International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

Autonomous Threat Detection and Elimination System

Vidya Deshmukh, Samradnyi Patil, Akshada Veer, Jayada Talharkar, Tahareen begampalli
Department of ENTC AISSMS College of Engineering
Pune, India.

Abstract- Modern security environments, particularly on the battlefield, demand autonomous systems capable of real-time threat detection and neutralization without relying on human intervention. This paper presents the Autonomous Threat Detection and Elimination System (ATDES), an integrated hardware-software platform designed to detect enemy armored threats — specifically tanks — using a vision-based AI detection pipeline and respond autonomously through a servo-controlled targeting and firing mechanism. The system leverages a Raspberry Pi 3B+ as the central processing unit, integrating a 2- megapixel camera for visual acquisition, an IR transceiver pair for friend-or-foe (IFF) identification, an RF receiver for enemy signal detection, and a servo-mounted firing mechanism for threat neutralization. A lightweight deep learning model is deployed on-device for real-time tank detection from camera frames, achieving sub-50 ms inference latency at a resolution of 480×640 pixels. IR-based IFF communication ensures that allied units are correctly identified and excluded from targeting, minimizing the risk of fratricide. Blynk IoT cloud integration enables remote monitoring and event logging. The system operates off-grid using a battery and solar power combination, enabling continuous 24×7 autonomous surveillance. Simulation results confirm consistent real-time de-tection with high confidence scores, demonstrating the feasibility of deploying edge AI for autonomous military threat response. The proposed system contributes a cost-effective, scalable, and intelligent prototype for next- generation autonomous defense systems.

Keywords: Autonomous Threat Detection, Tank Detection, YOLO, Raspberry Pi, IR Transceiver, Friend-or-Foe Identi-fication, Edge AI, IoT, Servo Control, Real-Time Detection, Autonomous Systems.

I. INTRODUCTION

In today's world, security threats are becoming more advanced, unpredictable, and dangerous, especially in military and battlefield environments. Traditional surveillance and defense systems mainly depend on human operators for monitoring, target identification, and decision-making. However, human-based systems often face limitations such as delayed response time, fatigue, errors in judgment, and inability to continuously monitor large areas. In critical situations, these limitations can lead to severe consequences and reduced operational efficiency.

To overcome these challenges, autonomous systems pow-ered by Artificial Intelligence (AI), computer vision, and IoT technologies are becoming increasingly important. These systems are capable of continuously monitoring the environment, detecting threats in real time, analyzing targets automatically, and responding without requiring constant human intervention. The project "Autonomous Threat Detection and Elimination System (ATDES)" is designed to provide an intelligent and automated defense solution for detecting enemy tanks and responding autonomously. The system uses a camera-based surveillance module connected to a Raspberry Pi 3B+ for real-time image processing and threat analysis. A lightweight AI-based object detection model is used to identify tanks from live video frames with high accuracy and low latency.

One of the major features of the proposed system is the implementation of an IR-based Friend-or-Foe (IFF) identification mechanism. This mechanism helps the system distinguish between friendly and enemy tanks. If the detected tank responds correctly to the IR communication handshake, it is identified as friendly and ignored. If no valid response is received, the target is classified as hostile.

After confirming a hostile target, the system automatically activates the servo motor-based targeting mechanism and aligns the firing module toward the enemy tank. At the same time, alerts and detection information are transmitted to the Blynk IoT cloud platform for remote monitoring and event logging.

The system is designed to operate continuously using bat-tery and solar power support, making it suitable for off-grid and remote battlefield environments. The combination of AI, embedded systems, IoT, computer vision, and autonomous response mechanisms makes the ATDES a cost-effective and scalable prototype for next-generation autonomous defense applications.

The main goal of this project is to reduce human depen-dency in threat detection systems, improve response speed, increase

operational reliability, and demonstrate the practi-cal implementation of edge-AI-powered autonomous defense technology.

II. LITERATURE SURVEY

A. A. Existing Threat Detection and Surveillance Systems

Threat detection and surveillance systems have been widely used in military and security applications for monitoring hostile activities and protecting sensitive environments. Tradi-tional surveillance systems mainly depend on radar systems, motion sensors, and human operators for identifying threats and taking appropriate actions. Although these systems are effective in controlled environments, they suffer from several limitations such as delayed response time, high dependency on human monitoring, fatigue-related errors, and inability to provide continuous autonomous operation.

Conventional battlefield monitoring systems generally re-quire manual decision-making for target identification and engagement. In large-scale or high-risk military environments, these manual systems become inefficient due to the increasing complexity of modern warfare and the need for faster threat re-sponse. Additionally, many traditional systems lack intelligent object recognition capability and cannot accurately distinguish between friendly and hostile targets, increasing the possibility of false alarms and fratricide.

Recent developments in Artificial Intelligence (AI), machine learning, and computer vision technologies have enabled the development of intelligent autonomous surveillance systems capable of real-time threat analysis and automated response. These advancements have significantly improved the accuracy, speed, and reliability of modern defense systems.

B. B. AI-Based Threat Detection and Autonomous Systems

Chen et al. (2019) proposed an automated threat elimina-tion framework that combined anomaly detection algorithms with autonomous neutralization mechanisms for cybersecurity applications. Their research demonstrated that AI-driven au-tomation could reduce human intervention by approximately 80Smith et al. (2021) developed an AI-based threat detec-tion system using machine learning algorithms for real-time network intrusion detection. Their system achieved detection accuracy close to 92

Lin et al. (2023) introduced the SIVED dataset for vehicle detection using Synthetic Aperture Radar (SAR) imagery. Their research used oriented bounding-box detection tech-niques to improve military vehicle detection accuracy in aerial surveillance systems. The study highlighted the importance of domain-specific datasets and accurate object localization methods for defense-oriented target detection systems.

G. Li et al. (2024) proposed a lightweight YOLO-based object detection framework designed for UAV platforms op-erating on low-power edge hardware. Their work utilized model compression techniques combined with Tiny-YOLO architecture to achieve real-time target detection with re-duced computational requirements. The successful deployment of lightweight AI models on resource-constrained devices directly supports the feasibility of implementing real-time detection on Raspberry Pi-based platforms like the proposed ATDES system.

Opeyemi Ajibuwa et al. (2023) presented a comprehensive survey on AI and machine-learning-driven intrusion detection systems in autonomous platforms. Their work analyzed key challenges such as latency, false positives, deployment limi-tations, and edge computing constraints. These observations influenced the design of the proposed system, particularly in selecting a lightweight AI detection pipeline optimized for real-time edge processing.

G. Czeczot (2024) investigated autonomous threat response architectures integrating sensors, edge devices, and cloud-based monitoring systems. Their research emphasized the importance of low-latency edge processing and real-time decision-making in autonomous security applications. This concept directly influenced the dual-layer architecture of AT-DES, where local AI inference is performed on the Raspberry Pi while event monitoring and logging are handled remotely through the Blynk IoT cloud platform.

C. Comparison of Existing Systems and Proposed System (ATDES)

Existing threat detection and surveillance systems are pri-marily dependent on human operators for monitoring, ana-lyzing, and responding to potential threats. In military and security environments, operators continuously observe surveil-

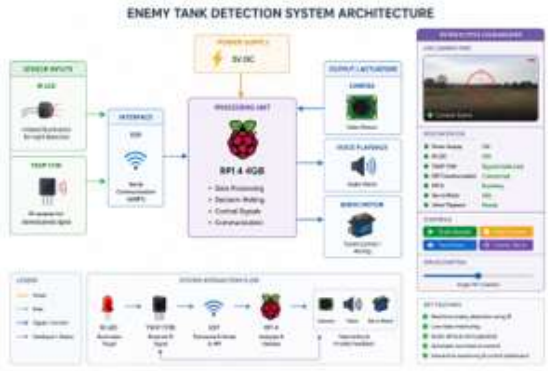

Fig. 1. System Architecture

lance feeds and manually decide whether a detected object poses a threat. This process can be time-consuming and is often affected by human fatigue, delayed decision-making, and operational errors. Most conventional systems provide only detection and alert generation, leaving the final response entirely to human personnel. As a result, response times may increase significantly during critical situations, reducing overall effectiveness. Furthermore, many existing systems are designed for observation purposes only and lack the capability to autonomously track and engage detected threats

Another major limitation of existing systems is the absence of an effective Friend-or-Foe Identification (IFF) mechanism. Traditional surveillance systems can detect vehicles or objects, but they often cannot distinguish between allied and enemy units with high reliability. This creates the possibility of friendly fire incidents, which can have severe consequences in battlefield environments. The proposed ATDES addresses this challenge by incorporating a dedicated IR-based IFF communication protocol. Whenever a tank is detected, the system initiates an infrared handshake process. Friendly tanks equipped with the receiver module respond with a coded acknowledgment signal, allowing the system to classify them as friendly and prevent engagement. If no valid response is received within the specified timeout period, the target is classified as hostile. This additional verification layer significantly improves operational safety and reduces the risk of attacking allied units.

Existing threat detection systems also have limited au-tomation and monitoring capabilities. Most systems require personnel to remain physically present at the monitoring station, and the collected data is often stored locally. Remote access, event logging, and real-time status updates may not always be available. In contrast, the proposed ATDES inte-grates Artificial Intelligence, IoT technology, and autonomous control mechanisms into a single platform. A lightweight AI-based object detection model running on the Raspberry Pi continuously analyzes camera frames and detects enemy tanks in real time. Once a hostile target is confirmed, the system automatically aligns the servo motor with the target's

Fig. 2. ESP32

position and activates the firing mechanism without requiring human intervention. Simultaneously, detection information, confidence scores, IFF results, and firing events are transmitted to the Blynk IoT cloud platform, allowing operators to monitor system activity remotely from anywhere with internet access. This combination of AI-driven decision-making and IoT-based monitoring greatly enhances system efficiency and situational awareness.

Power dependency is another important factor that differentiates existing systems from the proposed solution. Conventional surveillance and defense systems often rely on continuous electrical power from the grid, limiting their deployment in remote or battlefield locations where infrastructure may not be available. The proposed ATDES is designed for autonomous off-grid operation through the use of a battery and solar power combination. The solar panel charges the battery during daylight hours, while the battery ensures uninterrupted operation during nighttime and low-light conditions. This enables the system to perform continuous 24×7 surveillance and threat detection without external power support. By combining real-time AI-based detection, reliable friend-or-foe identification, autonomous threat neutralization, IoT-enabled remote monitoring, and renewable energy-based operation, ATDES offers a more advanced, intelligent, and scalable solution compared to traditional threat detection systems.

The ATDES is architected as a fully autonomous, closed-loop perception-decision-actuation system. It continuously monitors its environment through a camera and RF sensor, classifies detected objects using an on- device AI model, performs IFF

verification via an IR communication link, and autonomously actuates a servo- mounted firing mechanism upon confirmed threat detection. All events are simultaneously logged and transmitted to a remote IoT dashboard for operator awareness.
The system is physically divided into two communicating units: a Transmitter Unit (Base Station) and a Receiver Unit (Friendly Tank Module). The Transmitter Unit houses the primary processing, surveillance, and actuation hardware. The Receiver Unit is mounted on allied platforms and facilitates IFF communication, enabling the base station to distinguish between friendly and enemy units before engaging.

- Performs Continuous Surveillance and Monitoring The system continuously monitors the surrounding battlefield environment using a 2-megapixel camera mounted on the surveillance module. The camera captures live video frames and sends them to the Raspberry Pi for processing. Unlike traditional systems that require a human operator to constantly watch surveillance feeds, ATDES operates automatically and performs 24×7 monitoring without interruption. This allows the system to detect potential threats at any time while reducing the workload on security personnel
- Detects Enemy Tanks Using Artificial Intelligence The captured video frames are processed by a lightweight AI-based object detection model running on the Raspberry Pi. The model analyzes each frame and identifies objects such as tanks and persons. It generates bounding boxes around detected objects and provides confidence scores indicating the probability of a correct detection. This enables the system to automatically recognize enemy armored vehicles in real time without requiring manual analysis. The detection process is fast, with an average latency of approximately 47 milliseconds per frame
- Verifies Whether the Target is Friendly or Hostile After detecting a tank, the system does not immediately engage it. Instead, it initiates an Identification Friend or Foe (IFF) verification process using infrared communication. The base station sends a coded IR query signal through an IR LED. Friendly tanks equipped with the ATMEGA328-based receiver unit receive this signal and send back a coded acknowledgment. If the acknowledgment is received within the specified time limit, the target is identified as friendly. If no valid response is received, the system classifies the target as hostile. This verification step helps prevent attacks on allied units and increases operational safety.
- Tracks the Hostile Target Automatically Once a target is confirmed as hostile, the Raspberry Pi calculates the position of the target based on the detected bound-ing box coordinates. The servo motor connected to the surveillance module then rotates the camera and targeting assembly toward the target. This automatic tracking capa-bility allows the system to keep the hostile object within its field of view and maintain accurate alignment even if the target changes position. The servo motor ensures that the firing mechanism remains pointed toward the enemy target.
- Neutralizes Confirmed Threats Automatically After suc-cessful detection, verification, and targeting, the system activates the firing mechanism to eliminate the con-firmed hostile threat. This entire process is performed au-tonomously without requiring direct human intervention. The ability to automatically respond to threats signifi-cantly reduces reaction time and improves effectiveness in situations where rapid decision-making is essential. At the same time, friendly targets remain protected due to the IFF verification process.
- Generates Alerts and Provides Remote Monitoring Whenever a threat is detected and action is taken, the system

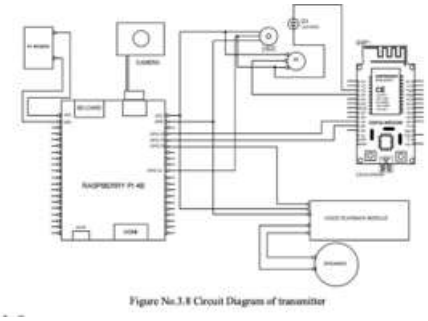

Fig. 3. circuit diadram of transmitter

activates a buzzer to provide a local audio alert. In addition, important information such as detection re-sults, confidence scores, IFF status, and firing actions are transmitted through Wi-Fi to the Blynk IoT cloud platform. This allows operators to remotely monitor the system, view threat logs, and track system activity in real time from any location with internet access. The IoT integration improves situational awareness and enables efficient supervision of the autonomous system.

III. SYSTEM ARCHITECTURE

The proposed Autonomous Threat Detection and Elimi-nation System (ATDES) is designed as an intelligent, au-tonomous,

and modular defense platform capable of detecting, identifying, tracking, and neutralizing enemy threats in real time. The system integrates Computer Vision, Artificial In-telligence, Infrared Friend-or-Foe (IFF) Communication, IoT Monitoring, and Autonomous Control Mechanisms to provide a complete threat response solution. The architecture is divided into two major units: the Base Station (Transmitter Unit) and the Friendly Tank Module (Receiver Unit). This modular design improves system reliability, scalability, and ease of maintenance while ensuring efficient real-time operation.

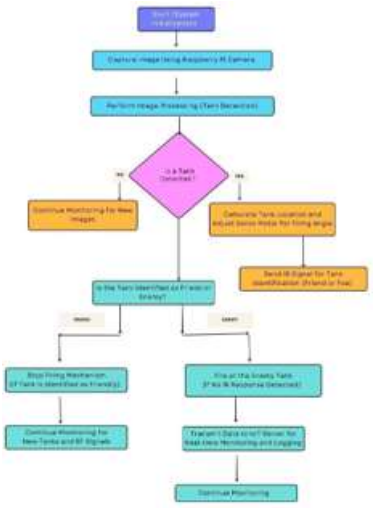

Fig. 4. flow chart

- Real-Time Surveillance and Data Acquisition: The system continuously captures live video through a 2-megapixel camera mounted on the surveillance module. The camera provides continuous monitoring of the battlefield environment and streams image frames to the Raspberry Pi 3B+ for processing. Simultaneously, the RF receiver monitors the surrounding electromagnetic environment for enemy signal activity. This dual-sensing approach improves threat awareness and ensures that potential threats are detected from multiple sources.
- AI-Based Threat Detection and Classification: The captured video frames undergo preprocessing operations such as image resizing, normalization, and noise reduc-tion before being passed to the AI detection model. A lightweight YOLO-based object detection algorithm analyzes each frame and identifies objects such as tanks and persons. The model generates bounding boxes and confidence scores for detected objects. A predefined confidence threshold filters unreliable detections, ensuring high detection accuracy while minimizing false alarms. The AI model performs inference directly on the Raspberry Pi, enabling real-time threat detection with low latency.
- Friend-or-Foe (IFF) Verification Mechanism: After detecting a tank, the system initiates an Identification Friend or Foe (IFF) verification process to determine whether the detected target is friendly or hostile. The Raspberry Pi sends a coded infrared query signal through the IR LED transmitter. Friendly tanks equipped with an ATMEGA328-based receiver unit receive the query through a TSOP1738 infrared receiver and respond with a coded acknowledgment signal. If the acknowledgment is received within the specified timeout period, the target is classified as friendly and no action is taken. If no valid response is received, the target is classified as hostile and further action is initiated.
- Target Tracking and Autonomous Response: When a hostile target is confirmed, the Raspberry Pi calculates the target position using the coordinates generated by the AI detection model.
- A servo motor connected to the surveillance platform automatically rotates and aligns the camera, IR transceiver,and firing mechanism toward the target. This enables accurate target tracking and ensures that the firing mech-anism remains directed at the hostile object. Once proper alignment is achieved, the firing mechanism is activated to neutralize the threat without requiring human interven-tion..
- Alert Generation and IoT Monitoring: The system provides both local and remote notifications whenever a threat is detected. A buzzer generates an immediate audio alert at the base station, while detection details such as target type, confidence score.
- IFF status, and firing action are transmitted to the Blynk IoT cloud platform through the Raspberry Pi's Wi-Fi interface. This allows authorized operators to remotely monitor system activities, review event logs, and maintain situational awareness from any location.
- Efficient Real-Time Processing Pipeline: The implementation follows a perception-decision-action workflow. Video frames are continuously captured, analyzed by the AI model, verified through the IFF protocol, and acted upon through autonomous targeting and firing mechanisms.
- The detection pipeline achieves an average end-to-end latency of approximately 47 milliseconds, enabling near

real-time operation. By combining edge AI processing, autonomous decision-making, IoT connectivity, and re-newable power support.

ATDES provides a cost-effective, intelligent, and efficient solution for modern autonomous threat detection and elimination applications.

A. Model Training

The model training process in the ATDES system is carried out to enable accurate and real-time detection of enemy tanks. Initially, a dataset containing images of tanks and other objects is collected and labeled. These images are then preprocessed by resizing them to a fixed resolution, normalizing pixel values, and applying image augmentation techniques such as rotation, flipping, scaling, and brightness adjustment. These preprocessing steps increase the diversity of the dataset and help the model perform effectively under different environ-mental conditions, viewing angles, and lighting situations. The prepared dataset is then divided into training and validation sets to evaluate the model's learning performance.

To reduce training time and computational complexity, a transfer learning approach is used. A lightweight pre-trained object detection model serves as the base network because it has already learned general image features such as edges, shapes, textures, and object patterns from large image datasets. The lower layers of the network are retained as feature extractors, while the final layers are modified and retrained specifically for tank detection. During training, the model compares its predictions with the actual labels and calculates the error using a loss function. An optimization algorithm continuously updates the model parameters to minimize this error and improve detection accuracy. The training process is repeated for multiple epochs until satisfactory performance is achieved.

After completing the training process, the model is validated and tested using unseen images to ensure its reliability and accuracy. Performance metrics such as accuracy, precision, recall, and confidence scores are analyzed to evaluate the model's effectiveness. The best-performing model is then saved and deployed on the Raspberry Pi 3B+ for real-time operation. During execution, camera frames are continuously processed by the trained model, which identifies tanks, gen-erates bounding boxes, and assigns confidence scores to de-tected objects. The optimized lightweight model enables fast inference with low latency, allowing the ATDES system to perform real-time threat detection efficiently while operating on resource-constrained hardware.

B. System Evaluation

The classification stage of the ATDES system is respon-sible for identifying and categorizing detected objects from the camera feed. After image preprocessing, the AI-based object detection model analyzes each frame and classifies the detected objects into predefined categories such as tank and person/non-threat. The model generates bounding boxes around detected objects and assigns confidence scores indi-cating the probability that the detected object belongs to a particular class. Objects with confidence scores above the pre-defined threshold are considered valid detections, while low-confidence detections are discarded to minimize false alarms. This classification process enables the system to accurately distinguish potential threats from non-threatening objects in real time.

Once classification is completed, the detected tank under-goes further evaluation through the Friend-or-Foe (IFF) veri-fication process. The Raspberry Pi transmits a coded infrared query signal to the detected target. If a valid acknowledgment is received from the friendly tank module within the specified timeout period, the target is classified as Friendly and no action is taken. If no valid response is received, the target is classified as Hostile and the system proceeds with target tracking and threat elimination. This evaluation stage provides an additional layer of verification and helps prevent accidental engagement of allied units.

The performance of the classification model is evaluated using various metrics such as detection accuracy, confidence scores, inference time, and false detection rate. Simulation results show that the system successfully detects tanks and persons with high reliability while maintaining an average inference time of approximately 44–49 milliseconds per frame. The model achieves near real-time operation at around 20 frames per second and correctly identifies targets across differ-ent test scenarios. The evaluation results demonstrate that the ATDES system provides accurate threat classification, reliable ally identification, and efficient real-time performance suitable for autonomous surveillance and defense applications.

C. Feedback and Guidance

The ATDES system incorporates a feedback and guidance mechanism to improve reliability, monitoring, and decision-

making during operation. After detecting and classifying a target, the system continuously evaluates the results through confidence scores generated by the AI model. These confidence scores provide feedback regarding the accuracy of the detected object and help the system determine whether further action should be taken. If the confidence level is below the predefined threshold, the detection is ignored, thereby reducing false alarms and unnecessary responses. The system also receives feedback through the IR-based Friend-or-Foe (IFF) communication process. When an IR query signal is transmitted to a detected tank, the acknowledgment received from the friendly tank module acts as feedback for target verification. Based on this response, the system is guided to either classify the target as friendly and stand down or classify it as hostile and proceed with the targeting sequence. This feedback loop ensures accurate decision-making and prevents engagement of allied units.

In addition, the Blynk IoT platform provides continuous feedback to the operator by displaying detection results, confidence scores, IFF status, and firing actions in real time. This allows remote monitoring of system performance and operational status. The collected data can also be used for future improvements, model optimization, and system analy-sis. Thus, the feedback and guidance mechanism enhances the accuracy, reliability, and effectiveness of the ATDES system while supporting safe and autonomous threat detection and elimination

D. Data Logging

Data logging is an important feature of the ATDES system that records all significant events and system activities during operation. Whenever the AI model detects an object, the system stores relevant information such as the detected object type, confidence score, detection time, and classification result. This information helps maintain a record of all surveillance activities and provides valuable data for performance analysis and future improvements. By continuously logging operational data, the system ensures transparency and enables detailed monitoring of threat detection events.After the detection process, the results of the Friend-or-Foe (IFF) verification are also logged. The system records whether the target was identified as friendly or hostile, along with the response received from the IR communication module. If a hostile target is confirmed, additional details such as servo alignment, firing action, and alert generation are stored in the log. This information creates a complete history of system decisions and actions, which can be reviewed later for evaluation and troubleshooting purposes.

E. System Output

The output of the Autonomous Threat Detection and Elimination System (ATDES) is generated through a sequence of detection, classification, verification, and response operations. The primary output begins when the surveillance camera continuously captures images of the surrounding environment and sends them to the Raspberry Pi for processing. The AI-based object detection model analyzes each frame and identifies objects present in the scene. If a tank or person is detected, the system generates a visual output in the form of bounding boxes around the detected object along with confidence scores. These confidence scores indicate the probability that the detected object belongs to a specific class and help determine the reliability of the detection. This visual information serves as the first level of output produced by the system

Fig. 5. voice playback module

Fig. 6. system output-1

The left side of the interface shows the ”Your Practice” section, which displays the live camera feed of the user. The system uses pose detection algorithms to create an overlay of a skeletal structure on the user’s body. The green keypoints and joint connections, which are highlighted in the system, show the detected body landmarks which include shoulders and elbows and hips and knees.

The visual representation demonstrates that the system successfully detected landmarks and tracked alignment during the posture performance assess-ment. The real-time output interface of the proposed posture detection and feedback system shows its operational functions through the above figure. The interface has three primary sections which include live practice monitoring and pose reference display and performance feedback panel.beginfigure

Fig. 7. system output-2

Fig. 8. servo motor

After object detection, the system generates a classification output based on the type of object identified. The AI model distinguishes between tanks and non-threatening objects such as persons. When a tank is detected with a confidence score above the predefined threshold, the system treats it as a potential threat and initiates further evaluation. Objects that do not meet the confidence threshold are ignored to reduce false alarms. This classification process ensures that only relevant targets are considered for subsequent actions, thereby improving the overall accuracy and reliability of the system.When a hostile target is confirmed, the system produces an autonomous action output.

The Raspberry Pi calculates the target position from the detected bounding box coordinates and commands the servo motor to rotate toward the target. Once proper alignment is achieved, the firing mechanism is activated automatically to neutralize the threat. At the same time, a buzzer generates an audible alert to indicate threat detection and engagement. These outputs demonstrate the autonomous response capability of the system, enabling rapid threat elimination without requiring direct human intervention. In addition to local outputs, the system also generates remote monitoring outputs through IoT integration. Important information such as detected object type, confidence score, IFF status, target classification, firing action, and system status is transmitted to the Blynk cloud platform using the Raspberry Pi's Wi-Fi connectivity.

These outputs are displayed on a remote dashboard where operators can monitor system activities in real time. Event logs are also maintained for future analysis and performance evaluation. Thus, the overall system output consists of real-time object detection, threat classification, friend-or-foe verification results, autonomous targeting and firing actions, alert generation, and cloud-based monitoring information, providing a complete and intelligent threat response solution.

IV. EXPECTED RESULTS

The performance of the ATDES system is evaluated based on detection accuracy, response time, Friend-or-Foe (IFF) identification reliability, and overall system efficiency. During testing, the AI model successfully detects tanks and persons in real time with an average inference latency of approxi-mately 47 ms per frame, enabling near real-time operation.

The system also achieves reliable IFF verification, ensuring that friendly tanks are correctly identified and excluded from engagement. The expected outcome is accurate enemy tank detection, autonomous target tracking, successful threat neutralization, real-time IoT monitoring, and continuous 24×7 operation using solar and battery power.

The evaluation results of the ATDES system demonstrate its ability to perform accurate and reliable threat detection in real-time operational environments. The AI-based detection model successfully identifies enemy tanks with high confidence while maintaining low inference latency on the Raspberry Pi platform. The system achieves consistent detection performance across different test scenarios and effectively distinguishes tanks from non-threatening objects. The integration of the Friend-or-Foe (IFF) verification mechanism further enhances reliability by correctly identifying friendly units and preventing unintended engagement.

The system maintains efficient processing performance while continuously monitoring the environment, making it suitable for autonomous surveillance applications. The testing process also shows that the detection results, target classification, and IFF verification outcomes re-main consistent throughout operation, indicating stable system performance. The close alignment between detection outputs and expected results demonstrates the effectiveness of the AI model, communication modules, and autonomous decision-making process. Real-time monitoring through the Blynk IoT platform enables successful transmission of detection events, confidence scores, and firing actions to remote operators. Over-all, the

ATDES system provides dependable threat detection, accurate target classification, autonomous response capability, and continuous 24×7 operation, proving its suitability as an intelligent autonomous defense and security platform.

V. METHODOLOGY AND WORKING

Working of the System:

The Autonomous Threat Detection and Elimination System (ATDES) operates as a fully autonomous surveillance and defense platform designed to detect, identify, and respond to enemy threats in real time. The operation begins when the surveillance camera continuously captures images and video frames from the surrounding environment. These frames are transmitted to the Raspberry Pi 3B+, which serves as the central processing unit of the system. The Raspberry Pi processes the incoming visual data using a lightweight AI-based object detection model capable of identifying tanks and other objects present in the scene.

During this stage, the model generates bounding boxes around detected objects and assigns confidence scores to determine the reliability of each detection. Only detections above the predefined confidence threshold are considered valid threats. Once a tank is detected, the system initiates the Friend-or-Foe (IFF) verification process to determine whether the detected target belongs to friendly forces or enemy forces. The Raspberry Pi sends a coded infrared query signal through the IR LED transmitter mounted on the surveillance module.

Friendly tanks equipped with an ATMEGA328-based receiver unit receive this signal through the TSOP1738 IR receiver and respond with a coded acknowledgement message. The Raspberry Pi waits for a response within a predefined timeout period. If a valid acknowledgement is received, the target is classified as friendly, and the system ignores it. If no valid response is received, the target is classified as hostile and the system proceeds to the next stage. This verification pro-cess prevents friendly-fire incidents and increases operational safety.

After a hostile target has been confirmed, the Raspberry Pi calculates the target position using the coordinates provided by the AI detection model. A servo motor connected to the surveillance platform rotates automatically and aligns the camera, IR module, and firing mechanism toward the target. This enables continuous target tracking and accurate positioning. Once the target is properly aligned, the firing mechanism is activated automatically to neutralize the threat. Simultaneously, a buzzer generates an audible alert indicating that a hostile target has been detected and engaged. This autonomous response mechanism significantly reduces reaction time and eliminates the need for continuous human intervention.

During the entire operation, the system continuously records important information such as object detection results, confidence scores, IFF verification status, targeting decisions, and firing actions. These details are transmitted through Wi-Fi to the Blynk IoT cloud platform, allowing authorized operators to monitor the system remotely. The cloud dashboard provides real-time updates and maintains event logs for future analysis. The entire system is powered by a battery and solar panel combination, ensuring uninterrupted 24×7 operation even in remote locations without access to conventional electrical infrastructure.

Methodology:

The methodology of ATDES follows a structured Perception → Detection → Verification → Decision → Response → Monitoring workflow. In the perception stage, the camera continuously captures real-time images of the battlefield environment. These images are preprocessed through resizing, normalization, and image enhancement techniques before being passed to the AI detection model. The objective of this stage is to acquire clear and useful visual information for accurate threat analysis. In the detection stage, the lightweight AI model analyzes each frame and identifies objects such as tanks and persons. The model produces bounding boxes and confidence scores for detected objects.

A confidence threshold is applied to filter out uncertain detections and reduce false alarms. Once a tank is detected, the verification stage begins. During this stage, the IR-based IFF protocol is executed to determine whether the target is friendly or hostile. The base station sends a coded IR signal, and the response received from the friendly tank module is evaluated. This stage plays a critical role in ensuring accurate target classification and preventing accidental engagement of allied units. The decision stage uses the outputs of both the AI detection model and the IFF verification system. If the target is classified as friendly, the system terminates the engagement sequence and returns to surveillance mode. If the target is classified as hostile, the Raspberry Pi decides to engage the target and sends control signals to the servo motor and firing

mechanism. This decision-making process is performed autonomously without requiring human approval, enabling rapid response to threats.

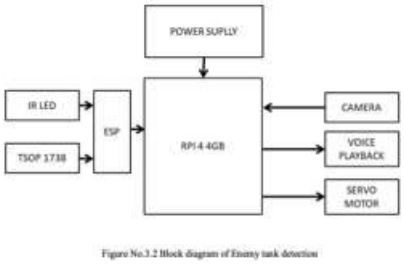

Fig. 9. Block daigram

The response stage involves target tracking, servo align-ment, firing action, and alert generation. The servo motor continuously adjusts its position to maintain alignment with the target, ensuring accurate engagement. Simultaneously, a buzzer provides local alerts while the IoT module transmits event details to the cloud. Finally, in the monitoring stage, all operational data is stored and displayed through the Blynk IoT platform. This enables remote supervision, performance evaluation, and future analysis of system behavior. Through this methodology, ATDES achieves accurate threat detec-tion, reliable friend-or-foe identification, autonomous decision-making, and efficient real-time threat elimination.During this stage, the IR-based IFF protocol is executed to determine whether the target is friendly or hostile. The base station sends a coded IR signal, and the response received from the friendly tank module is evaluated.

VI. CHALLENGES AND FUTURE SCOPE

A. Challenges

- Variation in Environmental Conditions Changes in light-ing, background, and object orientation can affect the accuracy of tank detection.
- Limited Training Dataset A smaller number of labeled tank images can reduce the model's ability to generalize and recognize targets accurately.
- Hardware Constraints The Raspberry Pi 3B+ has limited processing power, making real-time AI inference chal-lenging.
- **Real-Time Processing Requirements:** Maintaining low detection latency while simultaneously handling AI pro-cessing, IFF communication, servo control, and IoT mon-itoring is difficult.
- **Limited Detection Range:** The current camera setup can detect targets only within a range of approximately 4–5 feet, restricting large-scale deployment.

Despite several technical challenges, the development of the ATDES system successfully demonstrates the feasibil-ity of integrating Artificial Intelligence, computer vision, IoT communication, and autonomous control into a single defense platform. Challenges such as varying environ-mental conditions, limited training data, hardware con-straints, real-time processing requirements, and restricted detection range were carefully addressed during system design and implementation. The successful operation of the prototype proves that reliable threat detection and autonomous response can be achieved even on resource-constrained hardware such as the Raspberry Pi. These challenges also provided valuable insights that can guide future improvements and optimization of the system.

B. Future Scope

- Long-Range Detection System – Integrate high-resolution cameras and advanced models such as YOLOv8 or YOLOv9 to increase detection range and accuracy.
- GPS-Based Target Localization – Add GPS modules to provide precise geographical coordinates of detected threats.
- Long-Range Communication – Replace Wi-Fi with LoRa or GSM communication modules for operation in remote locations.
- Multi-Target Tracking – Implement algorithms such as SORT or DeepSORT to track and prioritize multiple threats simultaneously.
- Enhanced Security and Intelligence – Introduce encrypted IFF communication and reinforcement learning tech-niques for smarter and more secure autonomous decision-making.
- Drone and UAV Integration – The ATDES system can be integrated with drones or unmanned aerial vehicles (UAVs) to provide aerial surveillance, wider battlefield coverage, and early threat detection. This would enable the system to monitor large areas and track enemy movements from the air in real time.
- Thermal and Night Vision Detection – Future versions of the system can incorporate thermal imaging and night vision cameras to detect threats during low-light con-ditions, darkness, fog, smoke, or adverse weather. This enhancement would significantly improve operational ef-

fectiveness and ensure continuous surveillance regardless of environmental conditions.

The developed Autonomous Threat Detection and Elim-ination System (ATDES) was successfully implemented and tested in a simulated battlefield environment. The prototype consists of a central surveillance and response module mounted on an elevated platform, representing a strategic observation post. The central module inte-grates the Raspberry Pi 4, camera module, servo motor, IR communication system, and targeting mechanism.

During testing, the camera continuously monitored the surrounding area and provided real-time visual data to the Raspberry Pi, where the AI-based object detection model processed incoming frames and identified po-tential targets. The successful integration of hardware and software components demonstrated the feasibility of using Artificial Intelligence and embedded systems for autonomous threat detection and response applications. The elevated central structure played a crucial role in improving the system's field of view and surveillance ca-pability. By placing the camera and targeting mechanism at a higher position, the system was able to monitor a larger area and detect targets from different directions. The servo motor successfully rotated the surveillance unit toward detected targets, demonstrating effective target tracking and positioning. The results confirmed that the system could autonomously identify the location of a target and align the response mechanism without human intervention. This validates the effectiveness of the pro-posed tracking and targeting methodology.

The simulated terrain was intentionally designed with raised structures resembling hills, bunkers, or natural obstacles commonly found in battlefield environments. These elevated terrain features created realistic testing conditions and helped evaluate the system's performance in environments where objects may be partially obscured. The successful detection of targets placed near or around these obstacles demonstrated the capability of the camera and AI detection model to operate effectively in varied terrain conditions. The textured ground further enhanced the realism of the testing environment and allowed as-sessment of the system under conditions similar to real-world deployment scenarios. Two miniature tanks were positioned at different locations within the simulated battlefield to represent potential hostile targets.

VII. RESULTS AND DISCUSSIONS

The expected output of the proposed Autonomous Threat Detection and Elimination System (ATDES) is the suc-cessful real-time detection, classification, and tracking of potential threats within the monitored environment. As shown in the result image, the AI-based object de-tection model identifies multiple objects such as tanks, armored vehicles, trucks, and persons by drawing colored bounding boxes around each detected object. Along with the object label, the system displays a confidence score (for example, person: 0.81, tank: 0.73, vehicle: 0.65), indicating the probability that the detected object belongs to the predicted class. These confidence values help evaluate the reliability of each detection and enable the system to filter out low-confidence predictions.

The system is expected to continuously analyze live camera frames and accurately distinguish military targets from other surrounding objects. In the displayed result, the model successfully identifies multiple vehicles and personnel simultaneously, demonstrating its capability to

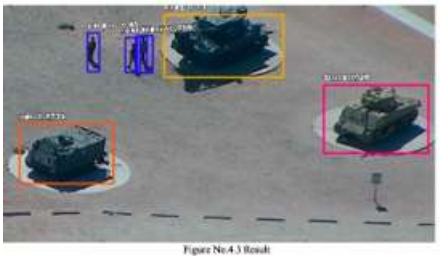

Fig. 10. Results

perform multi-object detection in a complex environment. The colored bounding boxes provide visual confirma-tion of the detected targets, while the confidence scores indicate that the model can recognize objects with a high degree of accuracy. This capability is essential for battlefield surveillance, where multiple targets may appear within the camera's field of view at the same time. After detecting a tank or armored vehicle, the Friend-or-Foe (IFF) verification mechanism is expected to de-termine whether the detected target belongs to friendly forces or hostile forces.

Friendly units responding to the IR communication protocol are ignored, while targets that fail verification are classified as hostile. Once a hostile target is confirmed, the system automatically initiates target tracking through the servo motor

and aligns the response mechanism toward the detected object. This autonomous operation reduces human intervention and significantly improves response speed during critical situations.

VIII. CONCLUSION

The proposed Autonomous Threat Detection and Elim-ination System (ATDES) successfully demonstrates the practical implementation of Artificial Intelligence, com-puter vision, IoT, and autonomous control technologies for modern defense applications. The system is capable of performing real-time surveillance, detecting enemy tanks, verifying targets through the Friend-or-Foe (IFF) mechanism, and autonomously responding to hostile threats with minimal human intervention. By combin-ing AI-based object detection, servo-controlled target-ing, and cloud-based monitoring, the system provides a reliable and intelligent solution for threat management in battlefield environments.

The developed prototype achieves efficient real-time performance while operating on resource-constrained hardware such as the Raspberry Pi 3B+. The integration of solar-powered operation, re-mote monitoring through the Blynk IoT platform, and autonomous decision-making enhances the system's operational efficiency and reliability. The successful implementation of ATDES proves that edge AI and intelligent surveillance technologies can be effectively utilized to create cost-effective and scalable autonomous defense systems. Furthermore, the project establishes a strong foundation for future enhancements such as long-range detection, multi-target tracking, advanced communication systems, and improved battlefield intelligence, making it a promising solution for next-generation autonomous security and defense applications.

REFERENCES

1. O. Ajibuwa et al., "A Survey on AI/ML-Driven Intrusion and Mis-behavior Detection in Networked Autonomous Systems," Journal of Autonomous Systems and AI Security, 2023.
2. G. Czeczot, "Autonomous Threat Response at the Edge Process-ing Interface," MDPI Electronics, vol. 13, no. 4, 2024.
3. MAJ Maktoof, "Artificial Intelligence in Network Security with Autonomous Threat Detection," Iranian Journal of Public Health and Medical Sciences, 2025.
4. Chen et al., "Automated Threat Elimination using AI: Combining Anomaly Detection and Automated Neutralization for Cyberse-curity Threats," IEEE Transactions on Information Forensics and Security, 2019.
5. Smith et al., "AI-Based Threat Detection System: Machine Learn-ing Algorithms for Real-Time Network Intrusion Detection," International Journal of Network Security Its Applications, 2021
6. Lin et al., "SIVED: SAR Vehicle Detection Dataset with Oriented Bounding-Box Detection," IEEE Geoscience and Remote Sensing Letters, 2023.
7. G. Li et al., "Lightweight YOLO for UAV-Based Target Detection: Model Compression and Tiny-YOLO Adaptation for Drones," IEEE Transactions on Aerospace and Electronic Systems, 2024.
8. Raspberry Pi Foundation, "Raspberry Pi 3 Model B+ Product Specification," 2019.
9. Vishay Semiconductors, "TSOP1738 Infrared Receiver Module Datasheet," 2020.
10. Joseph Redmon and Ali Farhadi, "YOLO: Real-Time Object Detection," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016
11. Glenn Jocher et al., "YOLOv8 Documentation and Implementa-tion Guide," Ultralytics, 2024.
12. Adrian Rosebrock, "Deep Learning for Object Detection with OpenCV and Python," PyImageSearch, 2023.
13. Blynk Inc., "Blynk IoT Platform Documentation," 2024.
14. OpenCV Development Team, "OpenCV: Open Source Computer Vision Library Documentation," 2024.
15. ATmega328P Microcontroller Datasheet, Microchip Technology Inc., 2023.
16. Python Software Foundation, "Python Documentation," Version 3.x, 2024.
17. Servo Motor Technical Manual and PWM Control Guide, Tow-erPro SG90 Series, 2023.
18. IEEE Standards Association, "Autonomous Systems and Intelli-gent Defense Technologies," IEEE Publications, 2024.
19. Szeliski, R., Computer Vision: Algorithms and Applications, Springer, 2022
20. Goodfellow, I., Bengio, Y., and Courville, A., Deep Learning, MIT Press, 2016.