Project title:

Tools & technology to secure IoT endpoints in railway maintenance

Significance/contribution to the discipline/research problem

- IoT devices will continue to manifold due to cheap electronics & batteries
- IoT devices and AI can be used to predict necessary railway maintenance better

→IoT devices influence railway safety

→AI can be easily maliciously altered, if training data is tampered

→ IoT endpoints need to be protected

Research Question

- What tools & technology can secure IoT railway endpoints cost effectively and what is their performance?

Aims and objectives incl. timeline

Month	1	2	3	4	5	6
Objective 1						
Objective 2						
Objective 3						
Objective 4						

Objectives

1. Overview of current state of the art in the technology
2. Investigate technologies that can be utilized for simulation
3. Simulation & Analysis of Simulation
4. Reporting

Key literature

- Kour, R., Karim, R. and Thaduri, A. (2020) ‘Cybersecurity for railways-A maturity model’, *Journal of rail and rapid transit*, 234(10), pp. 1129–1148. doi: 10.1177/0954409719881849.
- Valdivia, L. J. *et al.* (2018) ‘Cybersecurity-The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs; Cybersecurity-The Forgotten Issue in Railways: Security Can Be Woven into Safety Designs’, *IEEE Vehicular Technology Magazine*, 13. doi: 10.1109/MVT.2017.2736098.
- Kour, R. *et al.* (2019) ‘eMaintenance in railways: Issues and challenges in cybersecurity’, 223(10), pp. 1012–1022. doi: 10.1177/0954409718822915
- Mallah, R. Al, López, D. and Farooq, B. (2020) ‘Cyber-Security Risk Assessment Framework for Blockchains in Smart Mobility’. doi: 10.1109/OJITS.2021.3106863.

Methodology/development strategy/research design

Quantitative Research

- Experiment:
  - Create IoT nodes (Docker) feeding to an AI
  - Use various methods (Authentication, „IDS“, TLS, block chain) to secure the nodes
  - Attack nodes (replay attack, Denial of Service) and measure the impact on performance for the AI
  - Rate tools by performance impact, cost, exploitability

Ethical considerations

- Ethical
  - No surveys, interviews etc. No human participation
  - No data collection from any external sources
  - No data is analysed that contains sensitive or personal identifiable information

→ No ethical approval necessary

Risk assessment

Item	**Severity**	**Likeliness**	**Risk**
Implementation of block chain to complex	High	Low	Medium
Literature already discussing this exact topic	Medium	Low	Low

Description of artefact(s) that will be created

- MSc Thesis (written format)
- Code for blockchain implementation(s)
- Testing document showing performance etc.