Simona De Vivo

# Augmented AI for Sustainable Cyber Security in Railway Environment

Tutor: Prof. Domenico Cotroneo

Cycle: XXXVII

Year: First

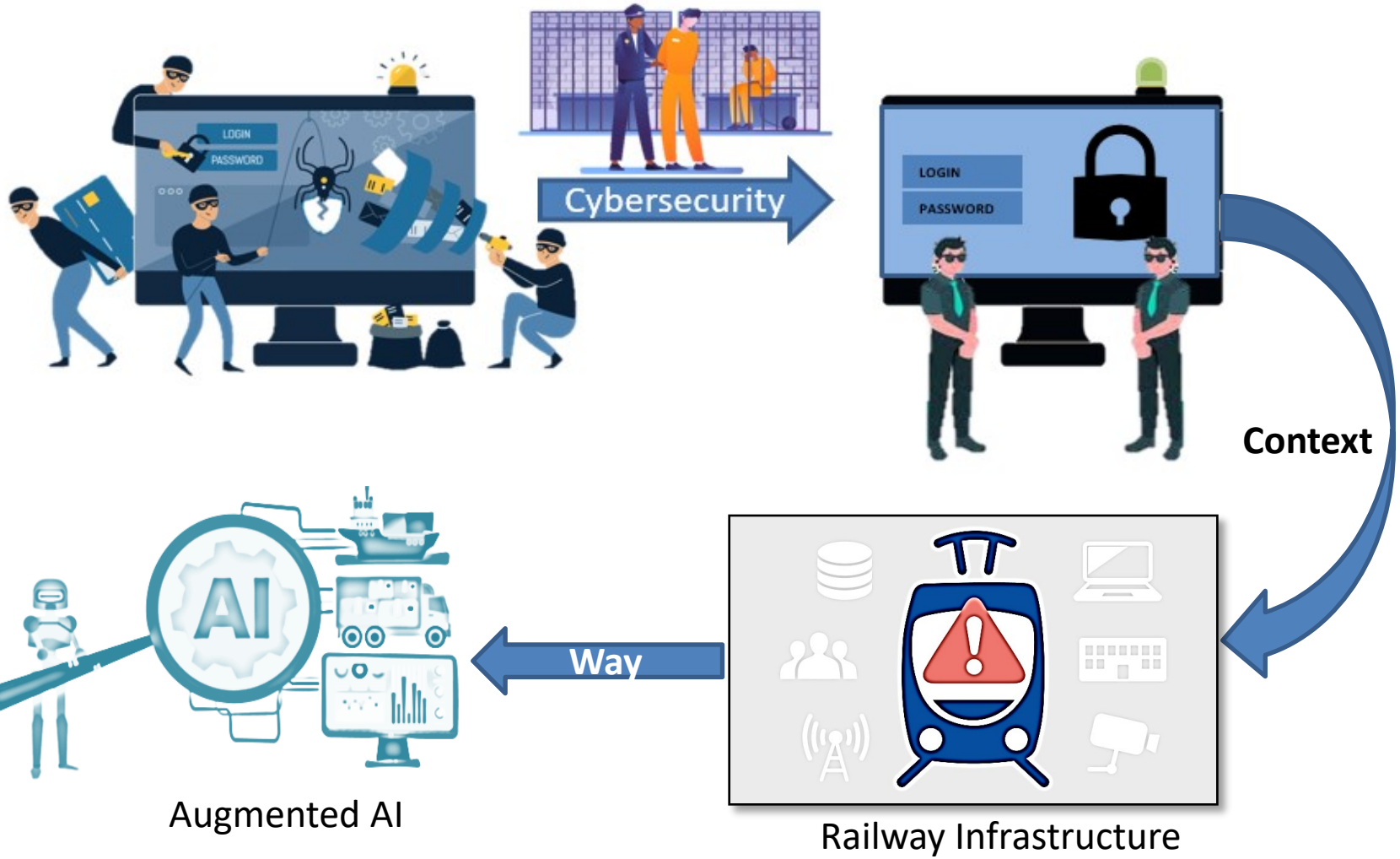
# Presentation Organization

- CONTENT
  - My background
  - My research topics
  - Summary of study activities
  - My research activity
  - Research products
  - Tutorship
  - Next year

# My background

- I received my M.Sc. in Computer Engineering (cum laude) from University of Naples Federico II in October 2021
- I work within the DESSERT group at DIETI
- My PhD started on 1st January 2022
- **Type of fellowship:** PhD student grant – Type: MUR PON

# Research field of interest



# Summary of study activities

**Conferences / events attended:**

- The 1st Intl. Workshop on Natural Language-based Software Engineering  Co-located with ICSE 2022

**Seminars:**

- Rails Mid-Term Workshop
- Project Vāc: Can a Text-to-Speech Engine Generate Human Sentiments?
- Explainable Natural Language Inference
- An Introduction to Deep Learning for Natural Language
- QoE management in 5G networks
- Cybercrime and Information warfare: national and international actors
- Privacy and Data Protection
- Privacy-Preserving Machine Learning

**Ad hoc PhD courses / schools:**

- Virtualization technologies and their applications
- Statistical data analysis for science and engineering research
- Scientific Programming and Visualization with Python
- Imprenditorialità Accademica
- ARTISAN Summer School (Role and effects of ARTificial Intelligence in Secure ApplicatioNs)
- Machine Learning for Science and Engineering Research
- DataWeek (Python & Tableau)

**Courses borrowed from MSc curricula:**

- Data Security
- Critical Data Visualization

# Research activity: Problems

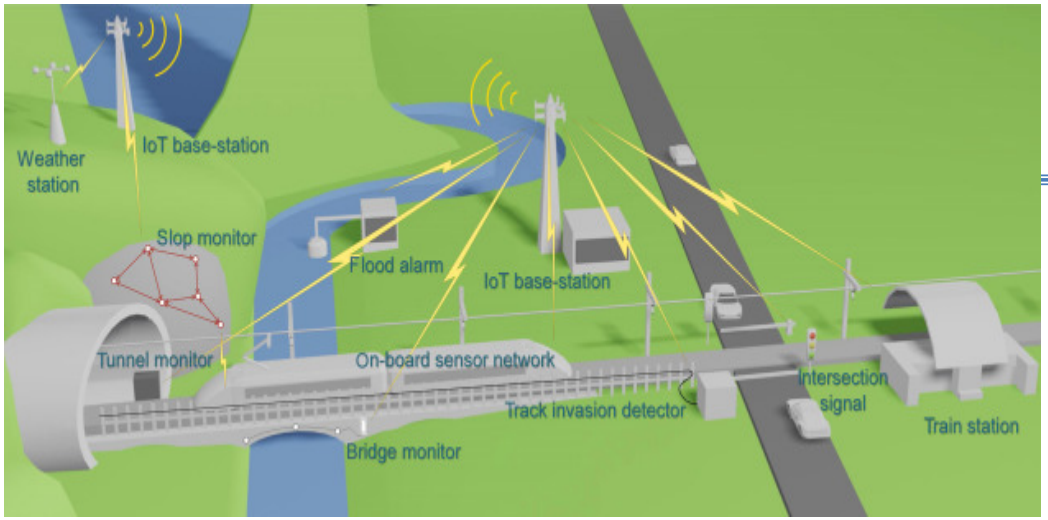
## Cybersecurity

- Data dumps and junk data;
- Use of artificial intelligence techniques (e.g., deep learning models) that are computationally very complex and result in excessive waste of resources;
- Emission of massive amounts of $CO_2$.

## Railway Infrastructure

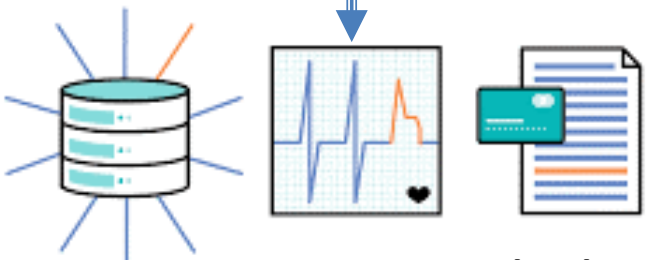
- Railway maintenance requires machines and operation that usually emit significant amounts of carbon;
- Railway infrastructure must satisfy safety regulations that include preventive maintenance;
- Cost optimization at every stage of the process, including maintenance;
- Maintenance of a wide variety of technological elements which are installed in railway infrastructure.

# Research Activity: Proposed Solution

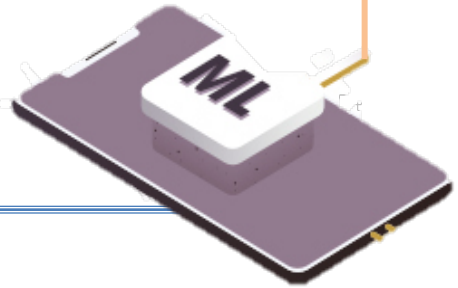



Collected Data

**Monitoring Solution**



**Anomaly Detection (AD)**




**Main Requirements:**

- **Real-Time** (e.g., Real-Time processing applied to anomaly detection)
- **Green** (e.g., transfer learning, distributed learning, TinyML, …)

# Research activity: Methodology


**..test the robustness of the monitoring solution?**

- **I will evaluate the accuracy in terms of metrics commonly used for anomaly detection (e.g., tre/false positive/negative rates).**

| | |
|---|---|
| **True negative**<br>Predicted negative<br>Actual negative | **False positive**<br>Predicted positive<br>Actual negative |
| **False negative**<br>Predicted negative<br>Actual positive | **True positive**<br>Predicted positive<br>Actual positive |

And


**.. assess the improvements made from an energy and computational point of view?**

- **I will evaluate the reductions in carbon emissions, energy consumption, execution time, the complexity of the models implemented, etc.**

# My Product

| | |
|---|---|
| Conference Paper | Liguori Pietro, Improta Cristina, **De Vivo Simona**, Natella Roberto, Cukic Bojan, & Cotroneo Domenico (2022). "**Can NMT Understand Me? Towards Perturbation-based Evaluation of NMT Models for Code Generation**". IEEE/ACM 1st International Workshop on Natural Language-Based Software Engineering (NLBSE), 2022. |

# Tutorship

- During the first year, I carried out 5 hours of tutoring as part of the "additional activities" called "Matlab and Simulink for Electrical Engineering".

# Future Activities

- Use of NLP techniques to monitor infrastructure and identify anomalies due to cyber attacks;
- Implementation of an intelligent attack analysis and detection solution using online data processing;
- Period abroad: University of North Carolina at Charlotte, under the supervision of the Dr. Bojan Cukic.

# Thank you!

Contact:
simona.devivo@unina.it

# Bibliography


- Li, Q.Y., Zhong, Z.D., Liu, M. and Fang, W.W., 2017. Smart railway based on the Internet of Things. In Big data analytics for sensor-network collected intelligence (pp. 280-297). Academic Press.
- Jo, O., Kim, Y.K. and Kim, J., 2017. Internet of things for smart railway: feasibility and applications. *IEEE Internet of Things Journal*, *5*(2), pp.482-490.
- Lydia, E.L., Jovith, A.A., Devaraj, A.F.S., Seo, C. and Joshi, G.P., 2021. Green energy efficient routing with deep learning based anomaly detection for internet of things (IoT) communications. *Mathematics*, *9*(5), p.500.
- Siegmund, N., Dorn, J., Weber, M., Kaltenecker, C. and Apel, S., 2022. Green Configuration: Can Artificial Intelligence Help Reduce Energy Consumption of Configurable Software Systems?. *Computer*, *55*(3), pp.74-81.
- Cai, H., Gan, C., Wang, T., Zhang, Z., & Han, S. (2019). Once-for-all: Train one network and specialize it for efficient deployment. *arXiv preprint arXiv:1908.09791*.
- Lenherr, Nicola, René Pawlitzek, and Bruno Michel. "New universal sustainability metrics to assess edge intelligence." *Sustainable Computing: Informatics and Systems* 31 (2021): 100580.
- Kashyap, Pankaj Kumar, et al. "DECENT: Deep Learning Enabled Green Computation for Edge centric 6G Networks." *IEEE Transactions on Network and Service Management* (2022).
- KOUR, Ravdeep, et al. A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, 2022, 09544097221089389.

# Bibliography


- Viegas, Eduardo, et al. "Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems." *IEEE Transactions on Computers* 66.1 (2016): 163-177.
- Abououf, Menatalla, et al. "Self-supervised Online and Light-Weight Anomaly and Event Detection for IoT Devices." *IEEE Internet of Things Journal* (2022).
- Paparrizos, John, et al. "Volume under the surface: a new accuracy evaluation measure for time-series anomaly detection." *Proceedings of the VLDB Endowment* 15.11 (2022): 2774-2787.
- Habeeb, Riyaz Ahamed Ariyaluran, et al. "Real-time big data processing for anomaly detection: A survey." *International Journal of Information Management* 45 (2019): 289-307.
- Yao, Yuan, et al. "Online anomaly detection for sensor systems: A simple and efficient approach." *Performance Evaluation* 67.11 (2010): 1059-1075.
- Ding, Nan, et al. "Real-time anomaly detection based on long short-Term memory and Gaussian Mixture Model." *Computers & Electrical Engineering* 79 (2019): 106458.
- Van Wyk, Franco, et al. "Real-time sensor anomaly detection and identification in automated vehicles." *IEEE Transactions on Intelligent Transportation Systems* 21.3 (2019): 1264-1276.