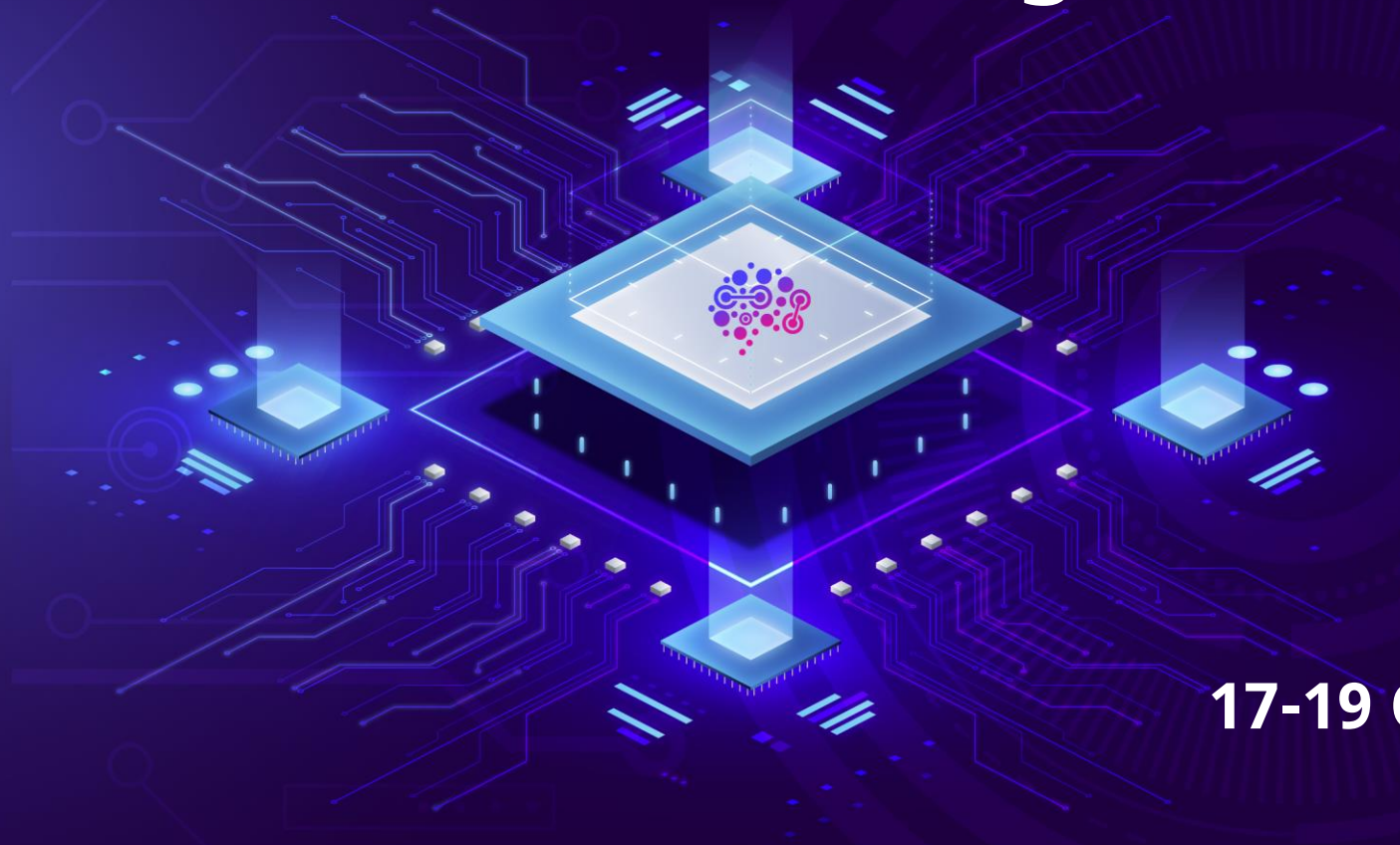
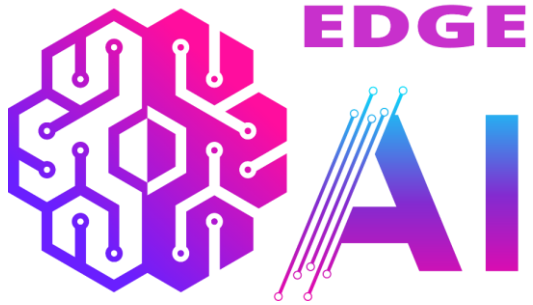
European Conference on EDGE AI Technologies and Applications - EEAI



Advancing emerging edge AI technologies and driving next generation intelligent applications.

17-19 October 2023, Athens, Greece

European Conference on EDGE AI Technologies and Applications - EEAI



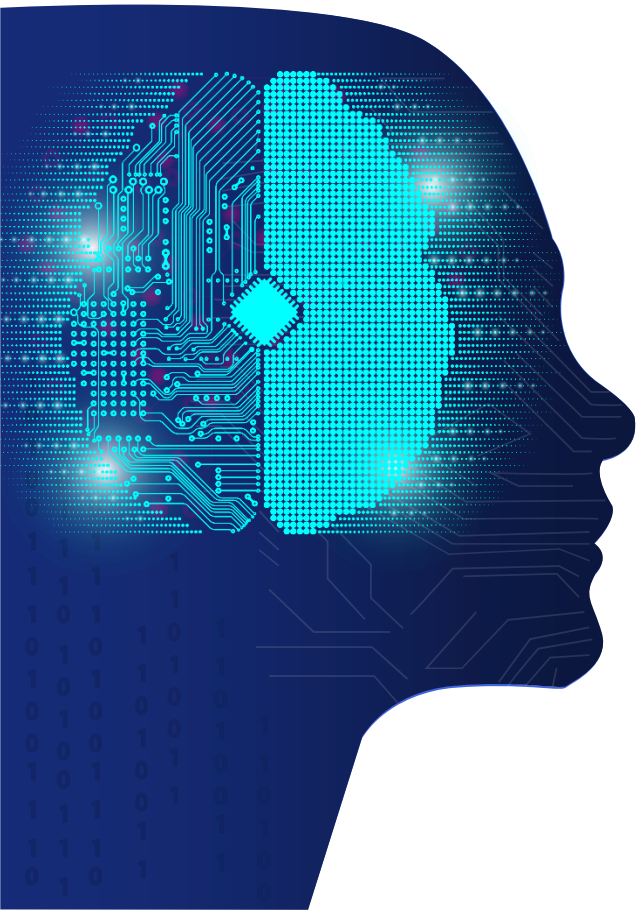
Efficient AI-based Attack Detection Methods for Sensitive Edge Devices and Systems

Celine Thermann, University of Lübeck, Germany

17-19 October 2023 Athens, Greece

Copyright © 2023

Presentation Outline



- Introduction
- State-of-the-art
- Research Goal
- Methodology
- Future Research
- Conclusion

Copyright © 2023

Introduction

- Increasing number of edge devices processing sensitive data
- Intelligent AI-based protection mechanisms to provide detection capabilities
- Focus on micro-edge level for selection of applicable AI algorithms
- *Attacker goal*:
  - Extract or manipulate data
  - Interrupt correct execution of device
- *Problems*:
  - Environmental stresses due to increased operation times
  - Techniques might have high false-positive rates
- *Contributions*:
  - Requirements of the protection mechanisms
  - Capabilities of state-of-the-art techniques

Copyright © 2023

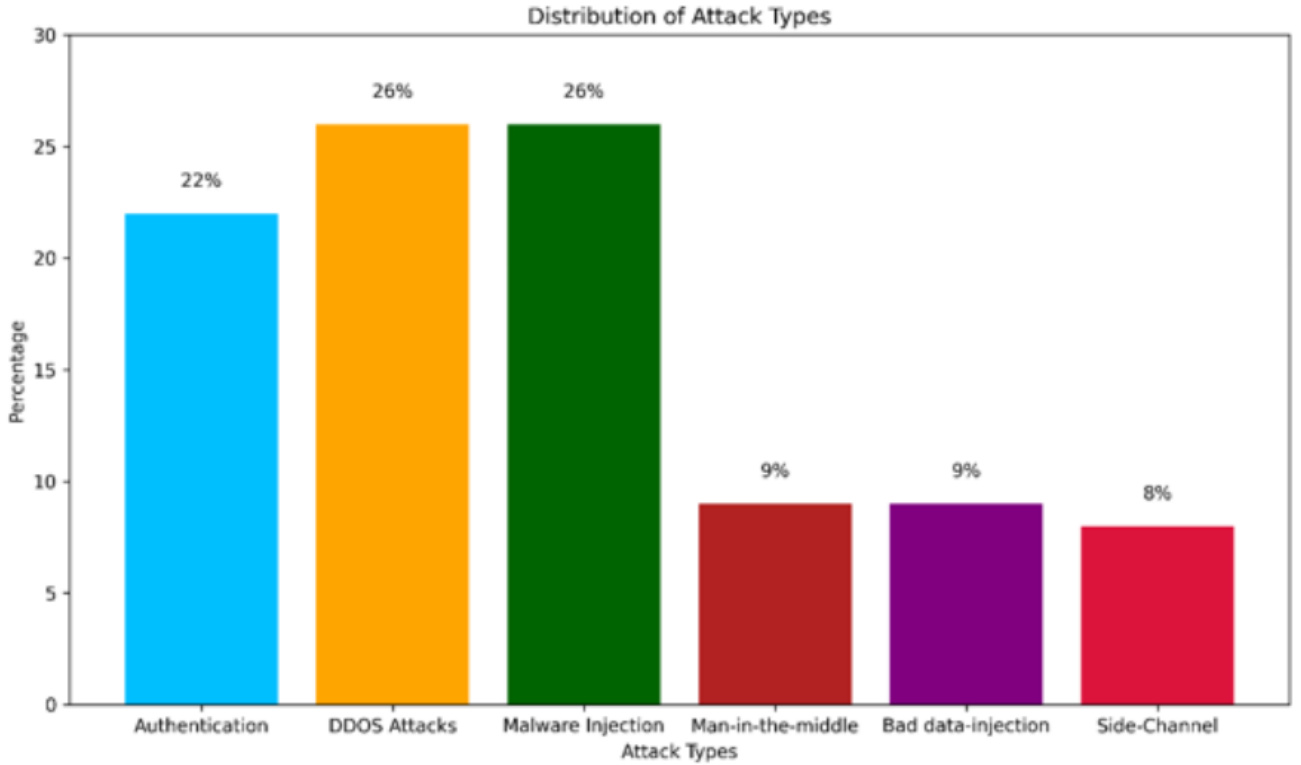
State-of-the-art Attacks

- Might have limitations compared to non-edge systems
- Possible attacks on edge devices and nodes:
  - Malware injection attacks
  - DDOS attacks
  - Authorization attacks
  - Physical attacks
    - Timing side-channel attacks
    - Power side-channel attacks
    - Fault injection attacks

Copyright © 2023

State-of-the-art Attacks

- Possible attacks on the cloud:
  - Escape of tenant separation e.g. using side-channel attacks
- Intrusion attacks on edge system:
  - Impersonation attack
  - Communication interception
  - Password guessing attack
  - Data integrity violation
  - Denial of service
  - Bad quality of service



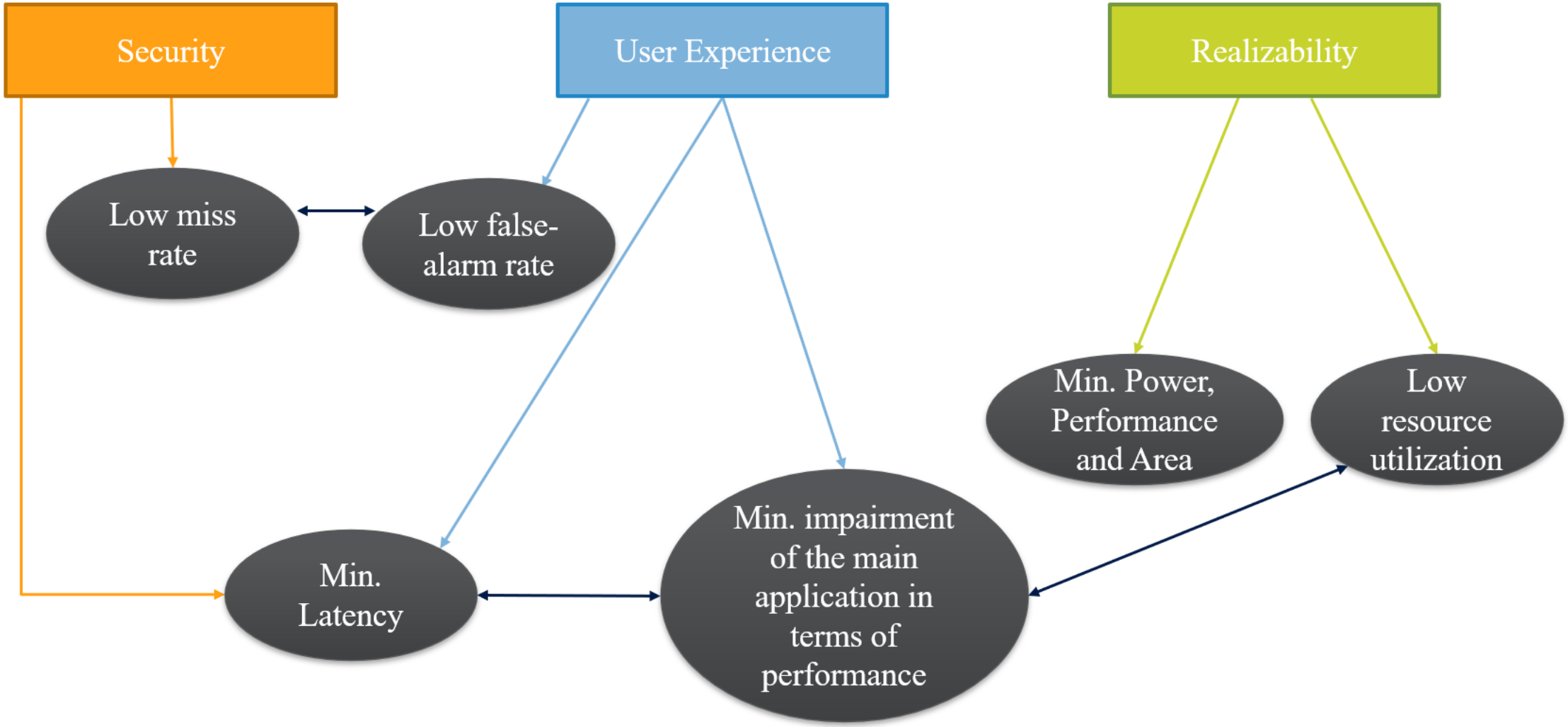
Copyright © 2023

State-of-the-art Detection

- AI-based detection on edge device level:
  - Different machine learning models
  - Features e.g. hardware performance counters
  - Shielded execution to prevent malicious execution
- AI-based detection at cloud level:
  - Combination of signature and anomaly-based techniques
  - Recurrent neural networks
- AI-based intrusion detections systems for edge systems:
  - AI methods to identify patterns and anomalies
  - Problems:
    - Quality of data
    - Accuracy and performance of model

Copyright © 2023

Research Goal



Copyright © 2023

Methodology

- Possible algorithms: Neural Networks, Trees, Support Vector Machine (SVM), Bayesian Network, Instance-based, Linear Regression, Discriminant Analysis, Ensembles
- *Considerations*:
  - Computational complexity
  - Storage requirements
  - Increased area due to accelerator
- Work often concentrates on non-edge devices

Copyright © 2023

Future Research

- Generate Dataset for training and validation
  - Analyze relevant phases of the application and available inputs
  - Combine capabilities and theoretical considerations of attacks to derive artificial dataset
- Select applicable algorithms
- Evaluate and compare algorithms based on results and computational loads

Copyright © 2023

Conclusion

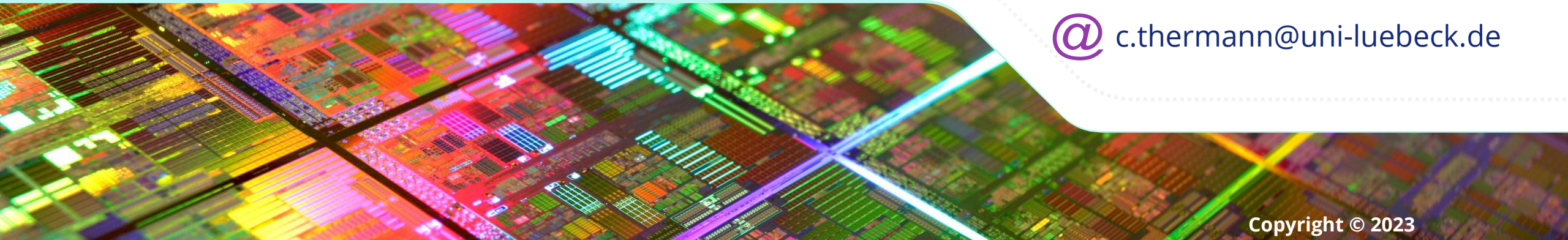
- Increasing use and uptime of devices increase sensor events during lifetime especially for micro-edge devices
- Solution shouldn’t influence operation or user experience negatively
- AI offers possibility for intelligent monitoring
- Choice of suitable AI algorithm important
- Research for these algorithms on the edge open

Copyright © 2023

EDGE AI

Thank You

For your attention



@ c.thermann@uni-luebeck.de

Copyright © 2023