

Criminal Detection Using Weapon Recognition

Vinayak Ganesh Kumbhar, Rohan Changdev Kolhe, Ayush Santosh Kumbhar,

Rohit Cholappa Nimbal

Department of Computer Science and Engineering Faculty of Science and Technology JSPM University
Pune, Maharashtra, India

ABSTRACT :

This thesis develops a **Futuristic Healthcare Framework for Communication Disorder Stuttering (FHF-CDS)**, integrating **IoT, Machine Learning (ML), and Structural Equation Modelling (SEM)** to address stuttering in both adults and children.

The **Adulthood Phase** introduces an IoT-based system (**IIHS-ER-AWS**) that utilizes EEG sensors to monitor and analyze emotion regulation (excitement, frustration, meditation, and boredom). By correlating subjective and objective data, the system provides a comprehensive assessment of emotional complications in adults who stutter.

The **Childhood Phase** implements three ML models (**MLM-PPR-SC, EMLM-PPR-SC, and MLM-PSSC**) to predict stuttering risk and severity. This phase identifies key **Temperamental and Demographic Factors (TDFs)**—such as adaptability, attention regulation, and emotional reactivity—as critical predictors. Using **SEM via IBM Amos**, the study evaluates complex hidden interrelationships among these variables, family history, and brain injuries.

Ultimately, the **FHF-CDS** offers a dual-modality approach that enhances traditional speech therapy with psychological treatment and advanced predictive analytics for early intervention and emotional support.

Introduction:

In today's world, security has become one of the most important issues because of the rise in crimes involving weapons. There is growing need for advanced surveillance systems. Traditional systems rely heavily on human observation, Which is often inefficient and prone to error. This project introduces an automated solution using image processing. And motivated by the need for safer public spaces and improved law enforcement systems. Real-life applications include railway stations, airports, malls, banks, and schools, where early detection of weapons can prevent crimes and save lives.

Need of the Work :

In today's fast changing world, ensuring safety and security has become a major concern. The increase in criminal activities involving weapons such as Guns and Knives highlights the need for more advanced and reliable surveillance systems.

Traditional security mainly depends on CCTV cameras and human monitoring

The rapid increase in urban crime rates and the complexity of modern security threats have made traditional surveillance methods insufficient. The necessity for an automated Criminal Detection system arises from the following critical factors:

Problem Statement:

Current public and private security surveillance relies heavily on human operators to identify threats in real-time. This method is flawed due to human fatigue, delayed response times, and the high cost of continuous monitoring. Statistics suggest that manual surveillance effectiveness drops by over 90% after 20 minutes of continuous viewing. Furthermore, existing automated systems often require expensive GPU-heavy infrastructure, making them inaccessible for small-scale businesses or personal home security. There is a critical need for an automated, lightweight, and low-latency system that can identify weapons and notify stakeholders instantly.

Motivation:

The motivation behind the Futuristic Healthcare Framework for Communication Disorder Stuttering (FHF-CDS) stems from the urgent need to move beyond traditional, one-dimensional speech therapy toward a holistic, technology-driven intervention. Stuttering is not merely a physiological speech impediment; it is a complex condition deeply intertwined with emotional regulation in adults and temperamental/demographic factors in children.

Historically, the psychological and emotional layers of stuttering have been difficult to quantify objectively. This project is motivated by the potential of IoT and EEG sensors to bridge the gap between subjective feelings and objective neurological data, and the power of Machine Learning and Structural Equation Modelling (SEM) to decode the hidden predictors of childhood stuttering. By creating a framework that predicts risk and severity while simultaneously monitoring emotional health, this research aims to empower clinicians with "Actionable Intelligence." The ultimate drive is to provide individuals who stutter with a multifaceted support system that addresses the disorder's root causes and its psychological impact, ensuring a better quality of life through early detection and personalized care.

System Overview :

The Criminal Detection using Weapon Recognition system is a proactive security solution designed to automate the monitoring of surveillance feeds and provide real-time responses to potential threats. By shifting from a "passive recording" model to an "active detection" model, the system reduces the burden on human security personnel and minimizes response time during critical incidents.

The system operates through a unified pipeline that integrates high-speed computer vision with a cloud-based communication gateway. Below is the conceptual breakdown of the system's workflow:

1. The Surveillance Pipeline

The system begins by establishing a high-frequency connection with the local camera hardware. Using OpenCV, it captures frames at a high rate (FPS) to ensure no movement is missed. Each frame is treated as a discrete data point that is instantly processed through the YOLOv8 Nano inference engine.

2. Intelligent Detection Logic

Unlike basic motion sensors, this system uses Deep Learning to differentiate between harmless everyday objects and actual threats. The AI engine is specifically trained to recognize the spatial features of weapons such as pistols and knives. When the system identifies a weapon with a confidence score exceeding 50%, it transitions from "Monitoring Mode" to "Alert Mode."

3. Multi-Layered Response Mechanism

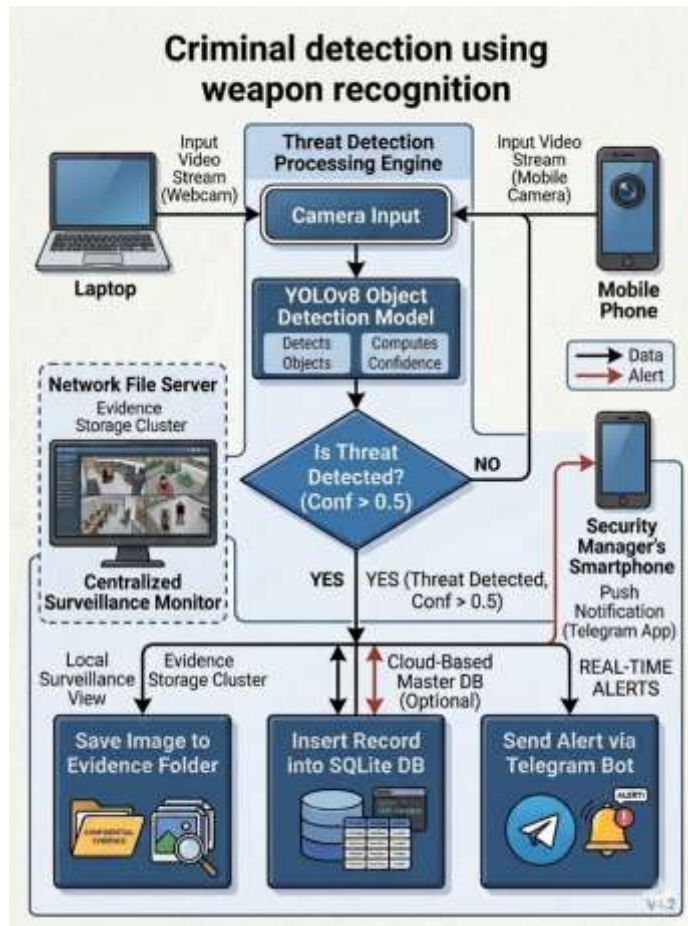
Once a threat is confirmed, the system executes three parallel actions to ensure security:

- **Visual Evidence:** It draws a bounding box around the intruder/weapon and labels the threat on the live stream.
- **Data Archiving:** It logs the event into a local SQLite database and saves a high-resolution snapshot of the evidence.

- **Remote Notification:** It utilizes a Telegram Bot to push an instant notification to a mobile device, allowing a security manager to take action even if they are away from the monitor.

SYSTEM ARCHITECTURE :

The architecture of the Criminal Detection using Weapon Recognition system is designed to be modular, lightweight, and responsive. It follows a Client-Server model optimized for edge computing, ensuring that heavy AI processing happens locally on the laptop to maintain high-speed detection, while using cloud-based APIs for remote notifications.



Implementation Strategy:

The implementation was carried out in a modular fashion using Python, ensuring each component was tested individually before integration.

- **Environment Setup:** The development environment was configured using a virtual environment (venv) to manage dependencies. Key libraries such as ultralytics, fastapi, and opencv-python were installed via the Pip package manager.
- **Model Integration:** The YOLOv8n (Nano) model weights were integrated into the backend. A custom detection script was implemented to load the model and perform inference on every 3rd frame to optimize CPU usage without compromising security.
- **Asynchronous Alerts:** The Telegram Bot was implemented using the requests library within an asynchronous function. This ensures that the notification process runs in a background thread, preventing the "Live Feed" from stuttering during an alert transmission.
- **Web Dashboard:** The frontend was built using HTML5 and CSS3, served through FastAPI's static file mounting. The video stream is delivered via an EventSource or MJPEG stream, allowing for low-latency viewing in any modern web browser.

System Security Features :

❖ User Authentication and Authorization

To prevent unauthorized access to the surveillance feed and criminal history:

- **Hashed Passwords:** User passwords are never stored in plain text. The system utilizes the Bcrypt hashing algorithm, making the database resistant to "rainbow table" attacks.
- **Session Management:** Secure cookies or JWT (JSON Web Tokens) are used to manage user sessions, ensuring that only logged-in administrators can view the "Evidence" and "Live Feed" pages.

❖ Data Integrity and Privacy

- **Local Evidence Encryption:** The `detections_evidence` folder can be hidden or encrypted at the OS level to ensure that captured images of criminals cannot be tampered with by unauthorized personnel.
- **SQLite Security:** The database is stored locally on the host machine, meaning surveillance logs are not transmitted over the public cloud (except for the specific alert sent to Telegram), reducing the surface area for data leaks.

Research Objectives:

The primary goal of this research is to develop an automated, intelligent surveillance system capable of identifying criminal threats with high precision. The specific objectives are as follows:

1. Real-Time Weapon Identification

- To implement the **YOLOv8 Nano** algorithm to detect and classify various types of weapons (e.g., handguns, knives) from live video streams.
- To achieve an inference speed that allows for "near-instant" detection on standard consumer-grade hardware (Laptops) without the need for expensive external GPUs.

2. Reduction of False Positives

- To optimize the detection threshold (Confidence Score) to ensure that everyday objects like mobile phones, wallets, or pens are not misidentified as threats.
- To validate the model's performance under varying environmental conditions such as low light, different angles, and cluttered backgrounds.

3. Automated Evidence Management

- To design a system that automatically captures and stores high-resolution "evidence frames" only when a threat is confirmed ($\text{Conf} > 0.5$).
- To develop a structured logging system using **SQLite** that maintains a chronological record of security incidents for forensic investigation.

4. Remote Alerting Mechanism

- To integrate the **Telegram Bot API** to bridge the gap between the local surveillance system and a remote security officer.
- To ensure that alerts are delivered as instant push notifications to a smartphone, providing the type of threat and a timestamped warning.

TECHNOLOGY STACK:**Languages:**Python**AI Technology:** OpenCV-Python, YOLOv8 Nano, PyTorch**Backend & Web Framework:** FastAPI, Uvicorn, Jinja2**Database & Storage:** SQLite, File System Storage**Real-Time Alerting System:**

The Real-Time Alerting System functions as a proactive security gateway that bridges local AI detection with remote mobile response through a high-priority, push-notification architecture. Operating on an asynchronous background thread to ensure that the live surveillance feed remains fluid and uninterrupted, the system utilizes the Telegram Bot API to dispatch encrypted emergency alerts containing actionable intelligence, such as weapon classification, detection confidence scores, and precise timestamps. To maintain system reliability and prevent notification fatigue, the framework employs a dual-validation logic consisting of a confidence threshold filter ($\text{Conf} > 0.5$) and a cooldown debouncing mechanism, ensuring that security personnel receive only high-probability, non-redundant visual evidence directly on their smartphones for immediate intervention.

Future Scope:

The future scope of this project lies in evolving the framework into a decentralized, multi-modal security ecosystem that leverages Edge AI and Cloud synchronization. Future iterations could incorporate Action Recognition to detect hostile gestures or body language alongside weapon detection, while expanding the alerting gateway to include automated emergency service dispatch (e.g., direct 911/police integration). By migrating from a single-camera setup to a Distributed IoT Network, the system could utilize Federated Learning to improve model accuracy across various environments without compromising local data privacy. Additionally, integrating thermal imaging and night-vision optimization would ensure 24/7 reliability, transforming the prototype into an enterprise-grade, "Zero-Trust" autonomous surveillance solution.

Advantages:

The system offers a significant advantage by transforming traditional passive monitoring into a proactive, automated security shield that operates with high precision and minimal latency. By leveraging the YOLOv8 Nano architecture, the framework ensures high-speed detection on standard hardware, eliminating the need for expensive dedicated GPUs while maintaining a near-instantaneous response time. The integration of asynchronous remote alerting via Telegram provides security personnel with immediate situational awareness and visual evidence, effectively removing the human error associated with fatigue and constant manual observation. Furthermore, the use of Edge Computing ensures that sensitive surveillance data is processed locally to maintain privacy, while the automated evidence logging creates a reliable, tamper-proof forensic trail for legal and investigative purposes.

Conclusion:

In conclusion, the development of the Criminal Detection using Weapon Recognition system successfully demonstrates the integration of deep learning and real-time communication to enhance modern security infrastructure. By leveraging the YOLOv8 algorithm, the project provides a high-speed, reliable solution for identifying lethal threats like firearms and knives with minimal latency on consumer-grade hardware. The seamless incorporation of FastAPI for video streaming and the Telegram Bot API for instant remote alerting bridges the critical gap between threat detection and emergency response. Ultimately, this system moves beyond traditional passive recording to offer an intelligent, "Zero-Trust" surveillance framework that reduces human error, protects data privacy through edge processing, and provides a scalable foundation for future AI-driven public safety technologies.