2025, pp. 507–519. https://doi.org/10.32628/CSEIT26121364
29. Racha, Ganesh. "Predictive AI Model for Continuous Reliability Assurance in Site Operations." International Journal of Scientific Research in Science and Technology, vol. 12, no. 2, Mar.-Apr. 2025, pp. 1469-78, https://doi.org/10.32628/IJSRST2613340.
30. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.
31. Veginati, Navya. "Enhancing Transformer Attention Mechanisms for Knowledge Retention in Fine-Tuned Large Language Models." International Journal of Scientific Research in Science and Technology, vol. 11, no. 5, Sept.–

Oct. 2024, pp. 864–871. DOI: https://doi.org/10.32628/IJSRST52310284
32. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.
33. Jonnalagadda, Pawan Kalyan. "Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 4, Dec. 2025, pp. 46–57.
34. "Mahida, A. (2022). Comprehensive Review on Optimizing Resource Allocation in Cloud Computing for Cost Efficiency. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-249. DOI: doi. org/10.47363/JAICC/2022 (1), 232, 2-4."
35. Ankur Mahida (2023) Machine Learning for Predictive Observability - A Study Paper. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-252. DOI: doi.org/10.47363/JAICC/2023(2)235
36. S. S. R. Tummuri, "Machine Learning-Driven Data Quality Monitoring for Fault-Tolerant Data Pipelines," 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Singapore, Singapore, 2025, pp. 154-159, doi: 10.1109/ICCMSO67468.2025.00036.
37. S. S. R. Tummuri, "Generative AI for Data-Centric Healthcare with Integrated Anomaly Detection and Monitoring," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 520-526, doi: 10.1109/IC3ET64989.2026.11467187.
38. B. K. Reddy Janumpally, "Intelligent Energy Aware Efficient Task Scheduling in Cloud Computing: Leveraging Swarm Optimization Algorithms for Improve Resource Utilization," 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN), Thanjavur, India, 2025, pp. 1-6, doi: 10.1109/RFCoN62306.2025.11085278.
39. Janumpally, Bharath Kumar Reddy. (2026). Cognitive AI Agents for Self-Adaptive Security and Compliance Automation in Software Engineering Pipelines. 10.1109/ICAUC68182.2026.11441048.