Francesco Caputo

Smart and Secure Low-power transducer network

Tutor: Pasquale Arpaia

Cycle: 37 Year: 2024

Outline

1. My Background
2. Research field of interest and study activities
3. Research activity
    1. Embedded Artificial Intelligence
    2. Cyber-physical Attacks on Embedded Devices
4. Future activities

My background

- MSc degree: Electronic Engineering (University of Naples “Federico II”)
- Research group/laboratory: ARHeMLab
- PhD start date: 01/01/2022
- Scholarship type: MUR PON – Green action
- Industry period: 12 months, STMicroelectronics, Marcianise, Italy
- Abroad period: 6 months, CSLab, STMicroelectronics Rousset, France (by remote)

Research field of interest

- Metrological approach for cybersecurity in Smart Industry

Smart Agriculture

Smart Building

Smart Home

Smart Vehicle

Smart Factory

Smart Health

Research field of interest

PRODUCTION OF DATA

Transducers, Edge Technologies, Connection Standards, Connection Protocols

ELABORATION OF DATA

Cloud computing, Edge Computing, Tiny Computing

SUSTAINABILITY

Energy Impact, Disposal

SECURITY

Data transmission, Cryptography, Denial of Service, Cyberattacks

Summary of study activities

1

EMBEDDED ARTIFICIAL INTELLIGENCE

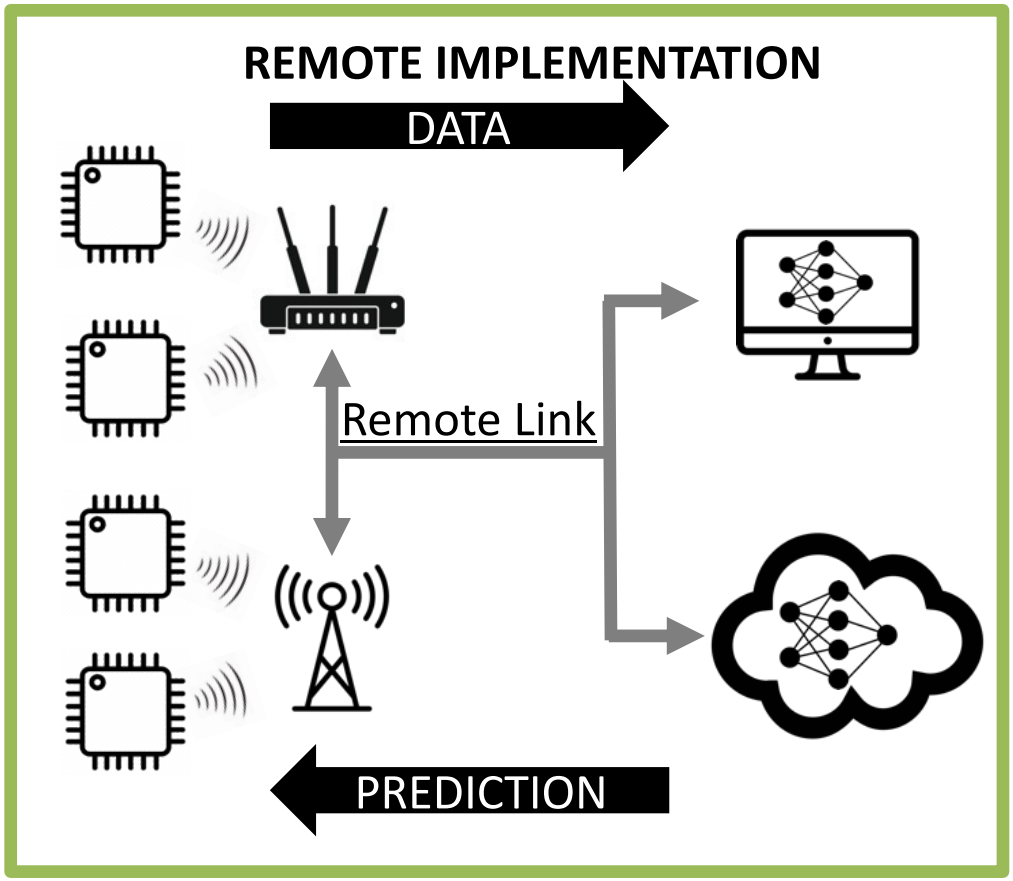
- Time and Energy performance metrics
- Optimization techniques
- Assessment measure setups
- Uncertainty estimation

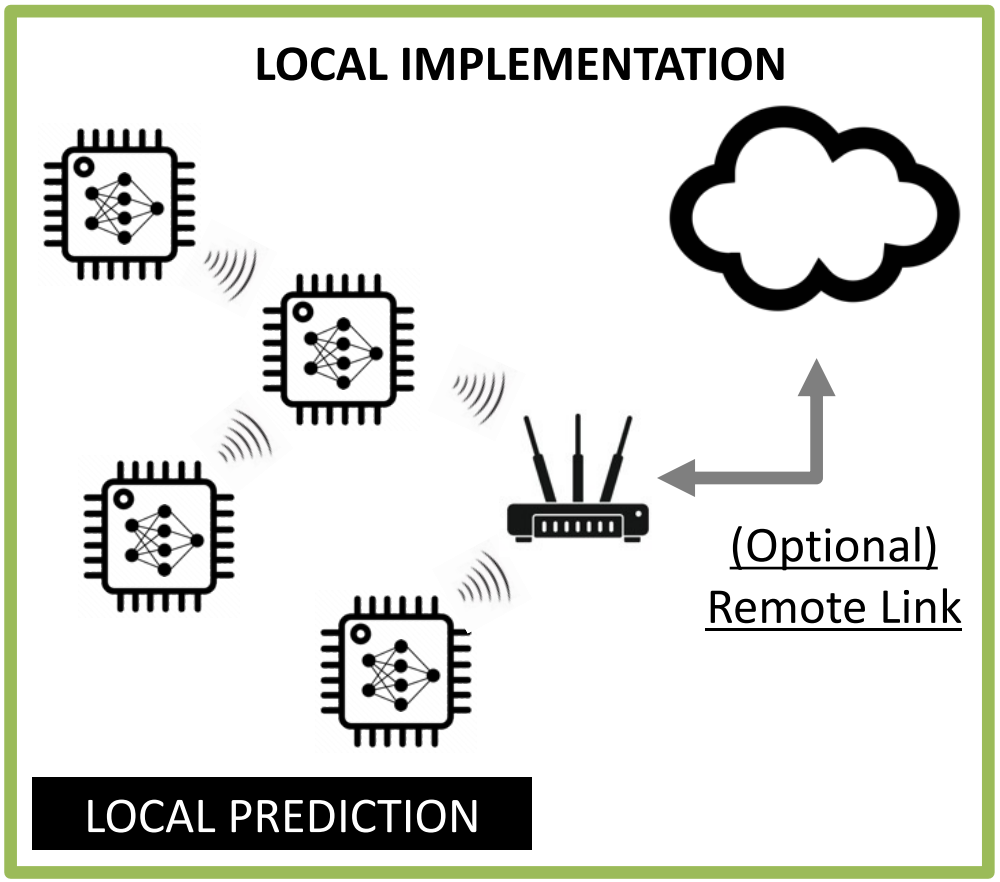
2

METROLOGY FOR CYBERATTACKS ON EMBEDDED DEVICES

- Side-Channel Attacks
- Machine learning techniques applied to Side-Channel
- Uncertainty estimation on such attacks

Embedded AI

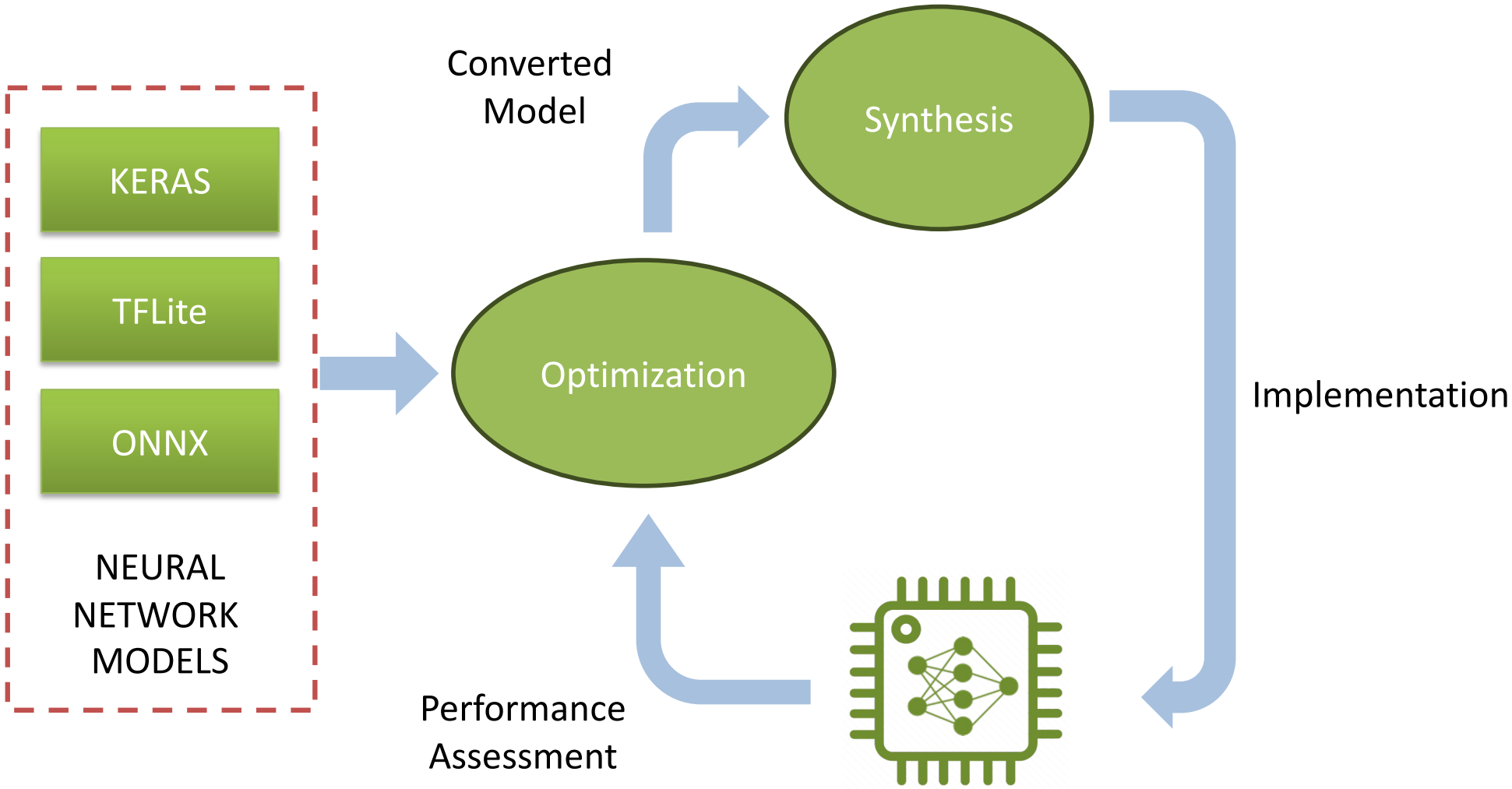

REMOTE IMPLEMENTATION
DATA
Remote Link
PREDICTION


LOCAL IMPLEMENTATION
(Optional)
Remote Link
LOCAL PREDICTION

Embedded AI

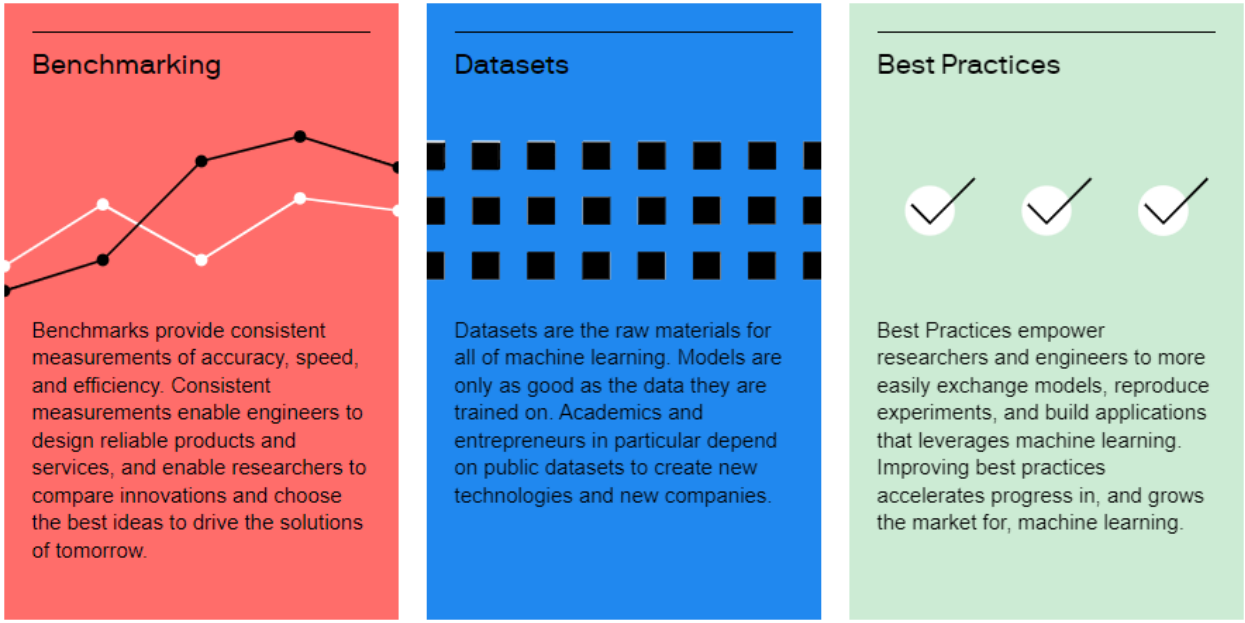
- Advantages
  - **Offline Elaboration**: A denial of remote service or no active network does not affect the functionality of the device
  - **Security & Safety**: Data stays on device and cannot be stolen or changed in transmission
  - **Economical & Green**: Remote computing is not needed
- Disadvantages
  - **Hardware**: Small amount of hardware resources and battery supplied
  - **Overheating**
- Challenges
  - **Timing Performance**
  - **Power Performance**

Embedded AI

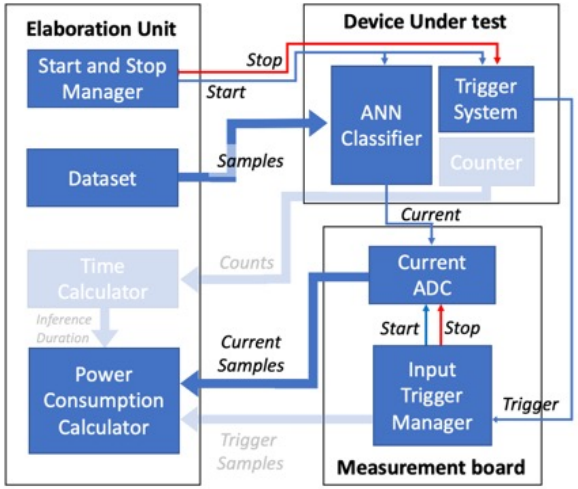

KERAS
TFLite
ONNX
NEURAL NETWORK MODELS
Converted Model
Optimization
Synthesis
Implementation
Performance Assessment

Embedded AI – MLCommons

MLCommons is an Artificial Intelligence engineering consortium, built on a philosophy of open collaboration to improve AI systems.
Through its collective engineering efforts with industry and academia it continually measures and improves the accuracy, safety, speed and efficiency of AI technologies, including tiny devices.



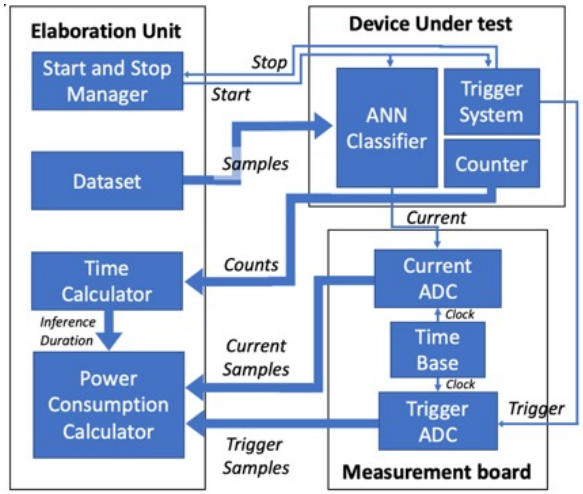
Embedded AI – MLCommons method



- The ***DUT*** hosting (i) a *Classifier* (an artificial neural network ANN) that executes N inferences in a certain inference time, (ii) a *Counter* for measuring the inference time, and (iii) a *General-Purpose Input-Output* transmitting a trigger signal to the measurement board.
- The **measurement board** hosting (i) an Ammeter that measures DUT current consumption, and (ii) a timestamp manager that receives measurement events from DUT
- The **elaboration unit** (a PC) hosting (i) datasets and ANNs used by the DUT to run inferences, and (ii) a measure program that collects the data from DUT and measurement board

Problem: between cycles are present some time window where inferences are not running. These can produce underestimation of power consumption.

Embedded AI – Improved method



There are two main changes:

- The trigger is not a simple pulse, but it is a reference signal that allows to segment the inference phase.
- The ammeter returns a vector with the current samples measured over all the inference run
- The trigger reference signal and the current consumption are sampled with the same time base

Benchmarking procedure measures the average inference time and power consumption over N classifications inference cycles.

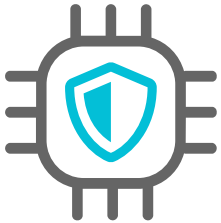
Each cycle is characterized by two phases:

- *pre-inference*, where the DUT prepares data into its memory to be inferenced by the ANN model
- *Inference*, where data are effectively processed by the ANN running on the DUT.

Embedded AI - Comparison

MLCommons Method	Proposed Method
Timing performance assessed as mean	Timing performance assessed as mean time on N inference cycles
Energy performance assessed as mean power consumption on a measure window that cover N inference cycles	Energy performance assessed as mean power consumption on N measure windows
The two measures are made in different time	The two measures are made in same time
The uncertainty can be assessed only on the timing performance	The uncertainty can be assessed on both measures

Cyber-physical Attacks

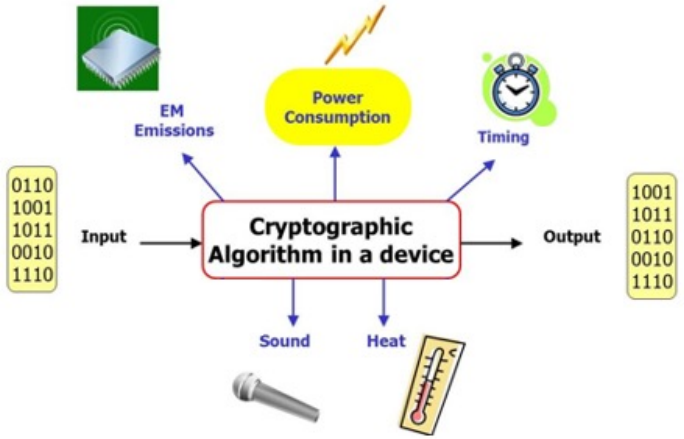


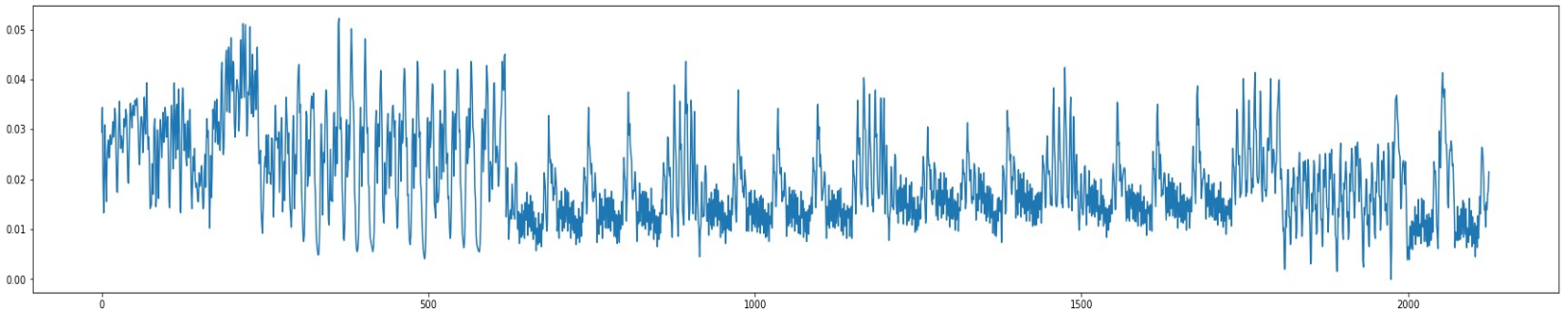
A **Secure Element** is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities

An **attack** is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission

Side-Channel Attacks

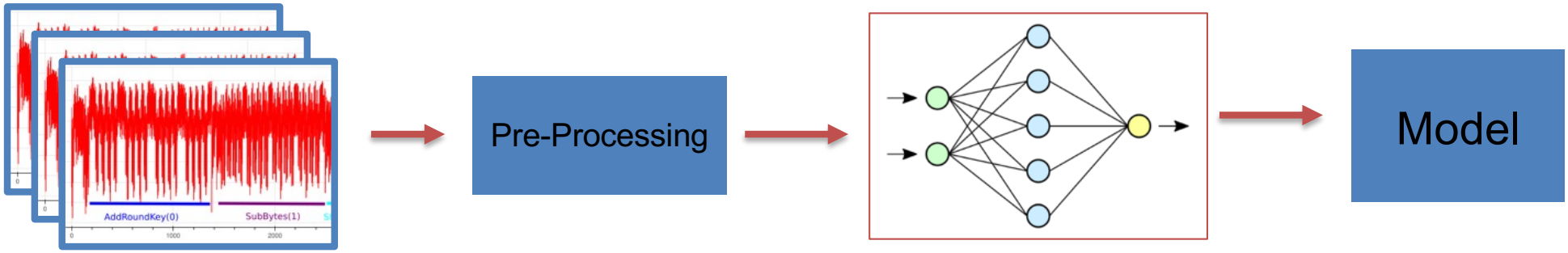
A **Side-Channel Attack** is a non-invasive attack aimed at extracting information that a particular system can exhibit



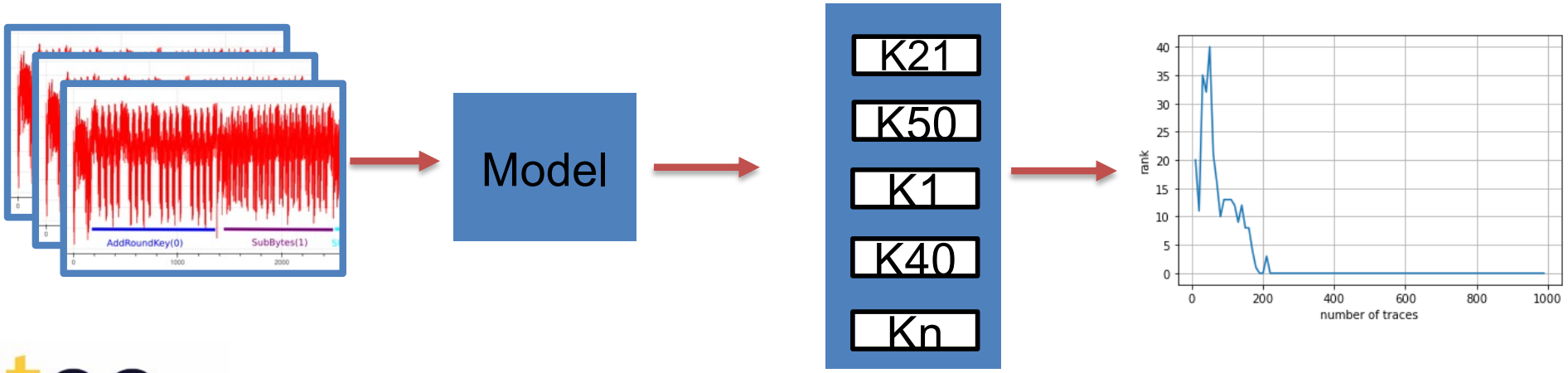


Side-Channel Attacks – ML Approach

Traces are pre-processed and used to Train the attack model



The model is used to attack the device and a rank was estimated



Products

[P1]	*P. Arpaia, F. Caputo, A. Cioffi, A. Esposito, F. Isgrò,* ***Uncertainty analysis in cryptographic key recovery for machine learning-based power measurements attacks****, IEEE Transactions for Instrumentation and Measurements (submitted), 2022*
[P2]	*IEEE International Conference On Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering in Milan, presenting a demo about* ***Side-Channel Attacks using Machine Learning models****, 2023*
[P3]	P.Arpaia, F.Caputo, A.Cioffi, A.Esposito, ***The role of metrology in the cyber-security of embedded devices***, Acta IMEKO, 2023
[P4]	P.Arpaia, L.Capobianco, F.Caputo, A.Cioffi, A.Esposito, F. Isgrò, N. Moccaldi, D. Pau, D. Siorpaes, E. Toscano, ***Accurate Energy Measurements for TinyML Workloads***, TinyML Summit, 2024
[P5]	P.Arpaia, L.Capobianco, F.Caputo, A.Cioffi, A.Esposito, F. Isgrò, N. Moccaldi, D. Pau, D. Siorpaes, E. Toscano, ***Accurate Energy Measurements for TinyML Workloads***, IEEE MetroXRAINE, St.Alban 2024
[P6]	P.Arpaia, L.Capobianco, F.Caputo, A.Cioffi, A.Esposito, F. Isgrò, N. Moccaldi, D. Pau, D. Siorpaes, E. Toscano, ***Toward a standardized assessment of microcontroller performance in embedded AI***, 2025

Future Activities

- Research on other types of attacks like side-channels that can be measured
- Build of a dataset of cyber-physical attacks like Side-Channel or Fault attacks
- Build a neural model that can predict such attacks from a real time monitoring
- Embed the model and optimize it to work on edge device to build a secure smart network