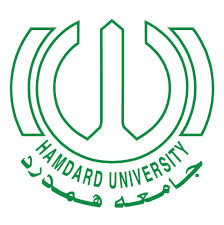
Hamdard University

Department of Computing

Final Year Project



**< INTEGRA GUARD SURVEILLANCE SYSTEM >**

**(<**FYP-022/FL24 **>)**

**Software Design Specifications**

Submitted by

Zainab Khalid (2326-2021)

Nida Aamir (2458-2021)

Supervisor

Mr.Afzal Hussain

Mr.Mustafa Ali

**Fall 2021**

**Document Sign off Sheet**

### Document Information

|  |  |
| --- | --- |
| **Project Title** | **INTEGRA GUARD SURVEILLANCE SYSTEM** |
| **Project Code** | FYP-022/FL24 |
| **Document Name** | Software Design Specifications |
| **Document Version** | <1.0> |
| **Document Identifier** | < FYP-022/FL24 >-SDS |
| **Document Status** | Final / |
| **Author(s)** | Zainab Khalid, Nida Aamir |
| **Approver(s)** | Afzal Hussain |
| **Issue Date** | 28-12-24 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Signature** | **Date** |
| Zainab Khalid | Team Lead |  | 24-12-24 |
| Nida Aamir | Team Member 2 |  | 24-12-24 |
| Mr.Afzal Hussain | Supervisor | Afzal Hussain | 28-12-24 |
| Mr.Mustafa Ali | Co-Supervisor | Mustafa Ali | 28-12-24 |
| Mr.Sulaiman Khan | Project Coordinator |  |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 5-11-2024 | 0.1 | First draft | Nida |
| 8-11-2024 | 0.2 | Received Version | Zainab |
|  |  |  |  |
|  |  |  |  |

**Definition of Terms, Acronyms, and Abbreviations**

*[This section should provide the definitions of all terms, acronyms, and abbreviations required to interpret the terms used in the document properly.]*

|  |  |
| --- | --- |
| **Term** | **Description** |
| ATM | Automated Teller Machine; enables banking transactions without human assistance. |
| AI | Artificial Intelligence; simulates human intelligence in machines. |
| CCTV | Closed-Circuit Television; used for real-time video surveillance. |
| UI | User Interface; the part of the system users interact with (e.g., dashboard) |
| Cloud Analysis | Uses cloud-based AI to analyze behavior patterns and enhance detection. |

# Table of Contents

[1.1.1 Document Information 2](#_Toc202716287)

[Table of Contents 4](#_Toc202716288)

[1 Introduction: 5](#_Toc202716289)

[1.1 Purpose of Document 5](#_Toc202716290)

[1.2 Intended Audience 5](#_Toc202716291)

[1.3 Document Convention 5](#_Toc202716292)

[1.4 Project Overview 5](#_Toc202716293)

[1.5 Scope 6](#_Toc202716294)

[1.6 Not in Scope 6](#_Toc202716295)

[2 System Level Architecture 6](#_Toc202716296)

[2.1 System Decomposition 6](#_Toc202716297)

[2.2 Element Relationships 7](#_Toc202716298)

[2.3 External Interfaces 7](#_Toc202716299)

[3 Software Architecture 8](#_Toc202716300)

[3.1 User Interface (UI) Layer 8](#_Toc202716301)

[3.2 Application Layer (Middle Tier) 8](#_Toc202716302)

[3.3 Data Access Layer (DAL) 9](#_Toc202716303)

[3.4 2.4.4 Database Layer 9](#_Toc202716304)

[4 Detailed System Design 12](#_Toc202716305)

[4.1 ER Diagram 13](#_Toc202716306)

[ USER 14](#_Toc202716307)

[ CAMERA 14](#_Toc202716308)

[ DETECTION 14](#_Toc202716309)

[ NOTIFICATION 14](#_Toc202716310)

[5 Application Design 14](#_Toc202716311)

[5.1 Sequence Diagram 14](#_Toc202716312)

[5.1.1 User: 15](#_Toc202716313)

[5.1.2 CCTV Camera: 15](#_Toc202716314)

[5.1.3 AI Detection System: 15](#_Toc202716315)

[5.1.4 Dashboard Admin: 15](#_Toc202716316)

[5.1.5 Security Personnel: 15](#_Toc202716317)

[5.1.6 Database: 15](#_Toc202716318)

[5.2 State Diagram 16](#_Toc202716319)

[References 17](#_Toc202716320)

# Introduction:

The Integra Guard Surveillance System is a comprehensive solution to address security challenges in ATM environments. The system focuses on identifying weapons and suspicious behaviors to improve user safety and secure financial transactions by utilizing cutting-edge technologies like real-time video analysis and AI-powered detection. The system is built to proactively mitigate threats while guaranteeing regulatory compliance thanks to its intuitive interface, strong detection algorithms, and smooth integration capabilities. Rapid notification systems, encrypted data storage, and scalability to accommodate an increasing number of ATM installations are important features.

## Purpose of Document

The Integra Guard Surveillance System was created using evolutionary prototyping, and this Software Requirements Specification (SRS) document offers comprehensive insights into its architecture, design considerations, and functionality. The technical requirements and specifications required for successful implementation are outlined in this document, which acts as a blueprint for the development team

## Intended Audience

* Development Team: Engineers and developers in charge of system design, implementation, and testing.
* Security analysts are experts who use the system's results to improve ATM surveillance.
* Project managers are in charge of the planning, carrying out, and completing phases of a project.
* Stakeholders: Anybody with an interest in the system's functionality and security, such as banks, law enforcement, and regulatory organizations.

## Document Convention

This document follows a consistent formatting style to ensure clarity and readability. All content is written using the ***Times New Roman*** font with a ***font size of 12 points***. Headings are bolded and appropriately numbered to reflect the structure of the report. Standard paragraph spacing and justified alignment are maintained throughout the document for a clean and professional appearance

## Project Overview

The project aims to develop an advanced Weapon Detection System specifically designed for ATM surveillance environments, focusing on identifying harmful weapons, such as pistols, in real-time using CCTV footage.

The system is tailored to operate efficiently in confined spaces and handle challenges such as varying camera angles, partial occlusions, and similar-looking objects that may cause false alerts. By integrating automated detection with real-time alert mechanisms, the system enhances response times and reduces reliance on manual supervision.

## Scope

The system will include functionalities for:

1. Real-time Surveillance:  
   AI-enabled cameras detect and record weapons, ensuring accurate monitoring with minimal false positives.
2. Cloud Analysis:  
   Machine learning analyzes behavior patterns and flags suspicious activity for proactive intervention.
3. Centralized Database:  
   Secure, encrypted cloud storage for managing recorded data and generating detailed reports.
4. Alerts:  
   Instant notifications via SMS, email, or mobile apps to authorized personnel for quick response.
5. Privacy and Compliance:  
   Safeguards anonymize non-essential data and ensure regulatory compliance for banking environments.
6. Integration and Scalability:  
   Seamlessly integrates with bank systems, supports multiple ATMs, and ensures low-latency performance.

## Not in Scope

1. Monitoring of private, non-ATM spaces.
2. Detection of fully concealed weapons.
3. Replacing manual audits or law enforcement investigations.
4. Detection of concealed or hidden weapons.
5. Facial expression or emotion recognition.Advanced AI features such as anomaly detection, audio threat detection

# System Level Architecture

## System Decomposition

The system is divided into the following subsystems:

**2.1.1 Suspicious Activity Detection Module**

* + Utilizes AI-based algorithms to analyze CCTV feeds for revealed weapons and anomalous facial expressions or behaviors.
  + Generates alerts when suspicious activity is detected.

**2.1.2 Surveillance Monitoring Unit**

* Provides monitoring personnel with a real-time dashboard to view alerts and live CCTV feeds.
* Facilitates user interaction for escalating confirmed threats to security teams.

**2.1.3 Notification System**

* Handles the dissemination of alerts to appropriate parties, including monitoring personnel and security teams.
* Supports real-time notifications via dashboard updates and external messaging systems.

## Element Relationships

* Subsystems communicate through defined interfaces to ensure seamless data flow:
  + The Detection Module sends alerts to the Monitoring Unit, including timestamps, video snapshots, and analysis details.
  + The Monitoring Unit processes user input to escalate verified threats, triggering the Notification System to alert security personnel.
  + Logged events are shared with the Data Storage Unit for future analysis and reporting.

## External Interfaces

**2.3.1 CCTV Cameras**: Provide live video feeds for the Detection Module to analyze.

**2.3.2 ATM Sensors**: Supplement video feeds with contextual data (e.g., motion detection).

**2.3.3 Remote Notification Services**: Send alerts to mobile devices or external systems for security personnel.

**2.3.4 Database**: Stores event logs, user actions, and configuration data.

**2.3.5 Execution Locations**

* + - **Back-End Processing**:  
      AI analysis and data processing are performed on dedicated servers to ensure high performance and reliability.
    - **Cloud Environment**:  
      Stores surveillance data, configuration files, and historical logs for scalability and accessibility.
    - **User Devices**:  
      Hosts the web-based dashboard for monitoring personnel.

**2.3.6 Global Design Strategies**

* + - **Error Handling Mechanisms**:
      * Retry logic ensures system resilience against transient network issues.
      * Fallback mechanisms address potential malfunctions in cameras or sensors.
    - **Security Measures**:
      * Secure communication channels (e.g., HTTPS, secure APIs) protect data integrity and privacy.
      * Role-based access controls safeguard sensitive system functionalities.

# Software Architecture

The software architecture for the Integraguard Surveillance System outlines the interaction between various layers of the system, ensuring a structured, scalable, and efficient design.

## User Interface (UI) Layer

* **Role**:  
  Serves as the primary interaction point for users, including monitoring personnel and administrators.
* **Functionality**:
  + Provides a web-based dashboard for real-time monitoring of ATM CCTV feeds.
  + Displays real-time alerts for detected weapons and suspicious behaviors.
  + Offers controls for triggering alarms and escalating alerts to security personnel.
  + Enables users to review historical logs and generate reports.

## Application Layer (Middle Tier)

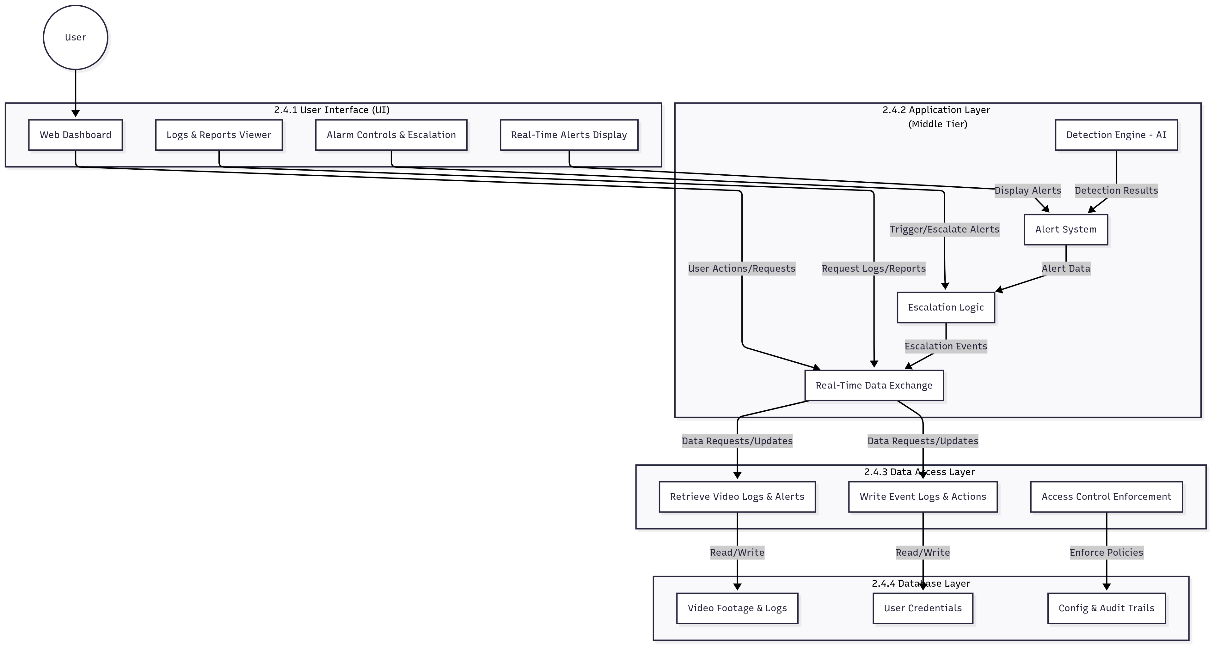
* **Role**:  
  Processes user actions, applies business logic, and facilitates communication between layers.
* **Functionality**:
  + **Detection Engine**: Uses AI algorithms to analyze video feeds for weapons and anomalies.
  + **Alert System**: Triggers notifications for detected suspicious activity.
  + **Escalation Logic**: Allows confirmation and escalation of threats to security teams.
  + Manages real-time data exchange between the UI and Data Access Layer.

## Data Access Layer (DAL)

* **Role**:  
  Bridges the Application Layer and the Database, ensuring secure and efficient transactions.
* **Functionality**:
  + Retrieves video logs, stored alerts, and configuration data.
  + Writes logs of suspicious events, user actions, and escalation records.
  + Enforces access controls on sensitive surveillance data.

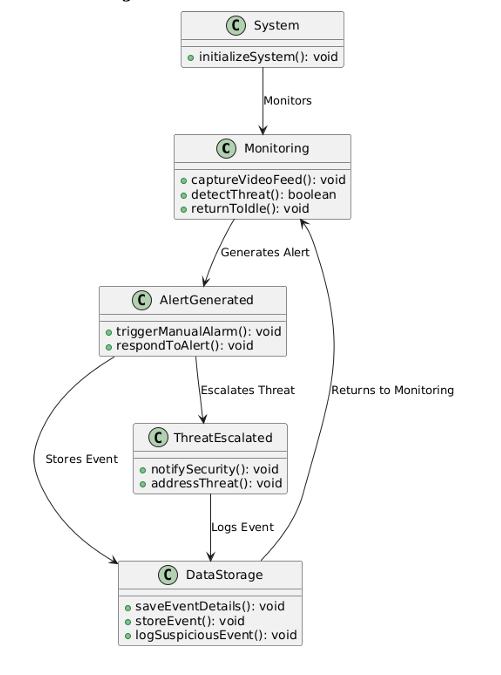
## 2.4.4 Database Layer

* **Role**:  
  Provides persistent storage for all core system data.
* **Functionality**:
  + Stores video footage, timestamps, logs, and user credentials.
  + Maintains system configuration settings and audit trails.
  + Supports querying for report generation and historical analysis.



*SYSTEM ARCHITECTURE DIAGRAM*

**3. Class Diagram**

****

**3.1 System**

* Starts the weapon detection system using the initializeSystem() function.

**3.2 Monitoring**

* Continuously watches the environment by:
  + Capturing video: captureVideoFeed()
  + Detecting threats: detectThreat()
  + Returning to normal if no threat is found: returnToIdle()

**3.3 Alert Generated**

* When a threat is detected, an alert is created.
* Functions include:
  + Manually triggering an alarm: triggerManualAlarm()
  + Responding to the detected alert: respondToAlert()

**3.4 Threat Escalated**

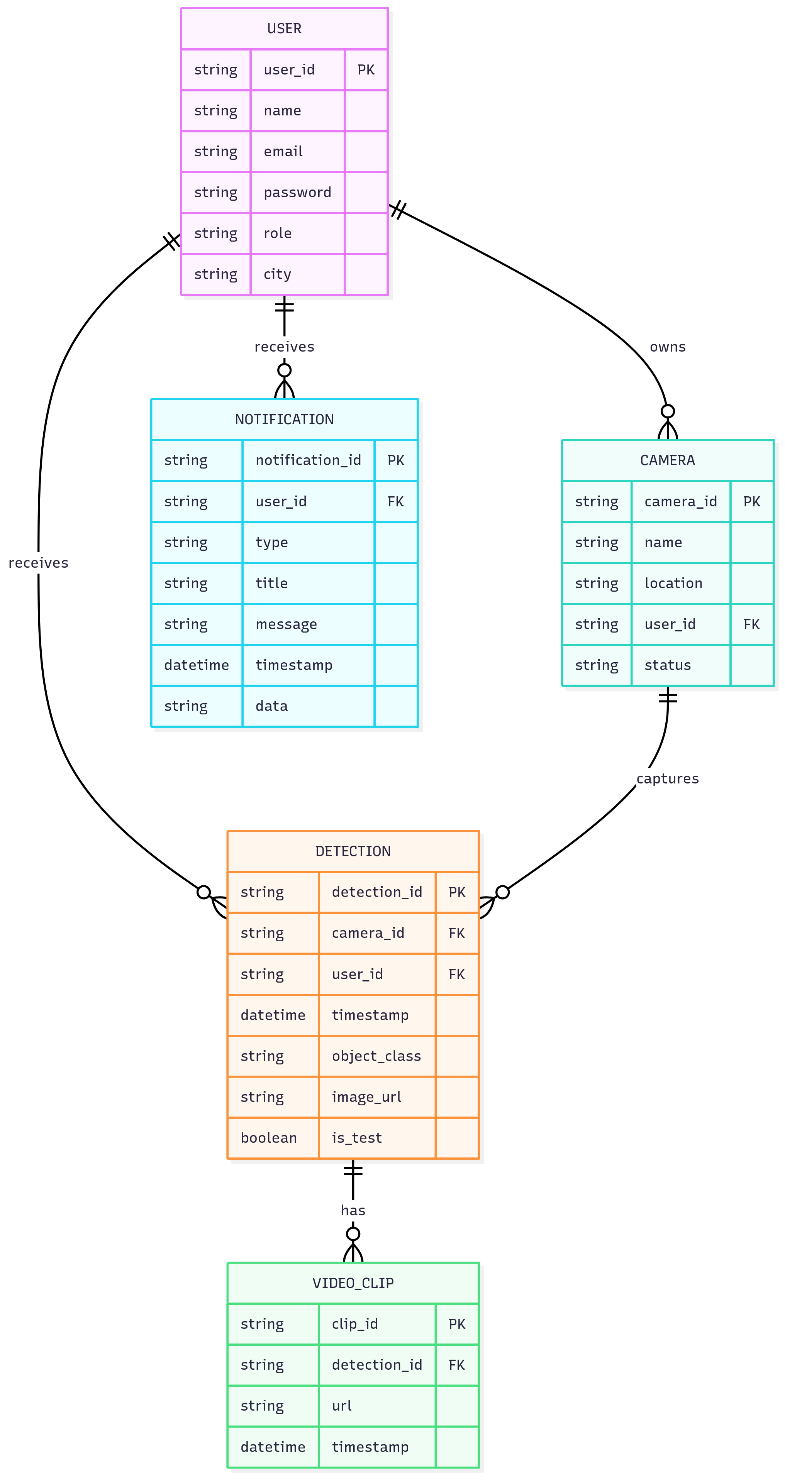
* If the threat is serious, it is escalated.
* The following actions are taken:
  + Notify security: notifySecurity()
  + Address the threat: addressThreat()

**3.5 DataStorage**

* Stores all event data for records and analysis.
* Core functions:
  + Save event details: saveEventDetails()
  + Log suspicious events: logSuspiciousEvent()
  + Store events: storeEvent()

# Detailed System Design

## ER Diagram



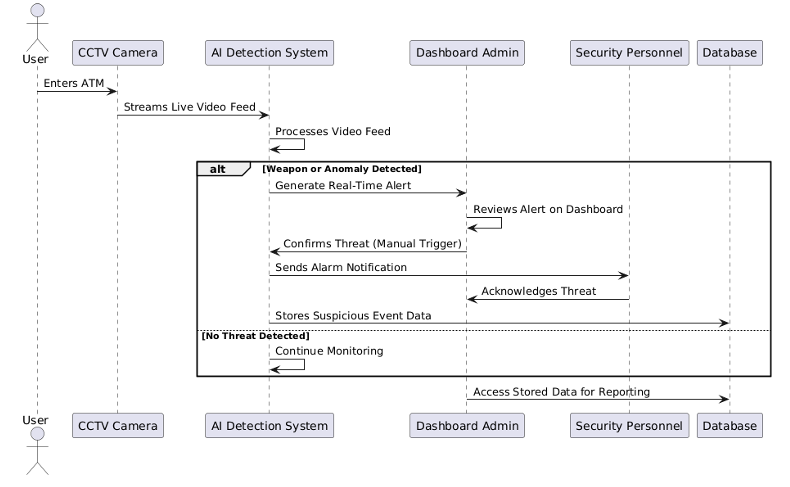
* USER: Represents system users (monitoring personnel, admins, etc.).
* CAMERA: Each camera is registered to a user.
* DETECTION: Each detection event is linked to a camera and a user.
* NOTIFICATION: Notifications are sent to users about detections or system events.

**Relationships:**

* A user can own multiple cameras.
* A user can receive multiple detections and notifications.
* A camera can capture multiple detections.
* Each detection can have multiple associated video clips.

# Application Design

## Sequence Diagram

****

### User:

* + Represents an individual using the ATM.

### CCTV Camera:

* + Captures the live video feed and streams it to the AI system.

### AI Detection System:

* + Processes the video feed to detect weapons
  + Decides if an alert should be generated.

### Dashboard Admin:

* + Monitors alerts on the web interface dashboard.
  + Confirms if an alert should escalate into a threat.

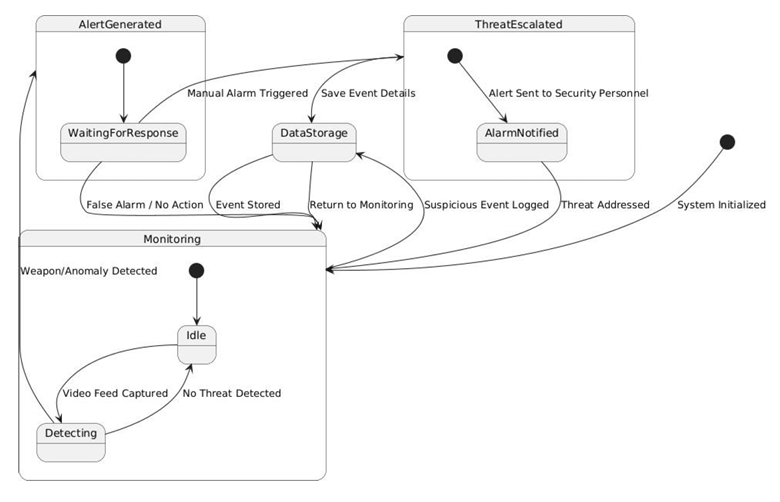
### Security Personnel:

* + Receives escalated alerts and responds accordingly.

### Database:

* + Stores event details for future reference and reporting.

## State Diagram

****

# References

[1] Ahmed, S., Bhatti, M. T., Khan, M. G., Lövström, B., & Shahid, M. (2022). Development and optimization of deep learning models for weapon detection in surveillance videos. Applied Sciences, 12(12), 5772. <https://doi.org/10.3390/app12125772>

[2] Abins, A. A., P, P., G C, R., & Cheran, R. (2024). Weapon Recognition in CCTV Videos: Deep Learning Solutions for Rapid Threat Identification. In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE) (pp. 1–8). 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE). IEEE. <https://doi.org/10.1109/ic-etite58242.2024.10493569>

[3] Wang, G., Ding, H., Duan, M., Pu, Y., Yang, Z., & Li, H. (2023). Fighting against terrorism: A real-time CCTV autonomous weapons detection based on improved YOLO v4. Digital Signal Processing, 132, 103790. <https://doi.org/10.1016/j.dsp.2022.103790>

[4] Salazar González, J. L., Zaccaro, C., Álvarez-García, J. A., Soria Morillo, L. M., & Sancho Caparrini, F. (2020). Real-time gun detection in CCTV: An open problem. Neural Networks, 132, 297–308. <https://doi.org/10.1016/j.neunet.2020.09.013>

[5] Bamnolkar, A. K., Khakre, K. R., Gadge, A. R., Waje, M. G., Raut, V., & Khan, M. S. (2025). Cutting Edge Weapon Detection in Real-Time CCTV Videos. In 2025 10th International Conference on Signal Processing and Communication (ICSC) (pp. 345–350). 2025 10th International Conference on Signal Processing and Communication (ICSC). IEEE. <https://doi.org/10.1109/icsc64553.2025.10968883>

[6] Keerthana, S. M., Sujitha, R., & Yazhini, P. (2024). Weapon Detection For Security Using The Yolo Algorithm With Email Alert Notification. In 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET) (pp. 1–6). 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET). IEEE. <https://doi.org/10.1109/icicet59348.2024.10616365>

[7] Kumar, J. A., Dhivya, G., Selvaraj, P., Karthikeyan, V. G., Ramesh, S. P., Lakshmi, S. J., & Saravanakumar, R. (2024). Weapon Detection Identification and Classification for DCNN and YOLO-V5 Techniques. In 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS) (pp. 1317–1323). 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS). IEEE

# 