Security Risks of Mobile Device Sensors

Author: Kateřina Henclová
Supervisor: Ing. Radek Hranický, Ph.D

Goal: Study the various types of possible attacks through mobile sensors and create such an attack.

Did you know you can perform advanced attacks using mobile sensors?

Sensor data is frequently used to perform fingerprinting and tracking, but also:

- **Accelerometer** can classify human walking patterns
- **Gyroscope** is capable of speech recognition
- **Ambient light sensor** can do PIN skimming
- **Magnetometer** could try to identify nearby objects

Want to see a sensor-based attack? Try it out here:

https://feta5.fit.vutbr.cz/attack/

Note: The sensor API is blocked on Privacy based browsers and iOS

Generic Sensor API

Exposes sensors in Andriod:

...

- Allowed by default
- Does not require user permission to collect mobile sensor data

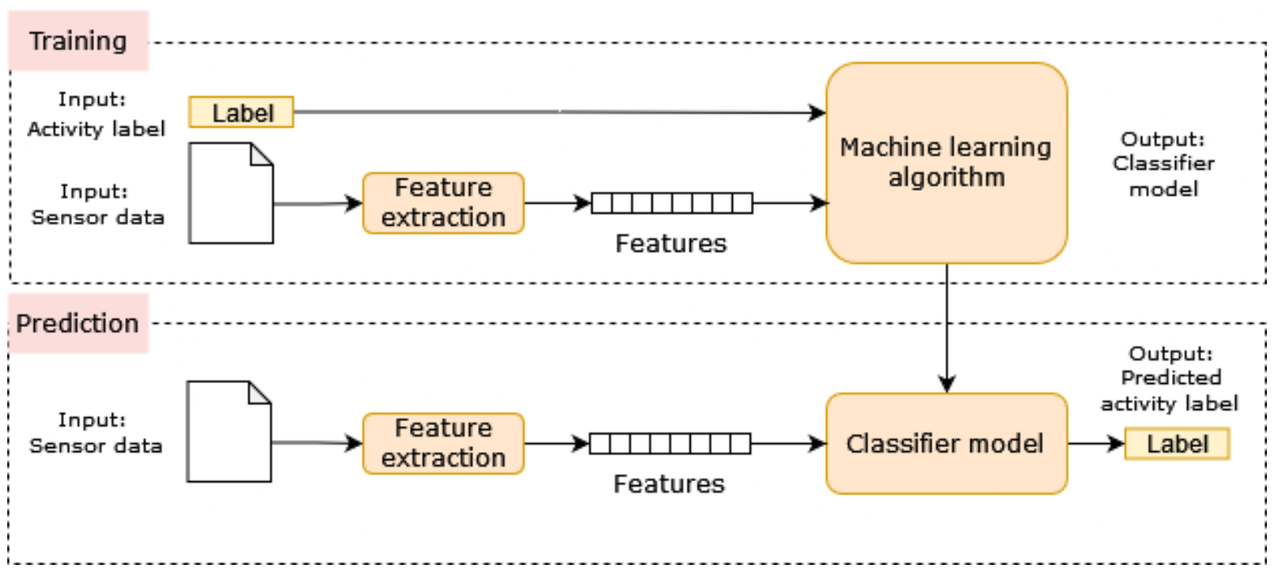
\+ Sensor data can only be accessed by webpages when they are visible

\+ Cannot run in the background

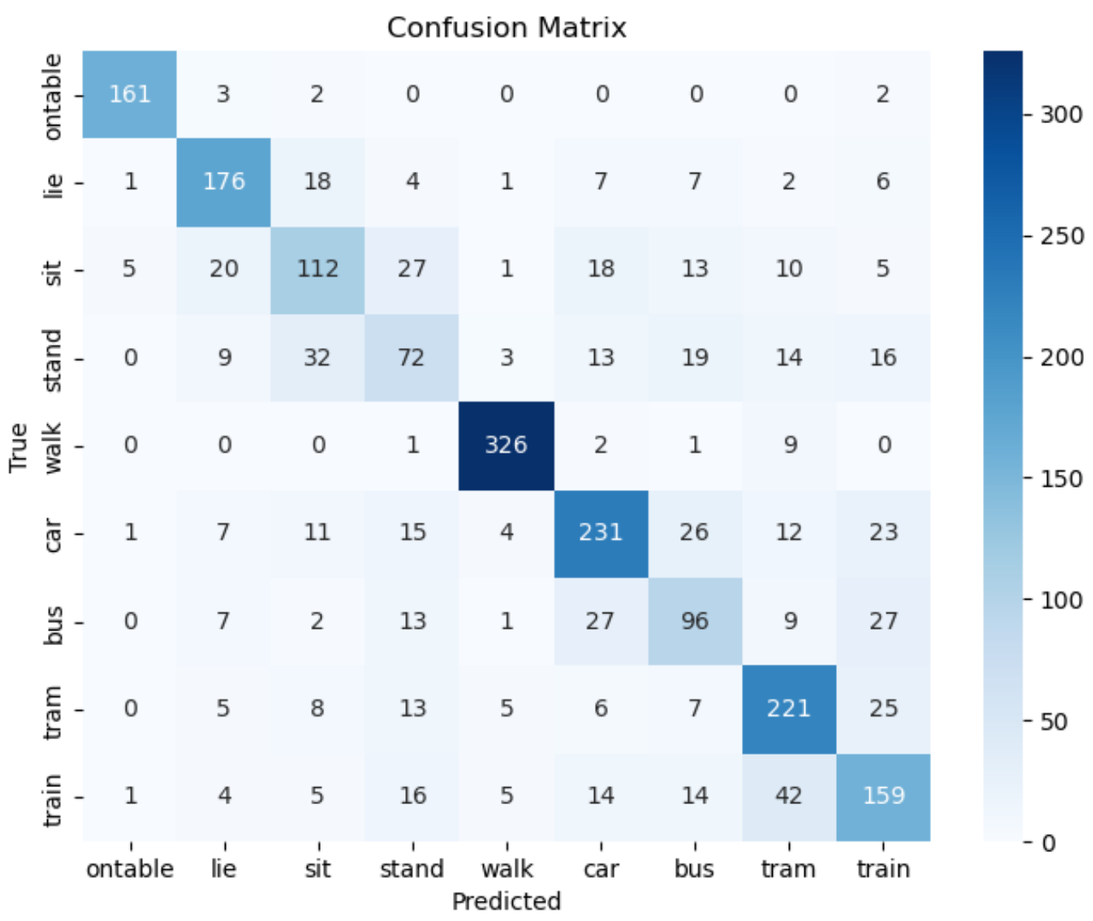
We made an activity recognition attack

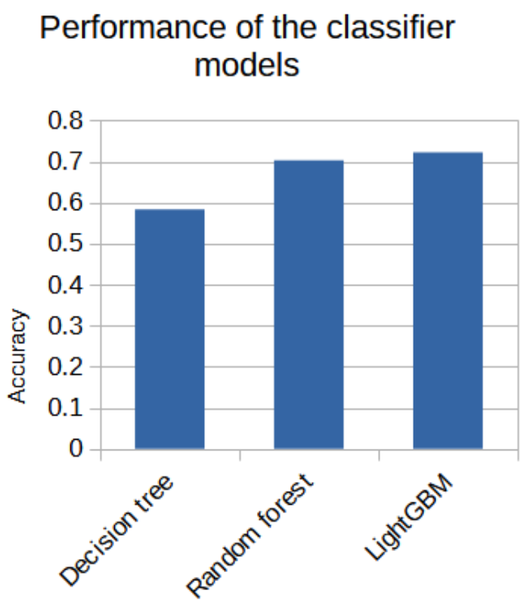
Using machine learning to predict the activity based on sensor data from the Accelerometer, Gyroscope and Magnetometer.

Our training and testing data consisted of **1282 readings**, totaling **13 hours**.



Classifier results:





How to block sites from accesing sensor data?

Quick solution:

Go to browser settings

→ Find Site settings

→ Find Motion or light sensors

→ Block