Simona De Vivo

GreenAI Approaches for IoT Intrusion Detection

Tutor: Prof. Domenico Cotroneo

Cycle: XXXVII

Year: Third

Candidate's information

- MSc degree in Computer Engineering (October 2021)
- DIETI Research group: DESSERT
- PhD start date 01/01/2022 – end date 31/12/2024
- Scholarship type: PON MUR
- Periods abroad: 8 months to University of North Carolina at Charlotte, USA, Under the supervision of Prof. Bojan Cukic and Prof. Dong Dai (08/06/2023 – 01/02/2024)
- Periods in company: 6 months to Digital Platforms S.p.A. (Roma)

Summary of study activities

- PhD schools:
  - ARTISAN Summer School (Role and effects of ARTificial Intelligence in Secure ApplicatioNs), Valence, France
- Courses:
  - Scientific Programming and Visualization with Python (PhD course, Prof. Alessio Botta)
  - Imprenditorialità Accademica (PhD course, Prof. Pierluigi Grippa)
  - Machine Learning for Science and Engineering Research (PhD course)
  - Data Security (MSc course)
  - Critical Data Visualization (MSc course)
  - Data Week (Online Academy)
  - RTA – REAL TIME ANALYTICS MOD. C
  - RTA – REAL TIME ANALYTICS MOD. D
  - Statistical data analysis for science and engineering research (PhD course)
  - Virtualization technologies and their applications (PhD course, Prof. Luigi De Simone) ù
- Conferences attended:
  - 1st International Workshop on Natural Language-based Software Engineering (remotely)

Research area(s)

- My research project is set in the **IoT context**, focusing on cybersecurity and sustainability.
- My research contribution focuses on **GreenAI**, which refers to using AI sustainably by applying energy-efficient techniques to intrusion detection to address **cybersecurity concerns** and the IoT systems **environmental impact**.

Research results

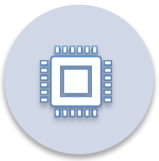
- **Major Contributions** (included in PhD Thesis)**:**
  - Evaluation of Traditional SIEM platforms in order to identify gaps in scalability and adaptability for IoT context;
  - Building an open-source, scalable IoT IDS-testbed, named DDoShield-IoT, supporting realistic traffic simulation, ML model evaluation, and dataset generation.
  - Use of Data Augmentation Techniques to improve the ML model performance for IoT security.
  - Novel methodology proposal that combines User Profiling and Federated Learning in a two-phase IDS for scalable and efficient IoT security, validate in a real-world scenario.

Research products

[P1]	Pietro Liguori, Cristina Improta, **Simona De Vivo**, Roberto Natella, Bojan Cukic, Domenico Cotroneo, *Can NMT understand me? towards perturbation-based evaluation of NMT models for code generation*, 1st International Workshop on Natural Language-based Software Engineering, Pittsburgh, Pennsylvania, May 2022, pp. 59-66, Association for Computing Machinery, DOI: 10.1145/3528588.3528653
[P2]	Alessandra Rizzardi, Raffaele Della Corte, Jesús F. Cevallos M., Vittorio Orbinato**, Simona De Vivo**, Sabrina Sicari, *RailRED: a Node-RED-Based Framework for Modeling Train Control Management Systems*, 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Paris, France, 2024, October 2024, pp. 671-674, IEEE, DOI: 10.1109/WiMob61911.2024.10770345.
[P3]	**Simona De Vivo**, Islam Obaidat, Dong Dai, Pietro Liguori *DDoShield-IoT: A Testbed for Simulating and Lightweight Detection of IoT Botnet DDoS Attacks* 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) Brisbane, Australia, June 2024, pp. 1-8, IEEE, DOI: 10.1109/DSN-W60302.2024.00014.
[P4]	**Simona De Vivo**, Pietro Liguori *Simulation Environment for the Evaluation of Lightweight Intrusion Detection Systems* 34th International Symposium on Software Reliability Engineering Workshops (ISSREW) Florence, Italy, October 2023, pp. 132-135, IEEE, DOI: 10.1109/ISSREW60843.2023.00061

Research context

IoT (Internet of Things) consists of numerous interconnected devices that collect and share data over the Internet to provide intelligent services and improve systems like homes, cities, and industries. Although this technology brings many benefits, it also brings significant critical challenges, especially for cybersecurity.



Scalability & Interoperability

Power and memory limitations

Real Time Monitoring

Comprehensive Evaluation Metrics

Scarcity of high-quality data and privacy concerns

Simplified Usability and Replicability

Autonomous IDS

PhD thesis overview

- **Problem statement from literature.**
  - Traditional IDSs and SIEMs ineffective at real-time adaptation to heterogeneous IoT threats.
  - Traditional AI methods are unsustainable and limited by IoT device constraints.
  - Lack of quality IoT datasets and synthetic data limits AI-driven security in complex IoT systems.

- **Objective:**

  Use Green AI techniques (such as FL and Lightweight IDS) to create a security solution capable of real-time detection of different cyber attacks, including zero-day attacks. This solution must be able to adapt to the resource constraints of IoT devices, achieve high performance, optimize energy and processing consumption, and ensure security, automation and sustainability.

- **Contribution:**
  - Evaluation of traditional security solutions to detect large scale attacks, typical of IoT context.
  - Implementation of a Lightweight IDS for DoS detection in an embedded network.
  - Implementation of DDoShield-IoT, an IDS testbed for building and evaluating IDSs in the IoT context that supports: Data Augmentation (DA) and FL Techniques.

PhD thesis Contribution

- In collaboration with **DigitalPlatforms S.p.A.** [1], have been evaluated RTA and LimaCharlie SIEM ability to detect DDoS attacks (simulated through **DDoSim** [2]), highlighting strengths and weaknesses.

«Which platform fits best in the IoT context?»

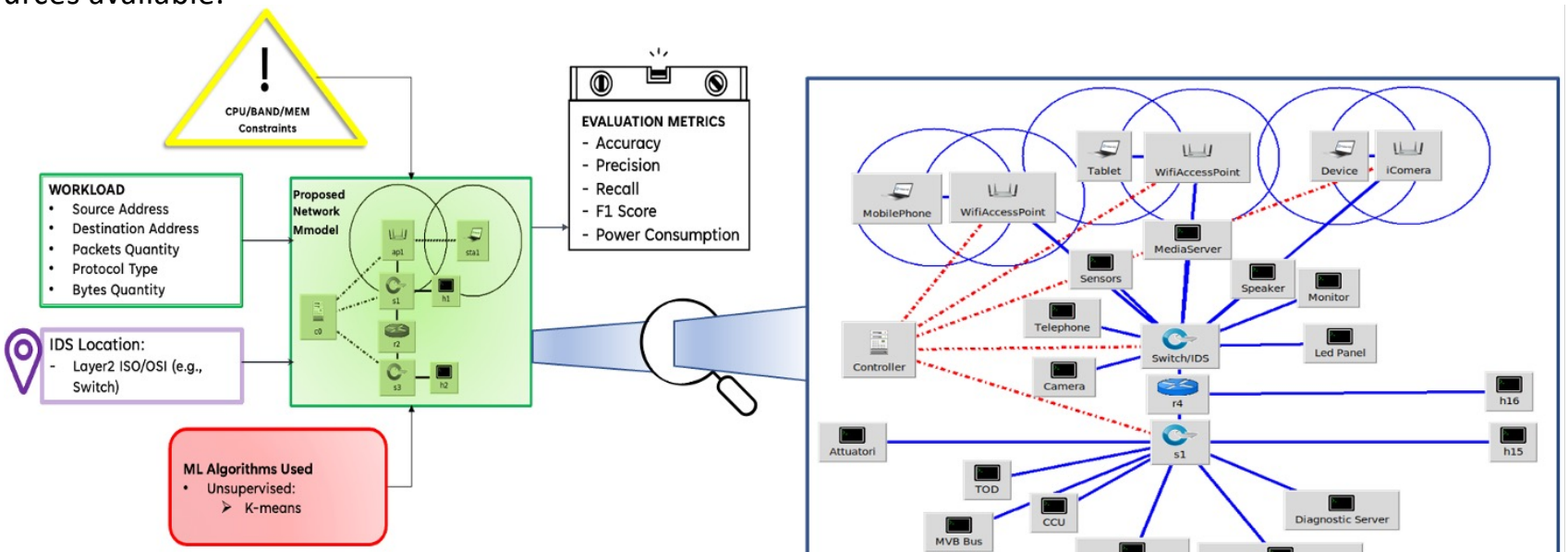
- Both platforms offer advanced security, particularly:
  - LimaCharlie seems more promising for highly scalable contexts with advanced automation needs.
  - RTA is a good choice for simpler, centralized environments.
- However, detection rules rigidity, limited temporal correlation, and lack of resource-constrained device optimization make these platforms unsuitable for dynamic IoT environments.

«How can we overcome the traditional security solution limitations to better address IoT-specific challenges?»

[1] DigitalPlatforms: https://www.dplatforms.it/
[2] I. Obaidat et al. "Creating a large-scale memory error iot botnet using ns3dockeremulator," 2023, DSN, DOI: https://doi.org/10.1109/DSN58367.2023.00051

PhD thesis Contribution

A simulation environment for evaluating the performance and power consumption of a lightweight IDS in an embedded network is presented. The goal is to assess the trade-off between the IDS's accuracy and its energy consumption, given the limited CPU and RAM resources available.



Embedded Network of on-board Train. Real-world topology.

RAM < 200 MB	200 MB < RAM < 1 GB
Memory error di Python (Cause: modules allocation failed)	When saturing memory, there is IDS crash (process killed)

CPU usage limitation by cpulimit tool:

- 35% → 0.9 GHz Raspberry Pi 2 Model B
- 60% → 1.5 GHz Raspberry Pi 4 Model B

PhD thesis Results

- 2 GB of RAM

	CPU Speed Clock	Dual Core	Quad Core
Accuracy	0.9 GHz	72.5%	77%
	1.5GHz	80.7%	85.1%
	2.6 GHz	85.6%	90.8%
Precision	0.9 GHz	61.7%	65.7%
	1.5GHz	70.9%	74.1%
	2.6 GHz	80.4%	84.3%
Recall	0.9 GHz	78.7%	82.7%
	1.5GHz	84.5%	89.7%
	2.6 GHz	90.8%	94.8%
F1-score	0.9 GHz	69.2%	73.2%
	1.5GHz	77.1%	81.2%
	2.6 GHz	85.3%	89.2%

- IDS accuracy drops as CPU speed and cores decrease.
- A 7% reduction occurs when the speed clock decreases from 2.6 GHz to 1.5 GHz, and 15% when it decreases to 0.9 GHz.
- Limiting cores from 4 to 2 reduces performance by about 4%.

- The IDS uses 0.25 to 1.5 Watts on average.
- These values are typical for a device like Raspberry Pi.
- Limiting resources affects performance but helps reduce power.

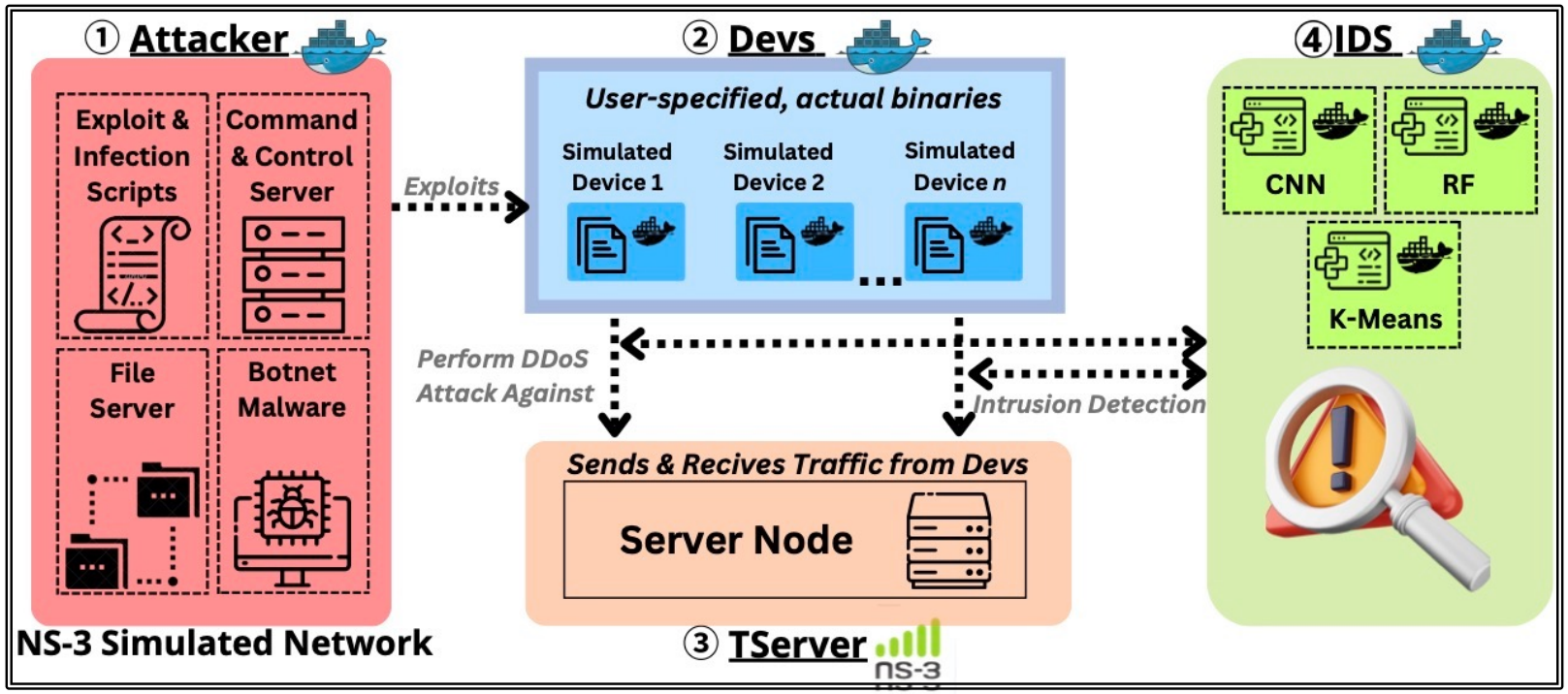
- *Critical infrastructure needs higher detection performance*
- *This solution works well in localized networks but requires enhancements for larger, dynamic IIoT systems.*

DDoShield-IoT

PhD thesis Results

Problems addressed

- Realistic Dataset
- Scalability
- Real-Time Monitoring
- Reproducibility
- Sustainability

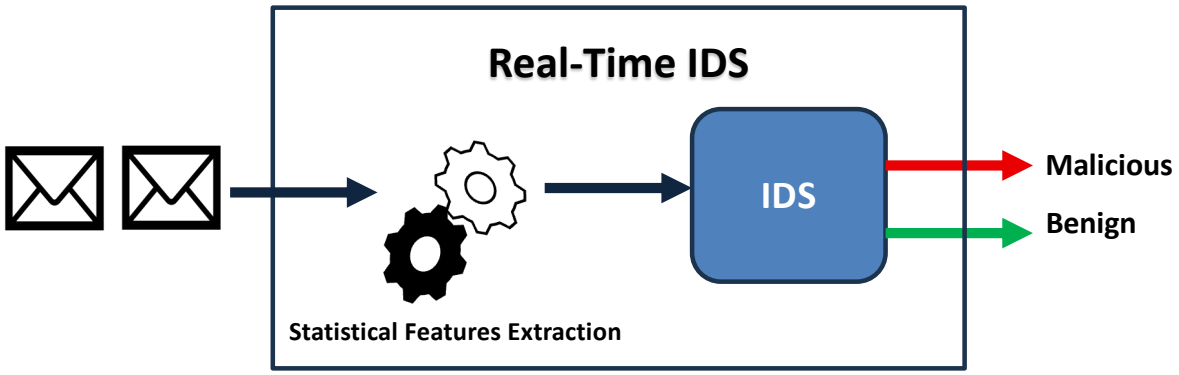


DDoShield-IoT

A platform that simulates IoT networks and devices using Docker and ns3 to create realistic traffic scenarios, helping to develop and test ML-based IDSs.

DDoShield-IoT GitHub

PhD thesis Contribution



- A 600-second simulation trained IDS models, followed by real-time classification and performance evaluation.

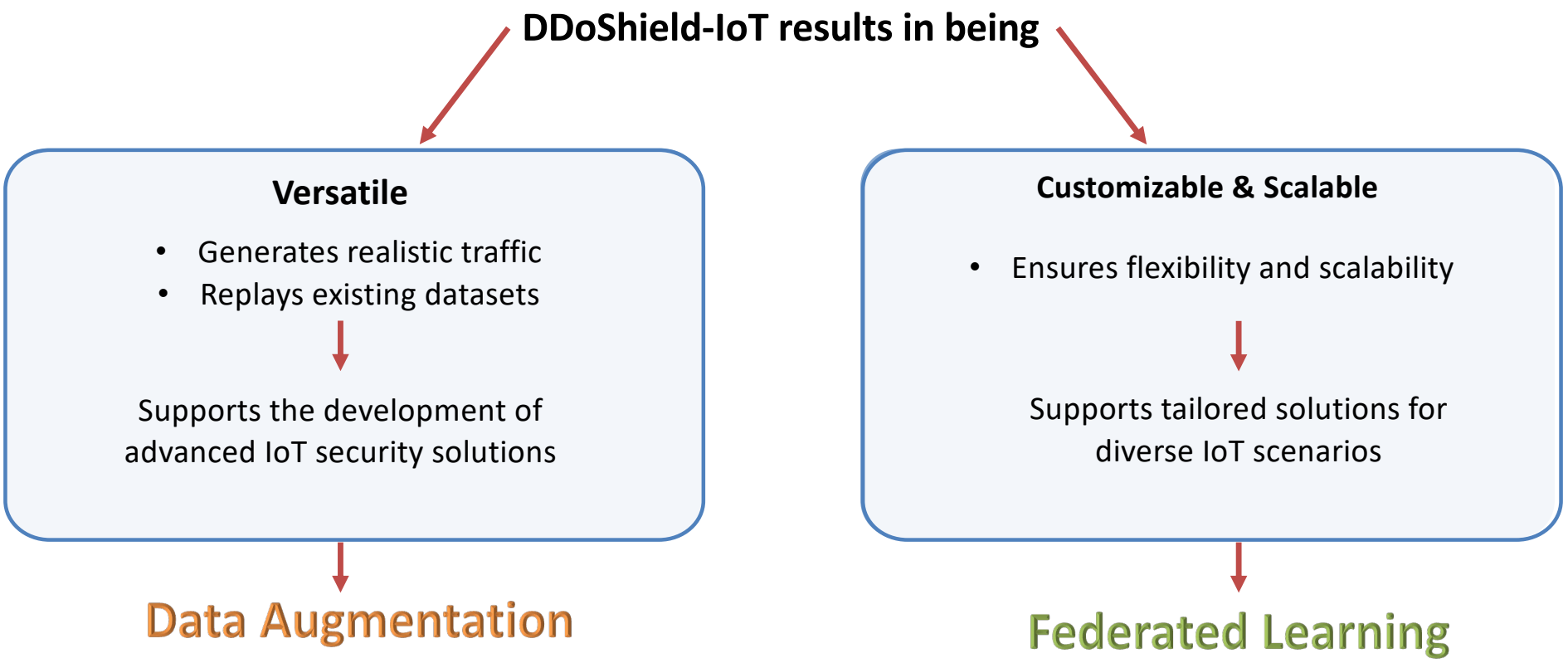
RQ1: How effective is DDoShield-IoT in detecting IoT botnet DDoS in Real-Time?

Model	Accuracy (%)
RF	61.22
K-Means	94.82
CNN	**95.47**

RQ2: How do IDS model resources affect DDoShield-IoT sustainability and compatibility with IoT devices?

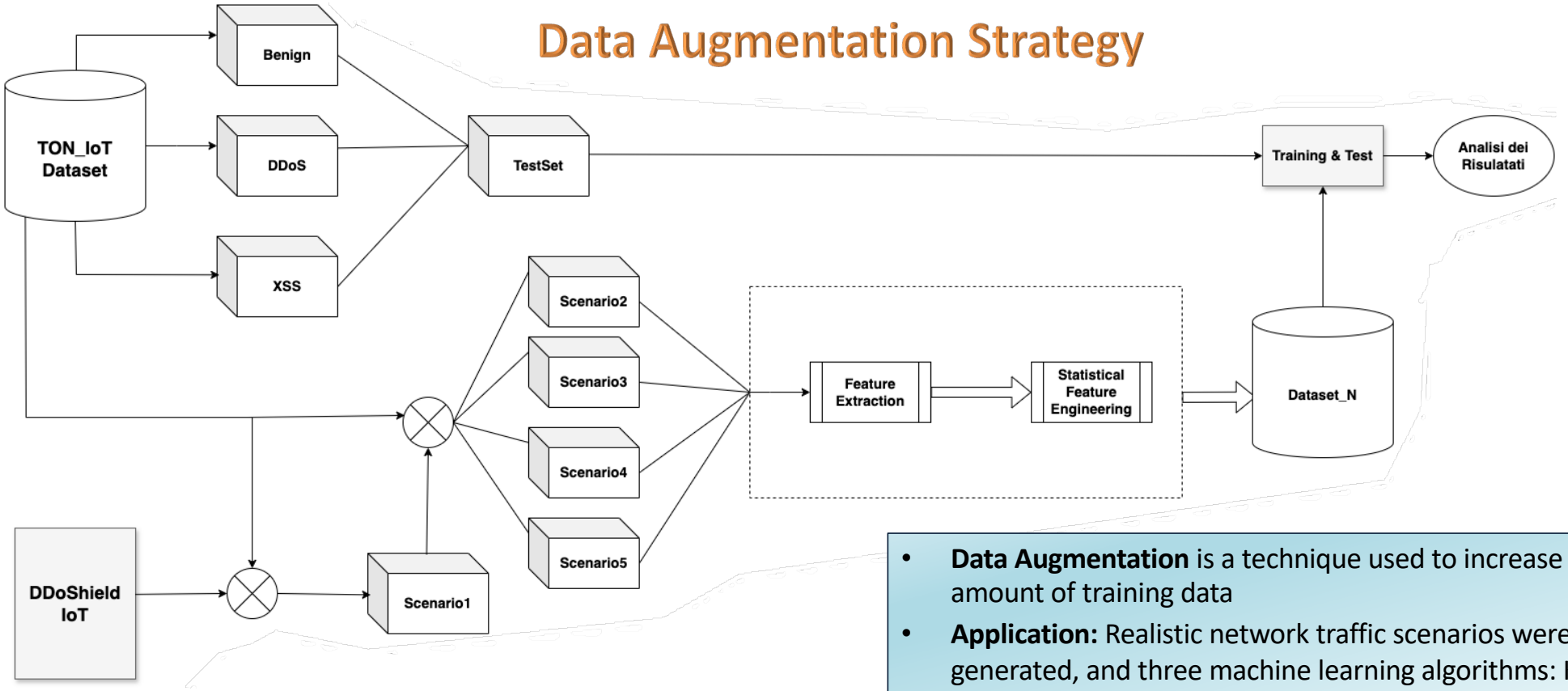
Model	CPU (% of usage)	Memory (Kb)	Model Size (Kb)
RF	**65.46**	98.07	712.30
K-Means	67.88	**86.83**	**11.20**
CNN	65.94	275.85	736.30

PhD thesis Discussion



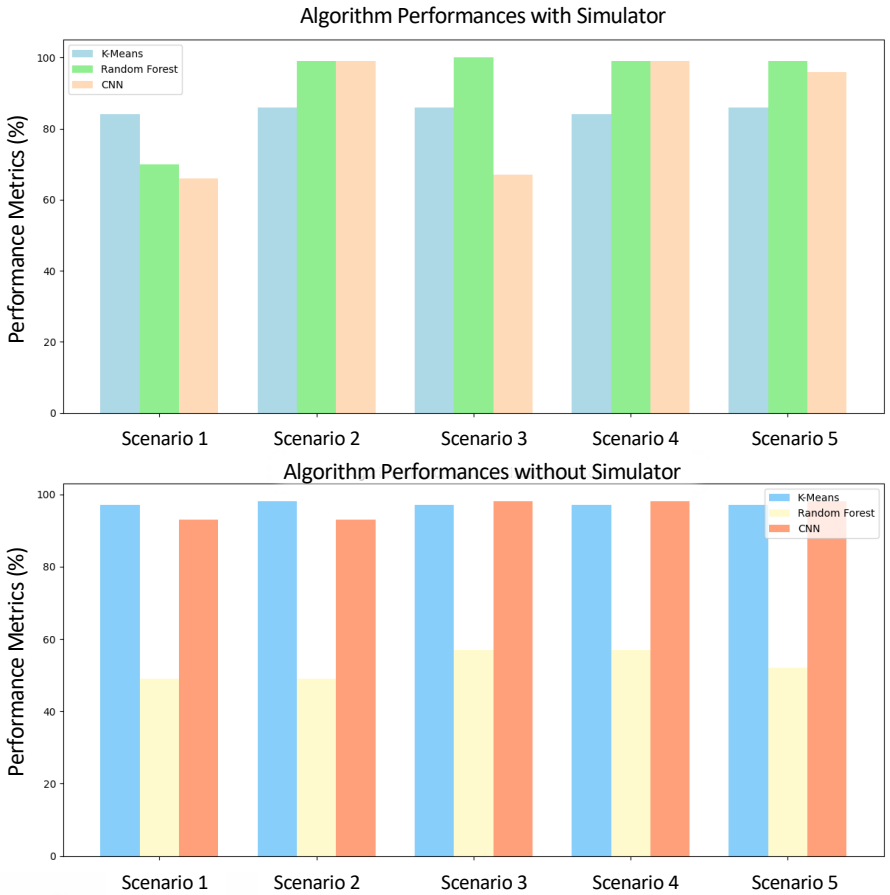
PhD thesis Contribution

Data Augmentation Strategy



- **Data Augmentation** is a technique used to increase the amount of training data
- **Application:** Realistic network traffic scenarios were generated, and three machine learning algorithms: K-Means, RF, and CNN, were trained on this data.

PhD thesis Results



DA technique with DDoShield-IoT data integration improved ML algorithm performance detection.

- RF achieved near-perfect performance, demonstrating its sensitivity to balanced datasets.
- CNN excelled in complex datasets, showing higher Recall and F1 scores.

Improved Performance

The simulator balanced datasets effectively, improving the detection of rare attack classes, while models without augmentation struggled with minority class detection.

Reduced Dataset Imbalance Impact

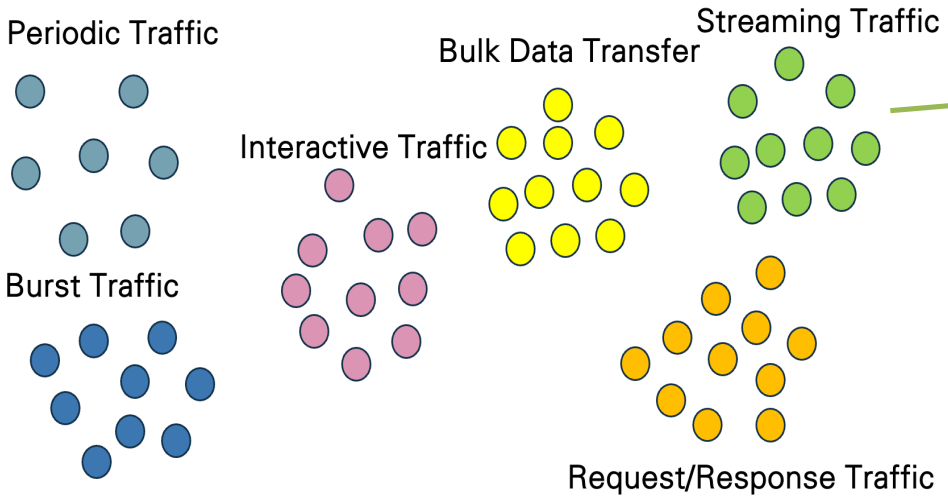
K-Means clustering remained stable across scenarios, indicating its effectiveness without augmented data.

K-Means Independence

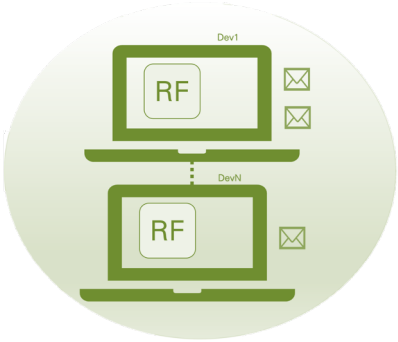
The DDoShield-IoT simulator shows strong potential for improving IDS performance, especially for models like RF and CNN, enhancing robustness in imbalanced IoT environments.

PhD thesis Contribution

This Thesis contribution aim at face scalability, real time monitoring, autonomous IDS, privacy concerns by propose a Two-Phase FL-based IDS, that leverages User Profiling technique at preprocessing phase.



User Profiling



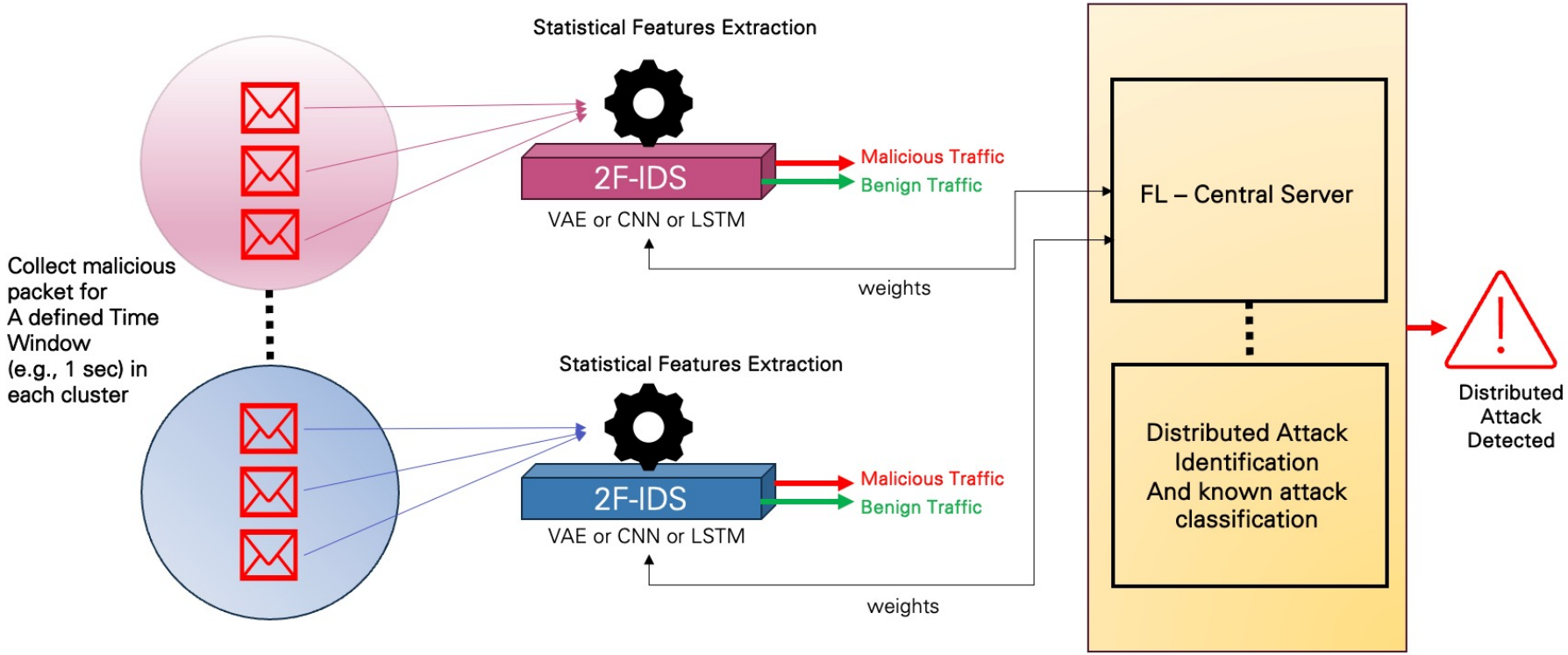
- In each device → IDS First Phase
- RF uses each packet raw features to decide if it is anomalous or benign
- Malicious packet are sent to IDS Phase 2

NOTE: Randomly a small portion of benign packet will be sent to IDS phase 2 to be sure there are no false negatives

PhD thesis Contribution

NOTE: In phase two, packets marked as malicious in phase one are re-evaluated. If the combined weight exceeds a threshold, the packet is confirmed as malicious.

Intrusion Detection Phase 2



PhD thesis Contribution

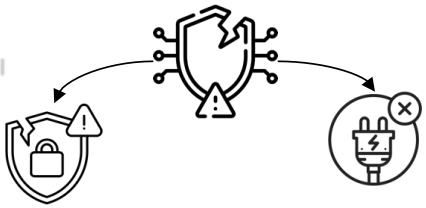
CyberSEAS Project

Problem

Improve the security of **Smart Grids**

Security Challenges

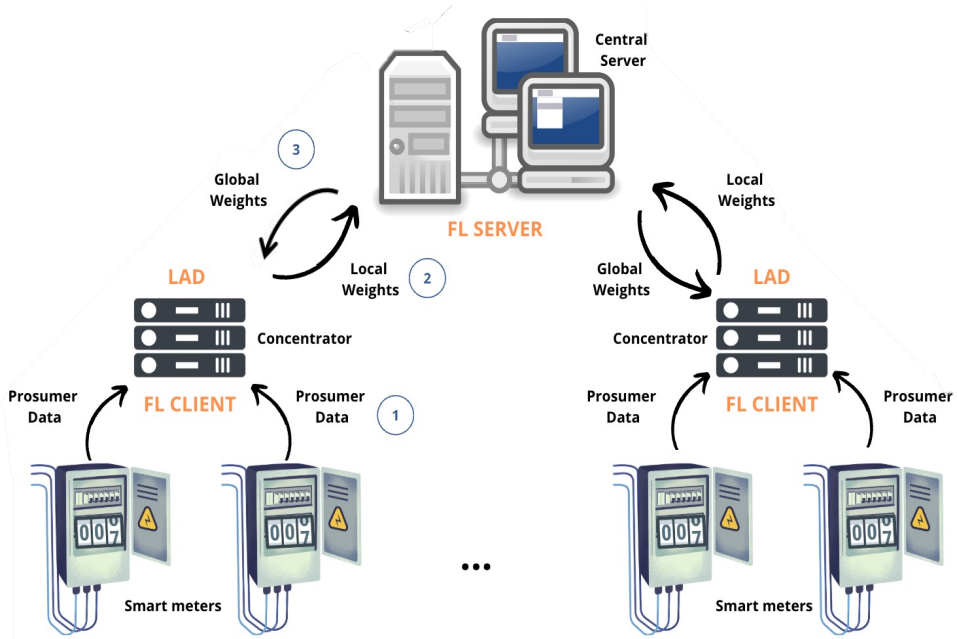
Exposure to Cyber Threats



Compromise of **privacy**

Interruption of services

Federated Learning and User Profiling based Intrusion Detection System (IDS)



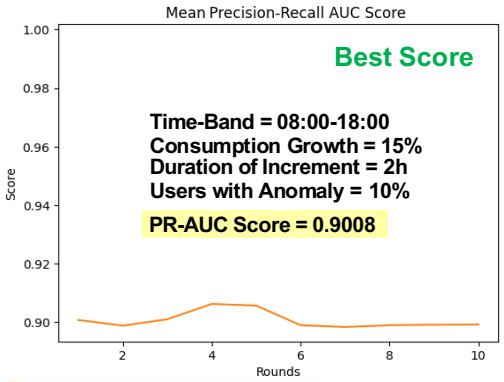
FL BASED IDS

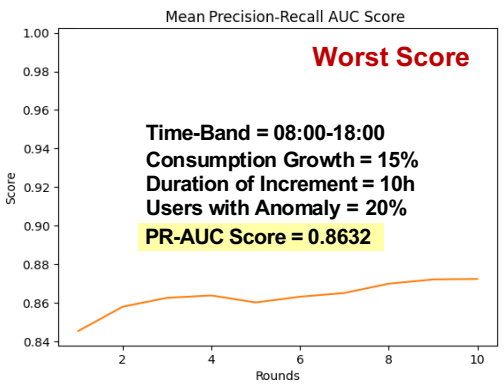
- **LADs** collect data from smart meters and train a model on it.
- The **central server** receives the model parameters and updates them to improve accuracy.

PhD thesis Results

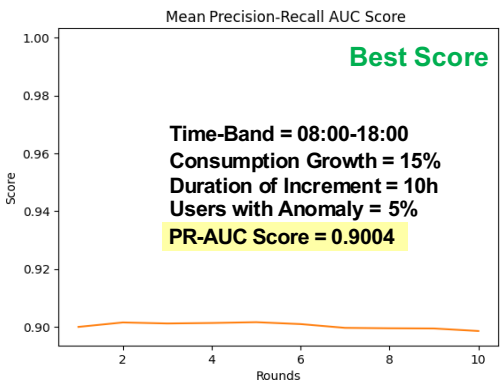
	Better performance	Slight degradation
Accuracy	Both FedAvg and FedYogi **are effective** with PR-AUC scores between 0.8632 and 0.9047.	
Time Band	At night.	During daytime.
Consumption Growth	With higher increments	With small increments.
Duration of Increment	With longer time windows.	With shorter time windows.
Users with Anomaly	With few abnormal users.	As they increase.

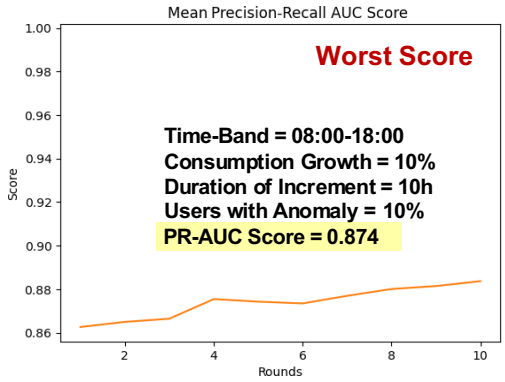
- **Scalability and Applicability**
  Applicable to real scenarios without the need for extended labelled datasets.
- **Accuracy**
  Combination of K-Means Clustering and Variational Autoencoder reduces false positives.
- **Privacy and Data Security**
  FL maintains local data during training without sharing them with a central server.





FedYogi





FedAvg

PhD thesis Conclusion

- This thesis tackled key challenges associated with securing IoT environments, with a particular focus on energy efficiency, scalability, and privacy.
- The goal was to design sustainable and adaptive Intrusion Detection Systems (IDS) tailored to the resource-constrained nature of IoT devices.
- To this purpose, four contributions were proposed, positioned in the fields of IoT cybersecurity, Green AI, and Federated Learning.