

The background is a vibrant blue digital landscape. It features glowing lines, nodes, and a network of connections. In the center, a high-speed train is visible, moving along tracks that recede into the distance. Several people are depicted in various poses, some standing and talking, others walking, all integrated into the digital environment. The overall aesthetic is high-tech and futuristic.

Project title:

# Tools & technology to secure IoT endpoints in a modern AI railway maintenance system

# Significance

- 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
- AI controlled IoT endpoints need to be protected in railway maintenance



# 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



Significance/contribution to the  
discipline/research problem

Tools & technology to secure IoT endpoints in a modern  
AI railway maintenance system

→ Topic not yet discussed in literature, whilst there is a need to do so

# Research Question

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



# Methodology/development strategy/research design

## Quantitative Research

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

Conclusive Research: Descriptive research design

# Aims and objectives incl. timeline

## Objectives

1. Overview of current state of the art in the technology

# Aims and objectives incl. timeline

## Objectives

- 1. Overview of current state of the art in the technology

Month	1	2	3	4	5	6
Objective 1						



# Aims and objectives incl. timeline

## Objectives

1. Overview of current state of the art in the technology
2. Investigate technologies that can be utilized for the experiment

Month	1	2	3	4	5	6
Objective 1						

# Aims and objectives incl. timeline

## Objectives

1. Overview of current state of the art in the technology
2. Investigate technologies that can be utilized for the experiment

Month	1	2	3	4	5	6
Objective 1						
Objective 2						

# Aims and objectives incl. timeline

## Objectives

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

Month	1	2	3	4	5	6
Objective 1						
Objective 2						

# Aims and objectives incl. timeline

## Objectives

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

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

# Aims and objectives incl. timeline

## Objectives

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

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

# Aims and objectives incl. timeline

## Objectives

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

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



# Ethical considerations

- 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 University of Essex Online (UoEO) ethical approval necessary



# Risk assessment

	Item	Severity	Likeliness	Risk
1.				
2.				

# Risk assessment

	Item	Severity	Likelihood	Risk
1.	Implementation of technology to complex	Medium	Medium	Medium
2.				

# Risk assessment

	Item	Severity	Likelihood	Risk
1.	Implementation of technology to complex	Medium	Medium	Medium
2.	Literature already discussing this exact topic	Medium	Low	Low

# Description of artefacts that will be created

- Master of Science Thesis
- Code for nodes, security counter measures, AI, training data, test scripts
- Test reports



# Conclusion

## Tools & technology to secure IoT endpoints in a modern AI railway maintenance system

- Close a significant gap in scientific literature
- Sufficient literature basis, with an appropriate gap to still do a Master thesis
- Aims and objectives (code, testing document, master thesis) fit into a six month timeline
- Methodology (experiment) fit for this purpose
- Ethical considerations conducted
- Only Medium risks expected

→ Suitable, challenging,  
relevant and realistic topic



# References

British Research Methodology (BRM) (n.d.) Research Design

Dawson, C. (2015) Projects in Computing and Information Systems A Student's Guide Third Edition

Mitchell, J. (2018) Ethics vs Morality

Miessler, D. (2020) The Difference between Deductive and Inductive Reasoning

Sage (2021) Sage Research Methods: Methods Map

Saunders, M., Lewis, P. & Thornhill, A. (2012) Research Methods for Business Students 6th ed. Pearson Education Limited