WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CAMDEC AI

Mrs. K. Srisathiya[1], Gokulavani K[2], Mehala K[3], Ramya K[4], Sneka T[5],

[1]Assistant Professor, Department of Artificial Intelligence and Data Science,
Dhirajlal Gandhi College of Technology (Autonomous), Salem - 636309
[2345] Department of Artificial Intelligence and Data Science,
Dhirajlal Gandhi College of Technology (Autonomous), Salem – 636309
[1]*srisathiya.aids@dgct.ac.in*, [2]*gokulavani.ai.ds@gmail.com*, [3]*mehala0609@gmail.com*, [4]*ramyakuberan56@gmail.com*, [5] *snehaammu364@gmail.com*

ABSTRACT :

This project presents a deep learning-based security solution titled "CAMDEC AI" for monitoring forest trails or restricted zones. The system is designed to detect potential threats such as weapons and suspicious individuals in real time using a camera and the YOLOv8 object detection algorithm. The dataset includes six critical classes: Knife, Machete, Person, Pistol, Rifle, and Rod. Raw images were collected, annotated, and processed using Roboflow, then trained in Google Collaboratory to develop a robust detection model.

On the hardware side, the system integrates an Arduino Uno, GPS, IoT, and LCD. Once a threat is detected, such as a person carrying a weapon, the system immediately retrieves the GPS coordinates and transmits the data to an IoT platform for real-time alerting. The LCD shows the class of the detected object and the alert status. This smart surveillance solution enhances security in remote or sensitive areas, such.

As wildlife reserves, borders, or isolated trails, by providing instant alerts and live threat monitoring. The combination of AI, GPS, and IoT ensures proactive responses to potential dangers, making it a reliable tool for modern digital surveillance and safety systems.

1. INTRODUCTION

1.1 GENERAL:

The CAMDEC AI Using Deep Learning is an innovative security solution to enhance surveillance and safety in remote areas such as forest trails, restricted zones, or wildlife reserves. The project leverages deep learning technology, specifically the YOLOv8 object detection algorithm, to identify potential threats, including weapons and suspicious individuals, in real time. With a focus on detecting six key objects—Knife, Machete, Person, Pistol, Rifle, and Rod—the system aims to provide instant alerts upon detection of any threat.

The process begins by collecting and annotating a raw dataset of images, which are then converted into a suitable format for training the YOLOv8 model. Google Collaboratory is used to train the model, which is capable of recognizing and classifying these objects accurately. Once deployed, the system is integrated with hardware components such as Arduino Uno, an LCD, a GPS module, and an IoT module. When a threat is detected, the system identifies the object, captures the GPS location, and sends this data to an IoT platform for real-time monitoring and alerting. The LCD provides on-site visual feedback of the detection status.

This project bridges the gap between artificial intelligence, hardware, and IoT, offering a reliable, scalable solution for real-time security monitoring and threat detection in isolated or high-risk environments.

2. LITERATURE SURVEY:

1. Title: Real-Time Object Detection Using YOLOv3 for Security Surveillance

Authors: A. Redmon, S. Divvala, R. Girshick, and A. Farhadi

Abstract: This paper introduces a real-time object detection method based on the YOLOv3 algorithm, which is widely used for detecting various objects in surveillance systems. YOLOv3 is trained on large datasets to recognize multiple object classes quickly, making it ideal for security applications. The study discusses its performance in real-world security settings, where real-time object detection is crucial for monitoring and alerting.

Published in: IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016

2. Title: Application of Deep Learning in Video Surveillance for Threat Detection

Authors: L. Zhang, H. Li, Y. Yang, and W. Chen

Abstract: This paper investigates the application of deep learning models, including Convolutional Neural Networks (CNNs), in video surveillance systems for detecting threats and abnormal activities. The authors highlight various object detection models, their applications in security systems, and the challenges of deploying deep learning in real-time surveillance environments.

Published in: Journal of Electronic Imaging, 2018

3. Title: Improved YOLO-Based Real-Time Detection of Threats in Surveillance Systems

Authors: M. K. Kundu, A. Mandal, and S. Banerjee

Abstract: This research explores an enhanced version of YOLO for real-time detection of threats in surveillance video feeds. The authors propose improvements in the YOLO framework to increase detection accuracy and processing speed for use in real-time security systems. The paper provides insights into optimizing deep learning models for use in surveillance applications.

Published in: International Journal of Computer Vision and Image Processing, 2020

4. Title: IoT-Enabled Security Systems for Remote Monitoring Using Object Detection

Authors: R. Kumar, M. Rajput, and S. Dey

Abstract: This study focuses on the integration of IoT technology with object detection systems for monitoring remote or restricted areas. The authors propose a system that uses AI-based object detection algorithms along with IoT modules for real-time monitoring and alerting. The paper discusses the potential for IoT to enhance security in isolated locations and improve situational awareness for emergency responders.

Published in: IEEE Access, 2020

5. Title: GPS-Based Real-Time Surveillance System for Remote Area Security

Authors: S. J. Parveen, P. R. Khanna, and N. Yadav

Abstract: This paper discusses a GPS-based real-time surveillance system that uses object detection models for identifying threats in remote areas. It integrates GPS technology to track locations of detected threats and send alerts via an IoT platform. The system is evaluated in various security scenarios, including forest monitoring and remote boundary surveillance, demonstrating its effectiveness in real-time applications.

Published in: International Journal of Advanced Computer Science and Applications (IJACSA), 2019

3. EXISTING SYSTEM:

Existing systems for trail or perimeter surveillance typically rely on traditional security measures such as cameras and motion detectors, which are often limited in their ability to accurately detect specific threats or provide real-time analysis. Many systems use basic object detection algorithms or human surveillance, but these approaches often lack precision and cannot differentiate between various types of objects, such as weapons or people. Moreover, conventional systems may not integrate easily with GPS or IoT technologies, limiting their ability to provide location-based alerts or remote monitoring. While some systems have attempted to use AI and deep learning for threat detection, real-time processing, object classification, and location tracking are still major challenges.

3.1 Disadvantages of Existing Systems:

- Low Detection Accuracy: Traditional systems often have low accuracy in detecting specific threats like weapons, leading to false positives or negatives.
- Lack of Real-Time Analysis: Many systems fail to process data in real time, causing delays in threat identification and response.
- Limited Object Classification: Basic systems cannot accurately classify a wide range of objects, limiting their effectiveness in security.
- No Integration with GPS: Existing systems rarely incorporate GPS to track threats and provide location-based alerts.
- Scalability Issues: These systems may not be scalable for large or remote areas, making them less effective for extensive surveillance.

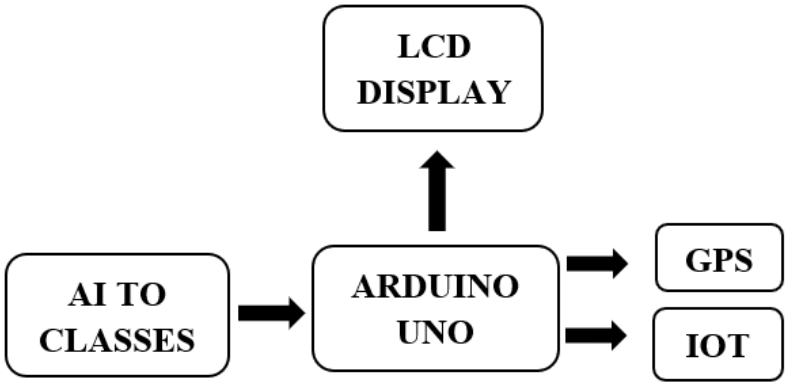
4. PROPOSED SYSTEM

The proposed CAMDEC AI System integrates deep learning-based object detection (YOLOv8) with real-time threat monitoring, GPS location tracking, and IoT for remote alerting. This system is designed to detect various objects, such as weapons (Knife, Machete, Pistol, Rifle, etc.) and suspicious individuals, using a camera and the YOLOv8 model trained on a custom dataset. The detection model is deployed on Arduino Uno, where real-time object detection data is displayed on an LCD. When a threat is identified, the GPS coordinates are captured and the information is sent to an IoT platform for immediate alerts. This combination of AI, GPS, and IoT provides robust monitoring, making it ideal for securing remote or sensitive areas such as trails or borders.

4.1 Advantages of Proposed System:

- High Detection Accuracy: YOLOv8 provides fast and accurate object classification, ensuring precise identification of threats.
- Real-Time Monitoring: The system processes data in real time, enabling immediate threat detection and alerting.
- Location Tracking: GPS integration allows the system to track and report the exact location of detected threats.
- IoT Integration: Sends alerts to an IoT platform for instant remote monitoring and response.
- Scalable and Flexible: The system is scalable for different environments, offering adaptable security solutions for various applications.

5. BLOCK DIAGRAM



6. SYSTEM SPECIFICATION:

6.1 HARDWARE REQUIREMENT:

- ARDUINO UNO
- LCD
- GPS
- IOT

SOFTWARE REQUIREMENT:

- ARDUINO IDE
- ANDROID STUDIOS
- AI AND YOLOv8

7. BLOCK DIAGRAM DESCRIPTION

HARDWARE REQUIREMENTS:

7.1 Arduino Uno:

Arduino/Genuino Uno is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. You can't tinker with your UNO without worrying too much about doing something wrong, worst-case scenario, you can replace the chip for a few dollars and start over again.

Figure 1.1: Arduino Uno board

TECHNICAL SPECS

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P) of which 0.5 KB is used by the bootloader
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
Length	68.6 mm
Width	53.4 mm
Weight	25 g

An Arduino board consists of an Atmel 8-bit AVR microcontroller with complementary components to facilitate programming and incorporation into other circuits. An important aspect of the Arduino is the standard way that connectors are exposed, allowing the CPU board to be connected to a variety of interchangeable add-on modules known as shields. Some shields communicate with the Arduino board directly over various pins, but many shields are individually addressable via an I²Cserial bus, allowing many shields to be stacked and used in parallel. Official Arduinos have used the megaAVR series of chips, specifically the ATmega8, ATmega168, ATmega328, ATmega1280, and ATmega2560. A handful of other processors have been used by Arduino compatibles. Most boards include a 5-volt linear regulator and a 16 MHz crystal oscillator (or ceramic resonator in some variants), although some designs, such as the LilyPad, run at 8 MHz and dispense with the onboard voltage regulator due to specific form-factor restrictions. An Arduino's microcontroller is also pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory, compared with other devices that typically need an external programmer.

At a conceptual level, when using the Arduino software stack, all boards are programmed over an RS-232 serial connection, but the way this is implemented varies by hardware version. Serial Arduino boards contain a level shifter circuit to convert between RS-232-level and TTL-level signals. Current Arduino boards are programmed via USB, implemented using USB-to-serial adapter chips such as the FTDI FT232. Some variants, such as the Arduino Mini and the unofficial Boarduino, use a detachable USB-to-serial adapter board or cable, Bluetooth, or other methods. (When used with traditional microcontroller tools instead of the Arduino IDE, standard AVR ISP programming is used.)

POWER SOURCE:

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically. External (non-USB) power can come either from an AC to-DC adapter (wall-wart) or battery. The adapter can be connected by plugging a 2.1mm center-positive plug into the board's power jack. Leads from a battery can be inserted into the Gnd and Vin pin headers of the POWER connector. The board can operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts, and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

7.2 LCD DISPLAY:

Figure 1.5: Liquid Crystal Display (LCD)

A **liquid crystal display** (**LCD**) is a thin, flat electronic visual display that uses the light-modulating properties of liquid crystals (LCs). LCs do not emit light directly.

7.3 GLOBAL POSITIONING SYSTEM (GPS)

Of all the applications of GPS, vehicle tracking and navigational systems have brought this technology to the day-to-day life of the common man. Today, GPS fitted cars; ambulances, fleets and police vehicles are common sights on the roads of developed countries. Known by many names such as Automatic Vehicle Locating System (AVLS), Vehicle Tracking and Information System (VTIS), Mobile Asset Management System (MAMS), these systems offer an effective tool for improving the operational efficiency and utilization of vehicles.

The switching off of SA has improved the accuracy of GPS to better than 30 meters, which makes it an ideal position sensor for vehicle tracking systems without the overhead of DGPS. Fig. 1 gives the block diagram of a DGPS based VTIS.

GPS is used in vehicles for both tracking and navigation. Tracking systems enable a base station to keep track of the vehicles without the intervention of the driver where, as navigation system helps the driver to reach the destination. Whether navigation system or tracking system, the architecture is more or less similar. The navigation system will have convenient, usually a graphic, display for the driver which is not needed for a tracking system. Vehicle Tracking Systems combine several well-developed technologies. Irrespective of the technology being used, VTS consists of three subsystems: a) In-vehicle unit (IVU), b) Base station, and c) Communication link. The IVU includes a suitable position sensor and an intelligent controller, together with an appropriate interface to the communication link. Thanks to the US Government announcement of 911E regulation, radio-based position technology has witnessed a spurt of developmental activities.

7.4 INTERNET OF THINGS (IOT)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data.
IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally *dumb* or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. With the arrival of driverless vehicles, a branch of IoT, i.e. the Internet of Vehicle starts to gain more attention.
The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994, Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.
The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet for things". At that point, he viewed Radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.
A research article mentioning the Internet of things was submitted to the conference for Nordic Researchers in Logistics, Norway, in June 2002, which was preceded by an article published in Finnish in January 2002.The implementation described there was developed by Kary Främling and his team at Helsinki University of Technology and more closely matches the modern one, i.e. an information system infrastructure for implementing smart, connected objects.
Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.

8. Software Requirements

8.1 arduino ide:

ARDUINO SOFTWARE (IDE)

- Writing Sketches
  - File
  - Edit
  - Sketch
  - Tools
  - Help
- Sketchbook
- Tabs, Multiple Files, and Compilation
- Uploading
- Libraries
- Third-Party Hardware
- Serial Monitor
- Preferences
- Language Support
- Boards

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

Writing Sketches

Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.

8.2 ANDROID STUDIO:

Android Studio is a windowed environment. To make the best use of limited screen real-estate, and to keep you from being overwhelmed, Android Studio displays only a small fraction of the available windows at any given time. Some of these windows are context-sensitive and appear only when the context is appropriate, while others remain hidden until you decide to
show them, or conversely remain visible until you decide to hide them. To take full advantage of Android Studio, you need to understand the functions of these windows, as well as how and when to display them. In this chapter, we're going to show you how to manage the windows within Android Studio.
One of the essential functions of any integrated development environment (IDE) is navigation. Android projects are typically composed of many packages, directories, and files, and an Android project of even modest complexity can contain hundreds of such assets. Your productivity with Android Studio will depend in large measure on how comfortable you are navigating within these assets and across them.

8.3 INTRODUCTION TO YOLOV8

YOLO (You Only Look Once) is a family of real-time object detection models that detect and classify multiple objects in a single forward pass of the neural network. YOLOv8 is the latest and most advanced version released by Ultralytics and offers several improvements over previous versions such as YOLOv5, YOLOv6 and YOLOv7.
YOLOv8 is designed for high performance, ease of use and fast deployment in real-time applications. It supports tasks like object detection, image segmentation, pose estimation and classification. In the context of CAMDEC AI System, YOLOv8 is used for object detection to identify potential threats such as weapons and persons.

9. ADVANTAGES:

- Real-Time Threat Detection
- High Accuracy with YOLOv8 Model
- Automatic GPS Location Tracking
- Instant IoT-Based Alert System
- Efficient Surveillance in Remote Areas
- Cost-Effective and Scalable Solution
- Integrated Display and Monitoring via LCD and Arduino

10. APPLICATIONS:

- Forest Trail and Wildlife Reserve Surveillance
- Border Security and Intruder Detection
- Smart Campus and Institutional Safety Monitoring
- Remote Area Military Surveillance Systems
- Railway and Highway Security Monitoring

11. FUTURE ENRICHMENT:

The current implementation of the **CAMDEC AI System using YOLOv8 with Real-Time Threat Monitoring via IoT and GPS** is a significant step toward automated, intelligent forest surveillance. However, as technology continues to evolve and the needs of forest conservation expand, there is great potential to enhance and enrich the system in future iterations.
The following are proposed areas for future development:

11.1 SMART VISION IN THE DARK: INTEGRATING THERMAL AND NIGHT VISION CAMERAS
11.2 FROM DETECTION TO UNDERSTANDING: AI-POWERED BEHAVIORAL INTELLIGENCE
11.3 EYES IN THE SKY: DRONE-BASED AERIAL PATROLLING
11.4 POWERING THE WILD: SOLAR-DRIVEN SELF-SUSTAINING SURVEILLANCE UNITS
11.5 CONNECTED INTELLIGENCE: CENTRALIZED CLOUD DASHBOARD AND PREDICTIVE ANALYTICS

The CAMDEC AI System lays a strong foundation for AI-driven forest security. Through these future enrichments—ranging from sensor upgrades and drone integration to behavioral AI and sustainable energy use—the system can evolve into a highly intelligent, scalable, and ethical conservation tool. These advancements will not only strengthen forest surveillance but also contribute to building safer, more resilient natural ecosystems for generations to come.
The proposed enhancements to the CAMDEC AI System represent a visionary step toward creating a smarter, more resilient forest surveillance infrastructure. By integrating advanced technologies such as thermal imaging, behavioral intelligence, drone-based monitoring, solar-powered autonomy

and centralized data analytics, the system can evolve from a basic threat detection tool into a fully autonomous and predictive security network. These enrichments not only improve detection accuracy and response time but also extend the system's operational range, environmental adaptability, and strategic value.

As environmental threats become more complex and widespread, the future of conservation depends on intelligent, adaptive technologies that can operate efficiently in challenging conditions. The proposed advancements align with this vision and offer a sustainable, scalable solution for protecting our forests, wildlife, and natural resources. With continuous innovation and real-world deployment, this system has the potential to become a benchmark for AI-driven environmental security worldwide.

12. CONCLUSION:

In conclusion, the CAMDEC AI system effectively combines deep learning with hardware integration to deliver a powerful and real-time threat detection solution. By utilizing the YOLOv8 object detection algorithm, the system can accurately identify and classify dangerous objects such as knives, pistols, rifles, and rods, along with detecting the presence of individuals in restricted or sensitive areas. This software component is trained on a custom dataset using Roboflow and Google Colaboratory, resulting in a robust model capable of functioning in real-world scenarios.

On the hardware side, components like Arduino Uno, GPS module, LCD display, and IoT connectivity work in unison to support real-time monitoring and alert systems. When a weapon is detected, the system immediately fetches the GPS location and sends an alert to the designated platform, ensuring rapid response and preventive measures. The LCD display provides local information for on-site personnel.

This integrated solution not only enhances surveillance but also reduces the reliance on constant human monitoring in remote and high-risk zones like forest trails, border areas, and protected zones. The system's adaptability, accuracy, and scalability make it a valuable contribution to modern security infrastructures, promoting safety through innovation and smart automation.

13. REFERENCES:

1. *"You Only Look Once: Unified, Real-Time Object Detection"* by Joseph Redmon et al., published in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.
2. *"YOLOv4: Optimal Speed and Accuracy of Object Detection"* by Alexey Bochkovskiy et al., published on arXiv preprint, 2020.
3. *"YOLOv5 by Ultralytics: A Scalable Object Detection Model for Real-Time Applications"* by Glenn Jocher, published on GitHub/Ultralytics, 2020.
4. *"YOLOv8: Ultralytics Next-Generation Real-Time Object Detection Model"* by Ultralytics Team, published on Ultralytics Documentation, 2023.
5. *"Deep Learning for Visual Object Detection: A Comparative Review"* by Q. Liu et al., published in IEEE Access, 2020.
6. *"Real-Time Object Detection System for Security Surveillance Using Deep Learning"* by R. Sharma and K. Patel, published in International Journal of Computer Applications, 2019.
7. *"IoT-Based Smart Surveillance and Alert System for Real-Time Monitoring"* by S. S. Jadhav and P. S. Patil, published in International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), 2021.
8. *"GPS and IoT Based Real-Time Vehicle and Object Tracking System"* by V. R. Priya et al., published in International Journal of Engineering Research & Technology (IJERT), 2020.
9. *"Weapons Detection in CCTV Surveillance Using Deep Learning"* by A. S. Naik and N. S. Kulkarni, published in IEEE International Conference on Smart Technologies and Management, 2019.
10. *"Artificial Intelligence and IoT in Modern Security Systems: A Review"* by M. Kumar and R. Singh, published in Journal of Information Technology & Software Engineering, 2022.
11. Nair, M. M., Deshmukh, A., & Tyagi, A. (2023).
    "Artificial Intelligence for Cyber Security: Current Trends and Future Challenges."
    This chapter discusses the current trends in applying AI to cybersecurity, addressing challenges and proposing future research directions to enhance security measures in various domains, including IoT.
12. Baral, S., Saha, S., & Haque, A. (2024).
    "An Adaptive End-to-End IoT Security Framework Using Explainable AI and LLMs."
    This study presents a comprehensive framework for real-time IoT attack detection and response, leveraging Machine Learning (ML), Explainable AI (XAI), and Large Language Models (LLMs). The integration of XAI techniques like SHAP and LIME ensures adaptability across various ML algorithms, enhancing the interpretability and accessibility of detection decisions.
13. Esmaeili, M., Rahimi, M., Pishdast, H., Farahmandazad, D., Khajavi, M., & Saray, H. J. (2024).

"Machine Learning-Assisted Intrusion Detection for Enhancing Internet of Things Security."
This paper investigates machine learning-based intrusion detection strategies for IoT security, focusing on real-time responsiveness, detection accuracy, and algorithm efficiency. It provides a taxonomy of existing approaches and outlines limitations of current IoT security frameworks.

14. Kumar, P. J., & Nedunchelіyan, S. (2024).
"A Novel Optimized Deep Learning Based Intrusion Detection Framework for IoT Networks."
This study proposes an optimized deep learning framework for intrusion detection in IoT networks, aiming to enhance detection accuracy and reduce false positives, thereby improving overall network security.

15. Aung, Y. L., Christian, I., Dong, Y., Ye, X., Chattopadhyay, S., & Zhou, J. (2025).
"Generative AI for Internet of Things Security: Challenges and Opportunities."
This paper explores the integration of Generative AI (GenAI) into IoT security, examining current implementations, potential benefits and research gaps. It provides case studies and discusses the effectiveness of GenAI in addressing prevailing challenges within IoT security.