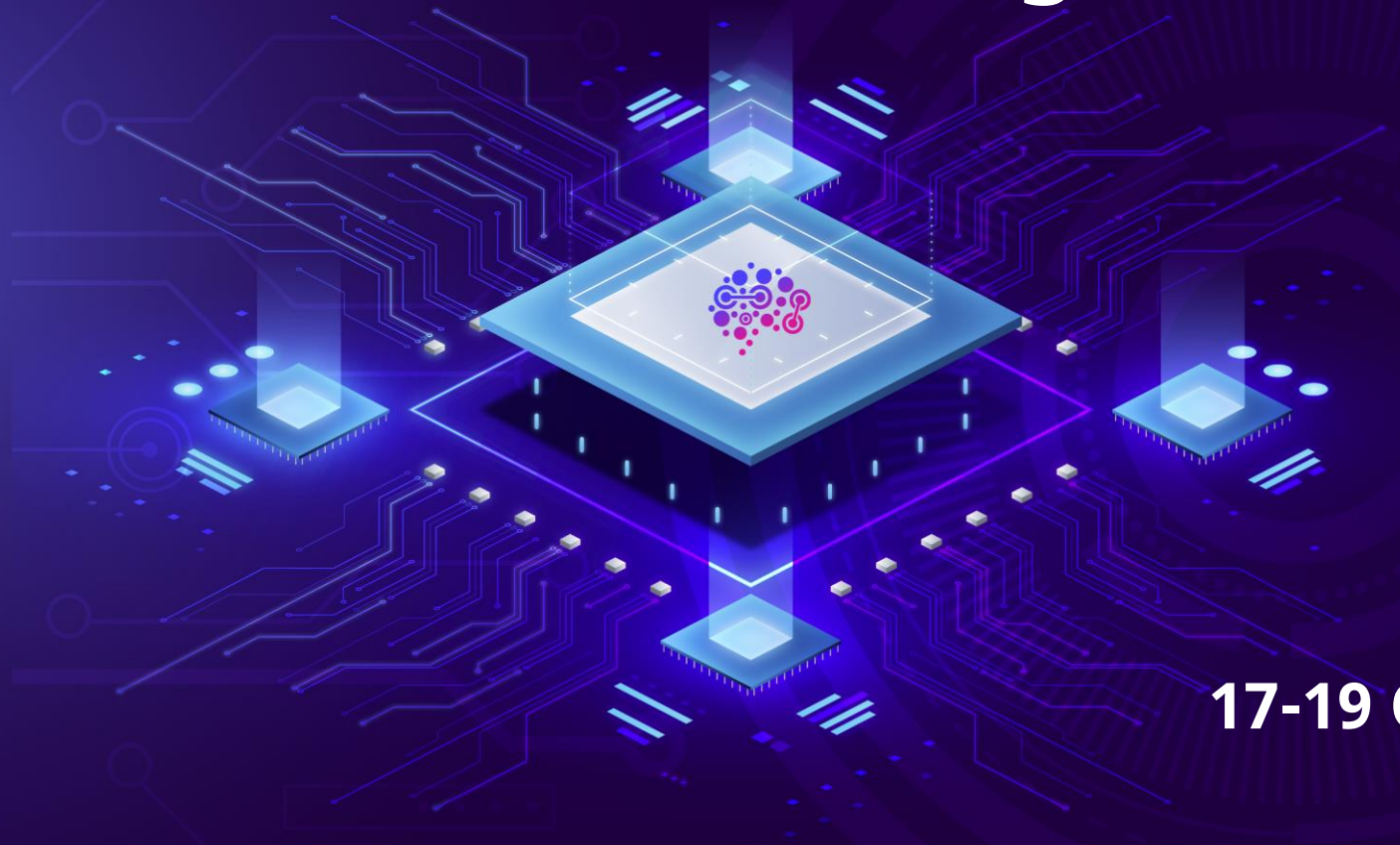
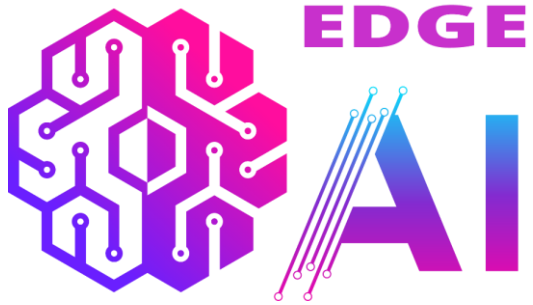
European Conference on EDGE AI Technologies and Applications - EEAI



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



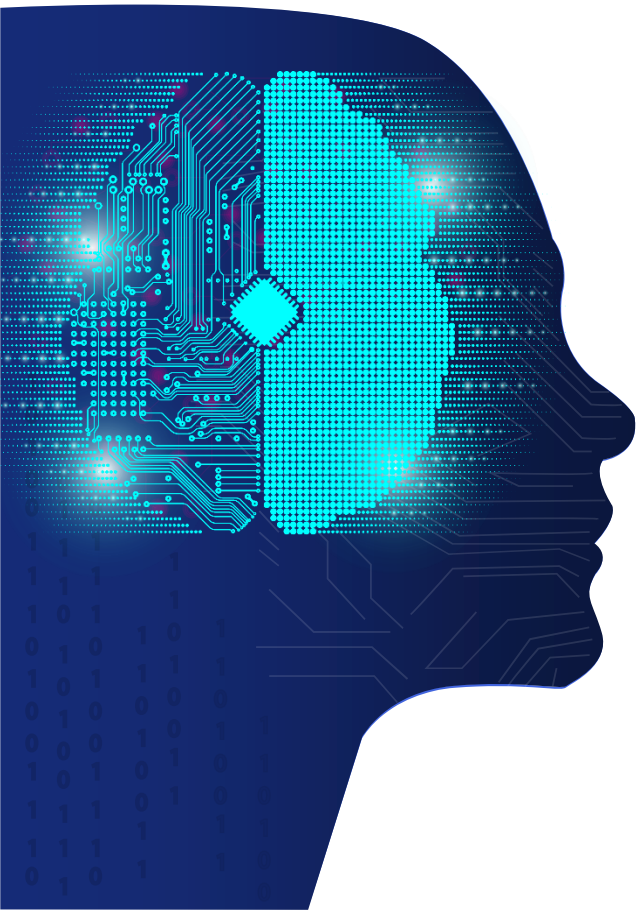
Federated Learning in Cybersecurity

Dimitrios Serpanos, CTI & University of Patras, Greece
Georgios Xenos, CTI & University of Patras, Greece

17-19 October 2023 Athens, Greece

Copyright © 2023

Presentation Outline



- Introduction
- State-of-the-art
- Research Goal
- Design and Implementation
- Experimental Results
- Conclusion

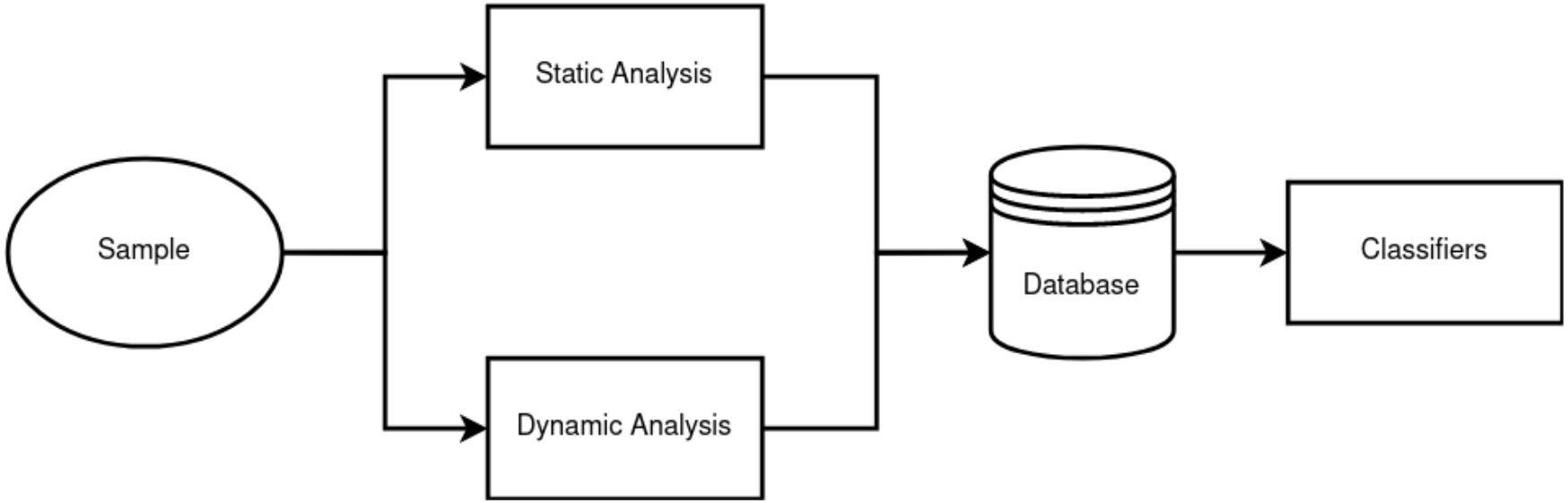
Copyright © 2023

Introduction

- Increasing cyberattack incidents in recent years
- ML-based malware detection systems require large amounts of training data
- Privacy and intellectual property restrictions limit data sharing
- Heterogeneous edge systems: Devices with different data availability and computing power
- Federated Learning (FL) enables the distributed building of detection models without source data exchange
- FL-based malware detection solution, where a detection model is developed employing FL in a cross-silo configuration

Copyright © 2023

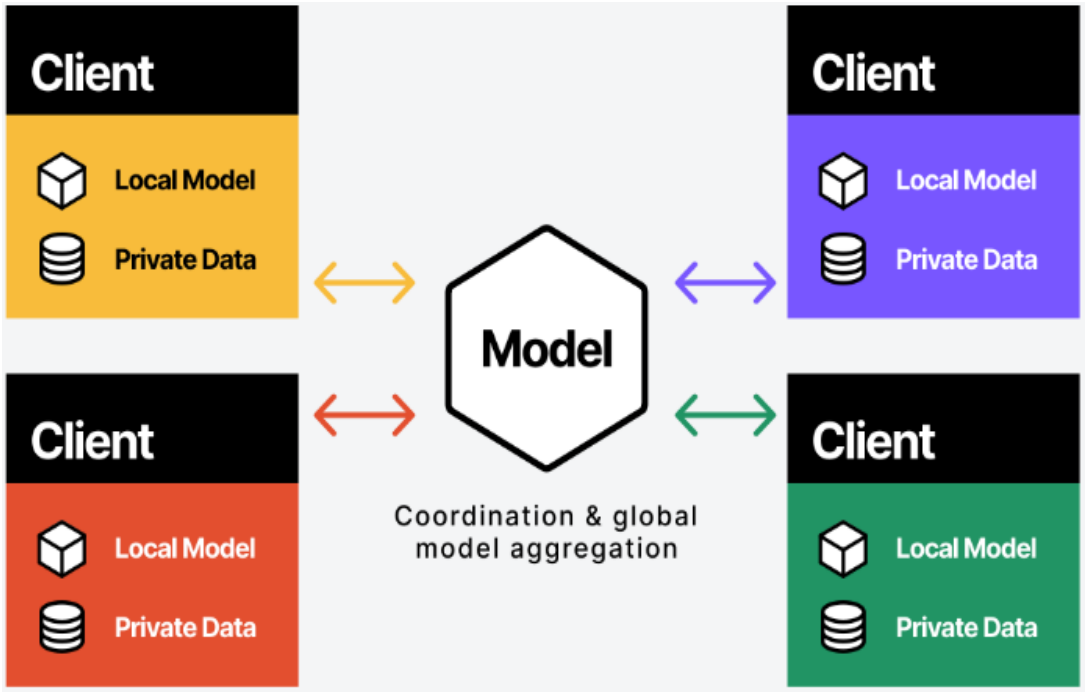
Introduction: Malware analysis and detection



Drawing from D. Serpanos, P. Michalopoulos, G. Xenos, and V. Ieronymakis, "Sisyfos: A Modular and Extendable Open Malware Analysis Platform," Applied Sciences, vol. 11, no. 7, p. 2980, Mar. 2021

Copyright © 2023

Introduction: Federated learning



Drawing from Scaleout: www.scaleoutsystems.com

- Multiple clients collaboratively train a model under the coordination of a central server, without sharing their private training data
- A repetitive process with the following three steps is performed:
  - each client updates the model locally using only their own independent data, creating different local models
  - the central server collects all local models and aggregates them into an updated global model
  - the aggregated model is shared with all clients

Copyright © 2023

Introduction: FL configurations

- **Cross-device:** clients are a large number of IoT devices (or smartphones) with limited computational power and varying device availability
- **Cross-silo:** clients are different organizations (typically 2-100) with large datasets (named data silos) and computational capabilities and high availability

- **Horizontal FL:** different parties hold different samples over the same set of features
- **Vertical FL:** different parties hold different features over the same set of samples

Copyright © 2023

State-of-the-art

- In cybersecurity, FL is employed in several directions such as attack detection, privacy, trust management, authentication and other IoT related tasks
- In malware detection, efforts have focused on developing FL-based solutions for IoT and Android systems
- Previous works focus mainly in cross-device setups
- Little effort has been spent on FL-based malware detection, considering cross-silo configurations

Copyright © 2023

Research Goal

- Explore an FL-based malware detection system for a real world scenario
- Measure the accuracy of the system on malware detection using a benchmark dataset
- Explore how different configurations impact the effectiveness of the system
- Compare FL-based vs centralized learning for malware detection

Copyright © 2023

Design and Implementation

- **Scenario:** Multiple security systems participate in the training of a common malware detection system
- **Cross-silo configuration:** Small number of participants with large datasets
- **Training architecture:** Widely adopted 3-layer neural network used for training
- **Dataset:** EMBER v2
  - 2381 features extracted from static analysis of Windows PE files
  - 600.000 samples labeled as benign or malicious for training (0 or 1)
  - 200.000 samples for testing

Copyright © 2023

Design and Implementation

- **Training** occurs in the following steps:
  1. each client trains its own local model using the employed NN and its own private training data
  2. each client sends its resulting local model to the centralized server
  3. the server aggregates all local models into a global one
  4. the server transmits the global model to all clients.

- When training is completed, at detection mode, all clients receive a copy of the aggregated model from the server (No federation)

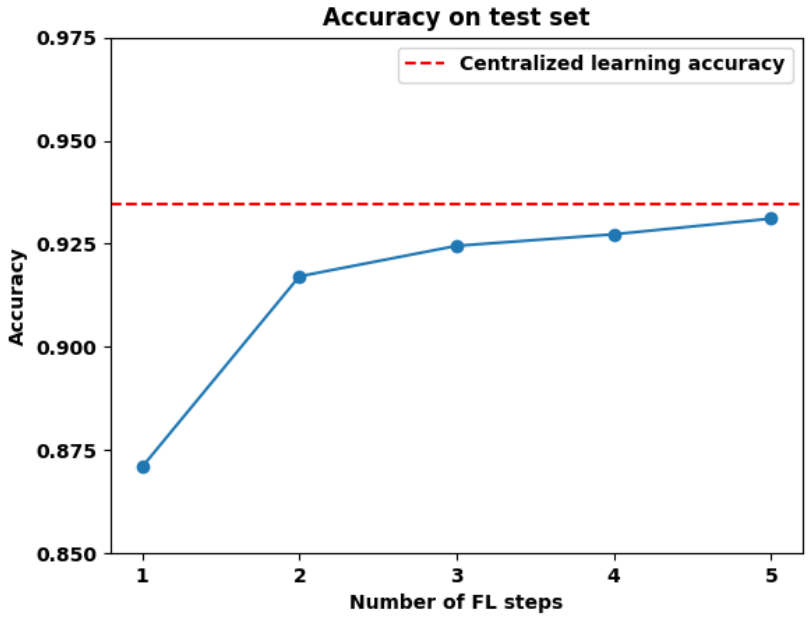
Copyright © 2023

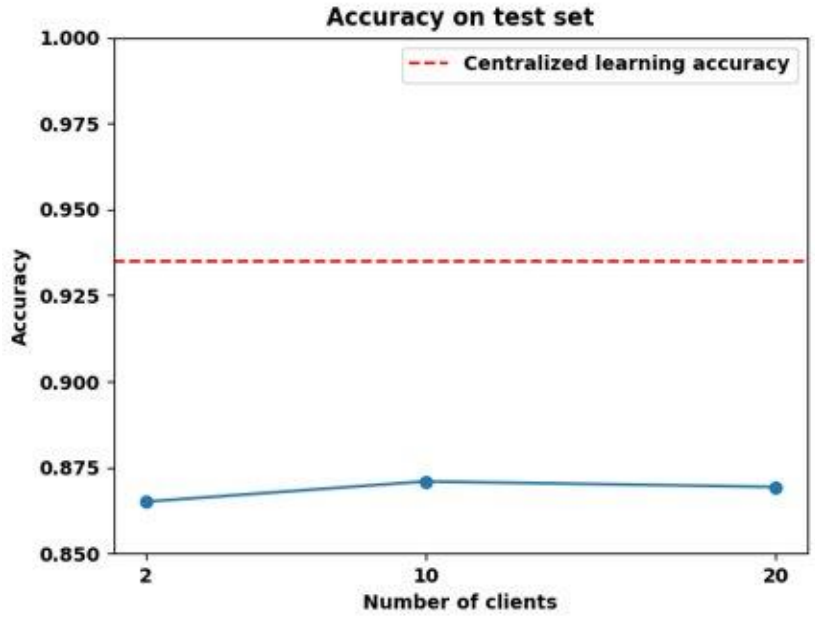
Design and Implementation

- Experiments are made for different steps of learning
- A range of different client populations is considered
- Different dataset sizes with variable percentages of common data (overlap) between participants; i.e. x=5 indicates 5% common data in the client datasets to simulate real-world scenarios
- Centralized model developed uses the same architecture as the FL model
- Experiments using the centralized model with different dataset sizes
- For all experiments we measure the detection accuracy on the benchmark test set

Copyright © 2023

Experimental Results

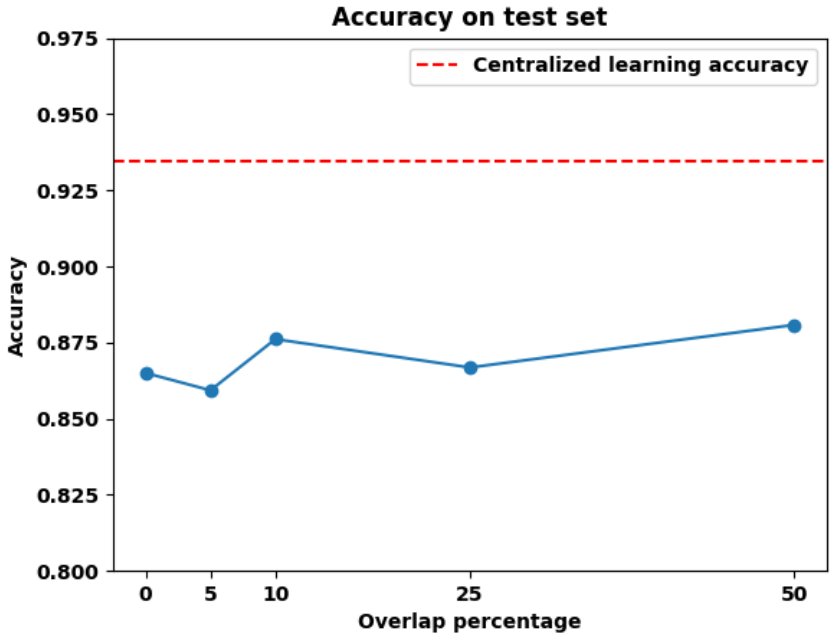


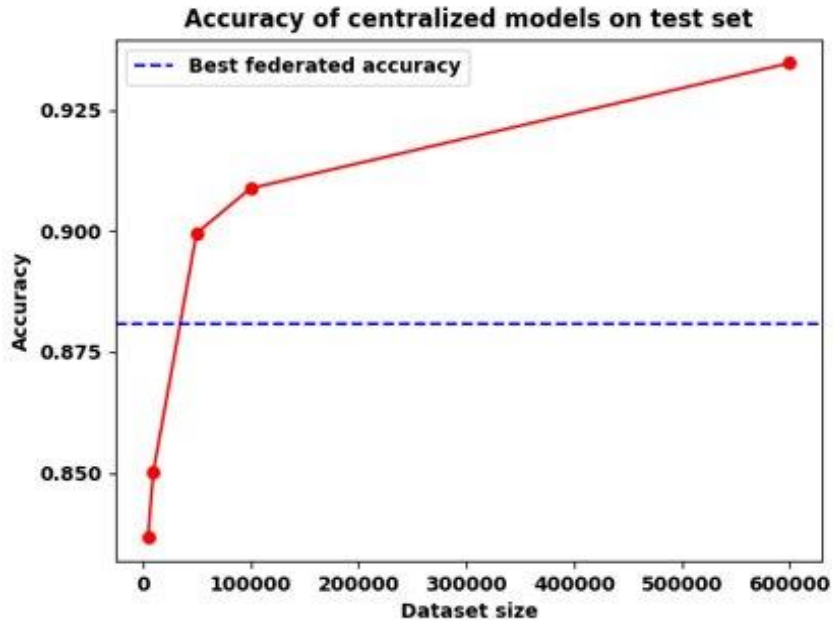


- With increased number of training steps, FL environments achieve the same accuracy, relative to the centralized case
- Accuracy is effectively independent of the number of clients in the cross-silo configuration

Copyright © 2023

Experimental Results





- Overlap up to 50% doesn't seem to impact the observed accuracy of the system
- In centralized scenarios, when the available dataset is smaller, accuracy is lower compared to that of FL, illustrating the main incentive for participants

Copyright © 2023

Conclusion

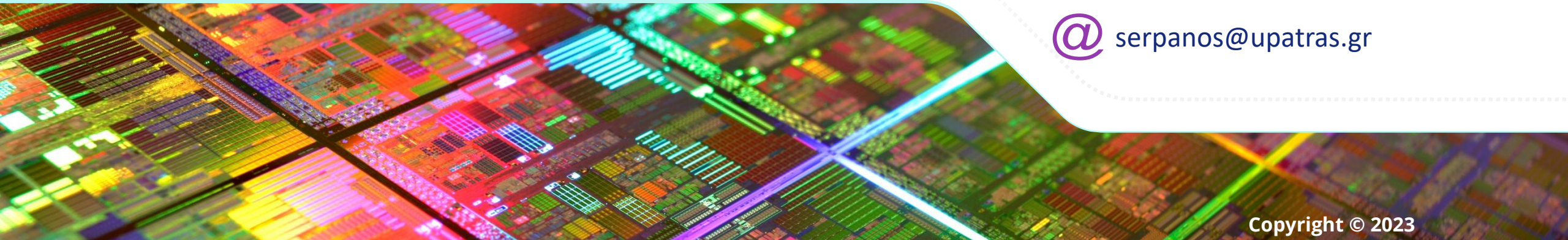
- Federated learning provides significant advantages in malware detection enabling the training of detection models by multiple, distributed participants without exchanging sample data
- Large configurations with an increased number of training steps, FL environments achieve the same accuracy, relative to the centralized case
- **Most important advantage of FL**: all participants achieve high accuracy, even those who do not have sufficiently large training datasets to achieve high detection

Copyright © 2023

EDGE AI

Thank You

For your attention



@ serpanos@upatras.gr

Copyright © 2023