Universität Bamberg

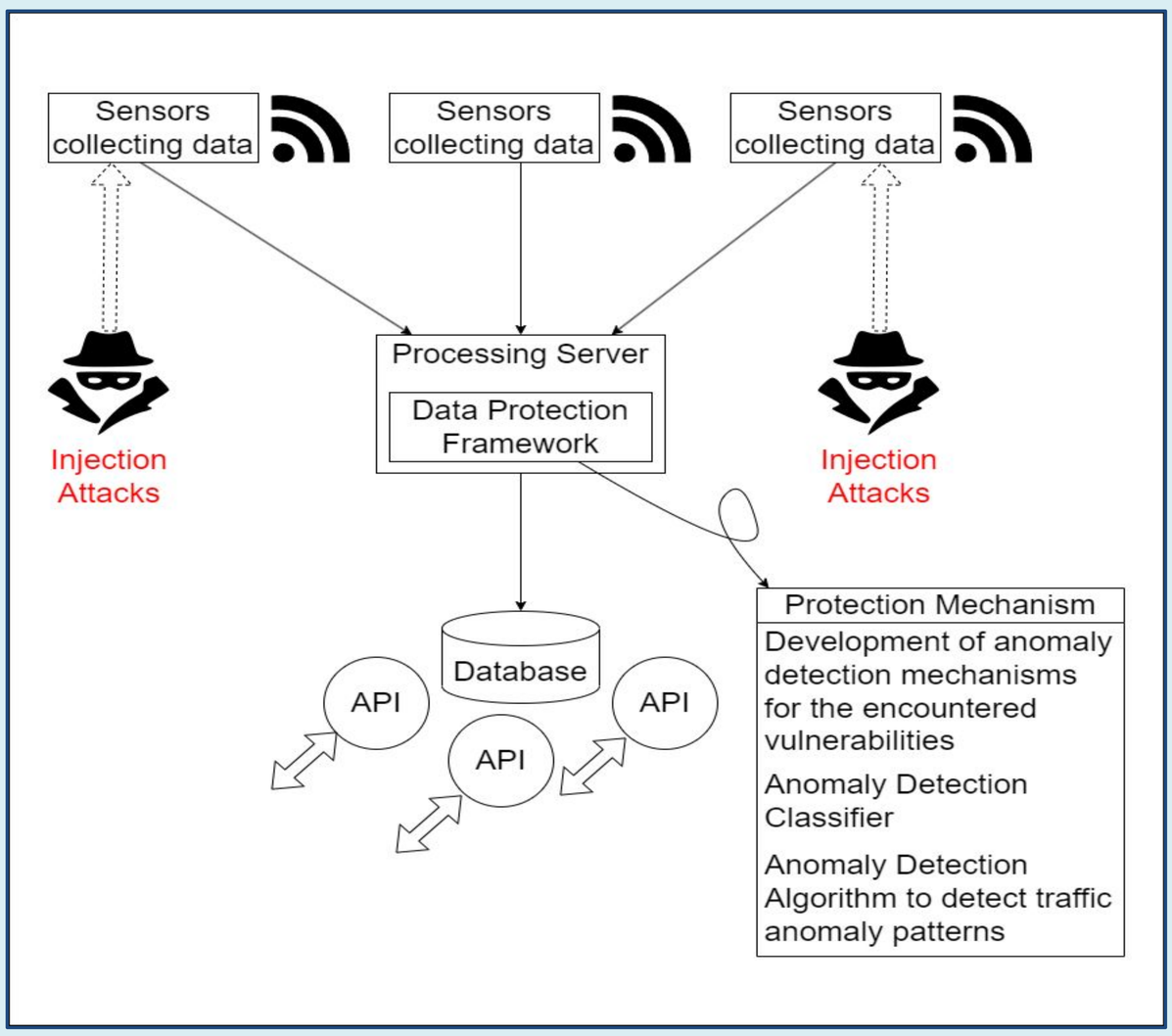
"Evaluating Data Manipulation Threats in WiFi-based People Counting: Risks and Defenses"

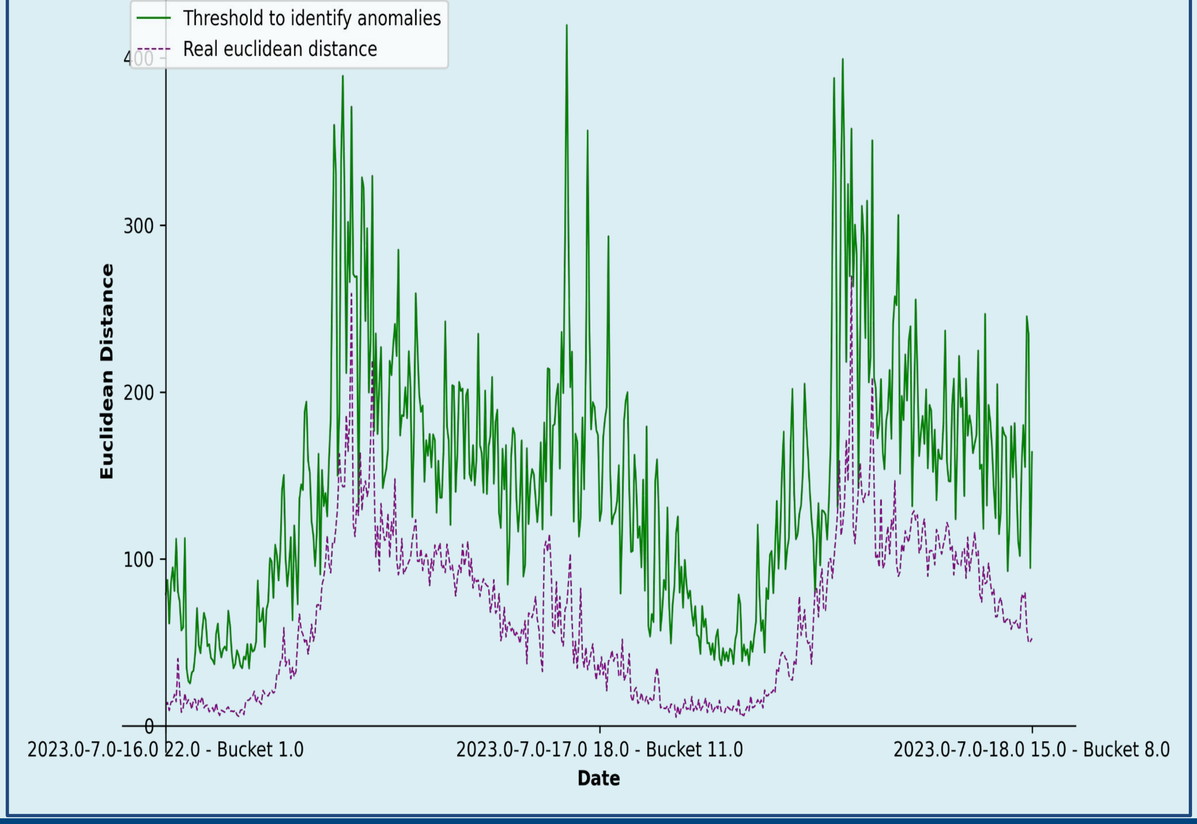
Sarah Asad, Anthony J. Bustamante, Ishraq Haider Chowdhury, Syed Ibrahim Khalil

Goals

- Identifying vulnerabilities in current Smart City architecture
- Testing out the security of the sensors
- Development of data protection framework

Project Architecture





Motivation

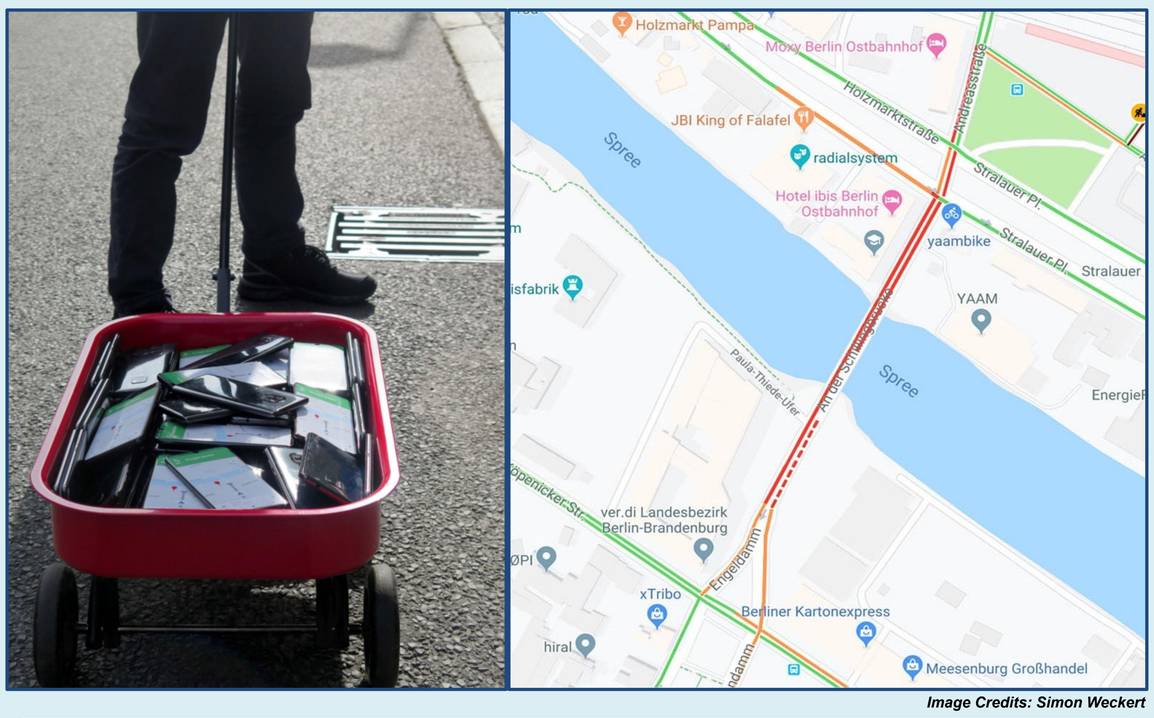
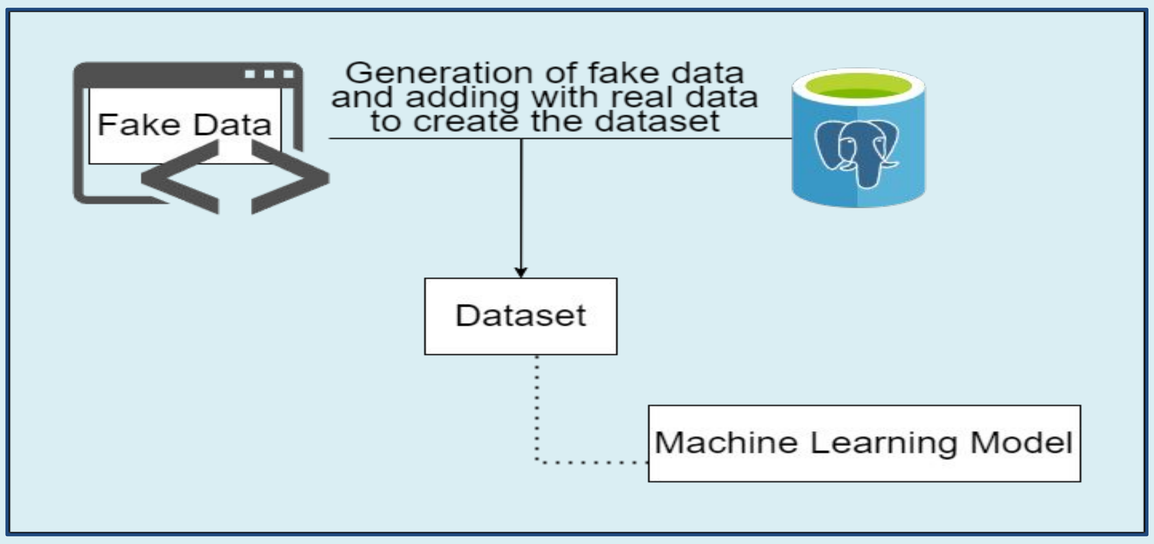


Image Credits: Simon Weckert

Data Generation



Experiments and Results

- We simulated the topology on VM and injected data and random noise to the normal traffic to further analyze anomaly patterns
- The anomaly detection classifier is able to detect any type of data injection attack with 100% precision
- The anomaly traffic detection mechanism can detect flooding attacks with great precision

Future Work

- Incorporating the implemented algorithms into the existing backend technology
- Implementing safeguards for MAC Spoofing
- Implementing safeguards to protect privacy
- Continuing Security Enhancement

unterstützt durch die TechnologieAllianzOberfranken