Lab Session 08: Flow diagram/Architectural Diagram/ Data Flow diagram

Date of the Session: Time of the Session:2:00pm to 4:30pm

System Architecture / Data Flow Diagram Overview – Burglary Prevention System

This is an AI-based real-time burglary prevention system designed to enhance small-scale security setups. It uses a webcam or CCTV camera to monitor environments and detect suspicious behavior using a pre-trained pose/action recognition model, all executed within the browser using TensorFlow.js. When suspicious behavior is detected, an alert is triggered, and optional logging is performed**.**

Main System Components:

1. **Camera Input (CCTV / Webcam)**
- Captures live video feed
- Streams input to web-based AI model
2. **Front-end Interface (Browser UI with TensorFlow.js)**
- Receives real-time video input
- Displays live status and alerts
3. **AI Model (Teachable Machine with TensorFlow.js)**
- Classifies poses/actions as normal or suspicious
- Executes locally in the browser
4. **Detection Engine (JavaScript Logic)**
- Interprets AI predictions
- Determines if the behavior is suspicious
5. **Alert System (Audio / Notification)**
- Emits beep or visual alert
- Notifies personnel immediately
6. **Cloud Storage (Optional - Firebase / GDrive API)**
- Stores detection logs (timestamp, prediction, image)
- Useful for audit and review
7. **Dashboard / Analytics Module**
- Web dashboard to view alert history
- Visual summary of system usage, frequency of detections.

Data Flow Steps Involved:

1. Input Module (Camera + Web Interface)

- **Live Streaming:** A live video feed from a surveillance camera is continuously streamed to the user's web browser, ensuring immediate access to visual information.
- **Frame Processing:** Selected frames from the video stream are simultaneously extracted and passed to the AI model for real-time behavioral analysis, enabling prompt detection of unusual activity.
- **User Interface:** A responsive web interface allows authorized personnel to monitor the stream, configure camera settings, and receive alerts without additional software installations.

2. Behavior Detection (AI Model + Decision Logic)

- **AI Analysis:** Each captured frame is analyzed by a pre-trained AI model capable of recognizing predefined suspicious behaviors (e.g., loitering, intrusion, aggression).
- **Detection Logic**: A decision-making engine interprets model outputs to determine if the detected behavior crosses the defined threshold for suspicion.
- **Alert System:** If suspicious activity is confirmed, the system immediately triggers an audio or visual alert (e.g., siren, voice warning) to deter potential threats or notify staff.

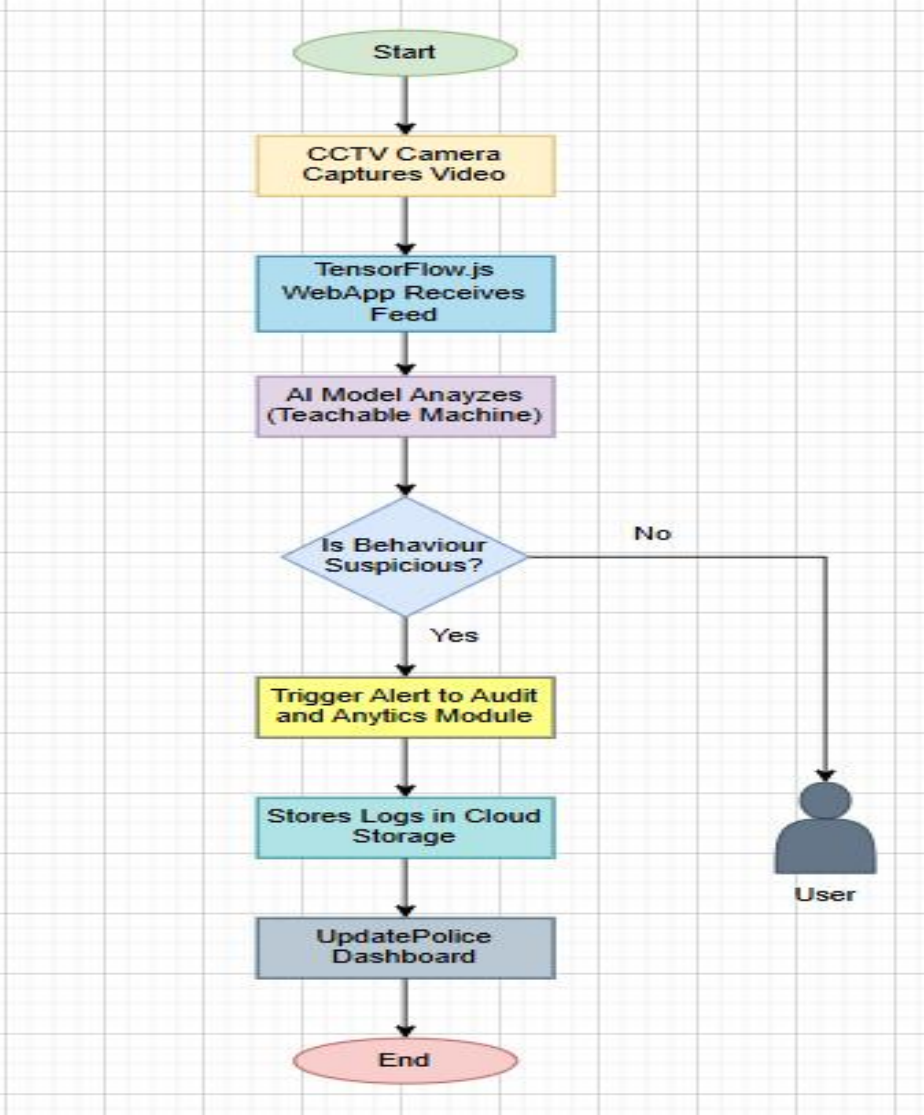
3. Optional Logging (Cloud Storage)

- **Data Logging:** When enabled, the system logs relevant details such as timestamps, behavior classification (e.g., "unauthorized entry"), and a snapshot of the flagged frame.
- **Cloud Integration:** These logs are securely transmitted and stored in a cloud database for later retrieval, auditing, or training of improved AI models.
- **Privacy Controls:** Data storage and access are governed by configurable privacy policies to ensure compliance with local laws and regulations.

4. Output Display (UI + Analytics Dashboard)

- **Real-Time Status:** The web interface displays the current alert status, including the type of behavior detected and the corresponding timestamp.
- **Analytics Dashboard:** A backend dashboard provides historical data visualization, such as detection trends, frequency of alerts, and behavior heatmaps, aiding in decision-making and pattern analysis.
- **User Management:** The dashboard can support multi-user access with role-based permissions, allowing supervisors, operators, and admins to view or manage system components as needed.

Main System Flowchart:



Students Signature

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation: