Title: Home Security System with AI Intrusion Prediction

Group members: Jensen Caestecker, Ward Govaert, Tobias Hungwe, Harman Singh
Draft: 0

Overview project

Develop a smart home security system that monitors for intrusions, uses AI to predict potential security breaches, and provides 3D visualisations of the home environment. The system is designed to ensure continuous monitoring and smart alerts while leveraging both edge computing for local analysis and cloud services for broader functionality. The goal is to build a lightweight, effective system using affordable hardware and sensors

Cloud and Edge Computing

Used hardware

Device: Raspberry Pi or Arduino (for the prototype)
Sensors:

- Motion sensors
- Door/window sensors
- Camera

Communication

The system involves communication between local devices and a cloud platform using MQTT for real-time alerts. Here’s how it works

Local processing: Sensor readings are analysed locally on the Raspberry Pi or Arduino for edge computing. This helps reduce latency and ensures that any unusual activities, like forced entry or unexpected movements, are immediately detected.

Alerts and data transmission: Once the system detects suspicious activity, it sends the processed data and an alert to the cloud MQTT broker. This alert is then forwarded to the user via an app. The communication follows this format, utilising JSON:

```
{
    “action”: “intrusion_detected,
    “sensor”: “front_door”
    “time”: “2024-10-11T14:23:34”
}
```

```
{
    “action”: “motion_detected,
    “location”: “living_room”
    “time”: “2024-10-11T14:25:22”
}
```

Data gathering

The system continuously gathers data from various sensors, including:

- **Motion data:** Whether motion was detected, saved as boolean (true/false)
- **Sensor readings:** From doors and windows, saved as boolean (true/false)
- **Camera feeds:** Captured images or videos from triggered events
- **Intrusion logs:** Details about detected intrusions, stored as logs with timestamps

The system also integrates with AI models to analyse patterns in these data streams and identify potential security threats before they occur.

Edge computing

The edge component is responsible for running local analysis on the Raspberry Pi or Arduino. When an anomaly is detected, it decides whether to trigger an alert, reducing the need for constant cloud communication.

Events

User event: The system will send immediate alerts to the user’s phone when a potential intrusion is detected
User action: Users can remotely control the system via the app (turning it off/on, reviewing alerts, looking at the live camera feed)
Cloud event: Notify the user if the AI predicts a higher risk of intrusion based on historical data

Computations

Average response time, sensor activity logs, intrusion risk score

3D Visualisation

The system used Three.js to render a 3D model of the home. The model includes real-time sensor status updates. The models will most likely be made using technologies like Blender

CMS

The CMS can contain reports with detailed summaries of intrusion attempts and security alerts, which can also be shared with the police.
We will make the CMS ourselves using lightweight packages / frameworks / programming languages to make sure that the Raspberry Pi or Arduino does not use a lot of memory.

For the AI models we will use LiteRT (formerly known as TensorFlow Lite)

Trending Topics

Application 1 in GO: a dashboard that allows users to track their home's security status, with the following content:

- Intrusion attempts logs
- AI-generated risk score
- 3D visual representation of sensor activities
- Rankings of high-risk zones based on sensor data