IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Real-time AI Based Power Assisted Malware Predictor

Supervisors:

*Yehya Nasser, **Mohammed Nassar, *Marc-Oliver Pahl, and *Samir Saoudi.

* IMT ATLANTIQUE
** University of New Haven

PhD Student:

Mohammed Mezaouli

Planning

- **Context**
- State of the art
- PhD Objective
- Methodology And Results

Context

- Industry 4.0 is based on connected computers to make decisions using AI, ML. Those industries may be affected by malware. Those Malware can cause data loses, decreasing productivity or causing financial loses. Malware can also cause disaster if it impacts the nuclear, water treatment industries.

- Malware is a harmful software, which can access (corrupt/ change) to important information such as:
  1. Personal
  2. Financial
  3. Corporate

Context

- Mirai Botnet:

  Description: One of the most infamous IoT malware, Mirai, turns networked devices running outdated versions of Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.

  Impact: In 2016, Mirai was responsible for some of the largest DDoS attacks, significantly disrupting internet services.

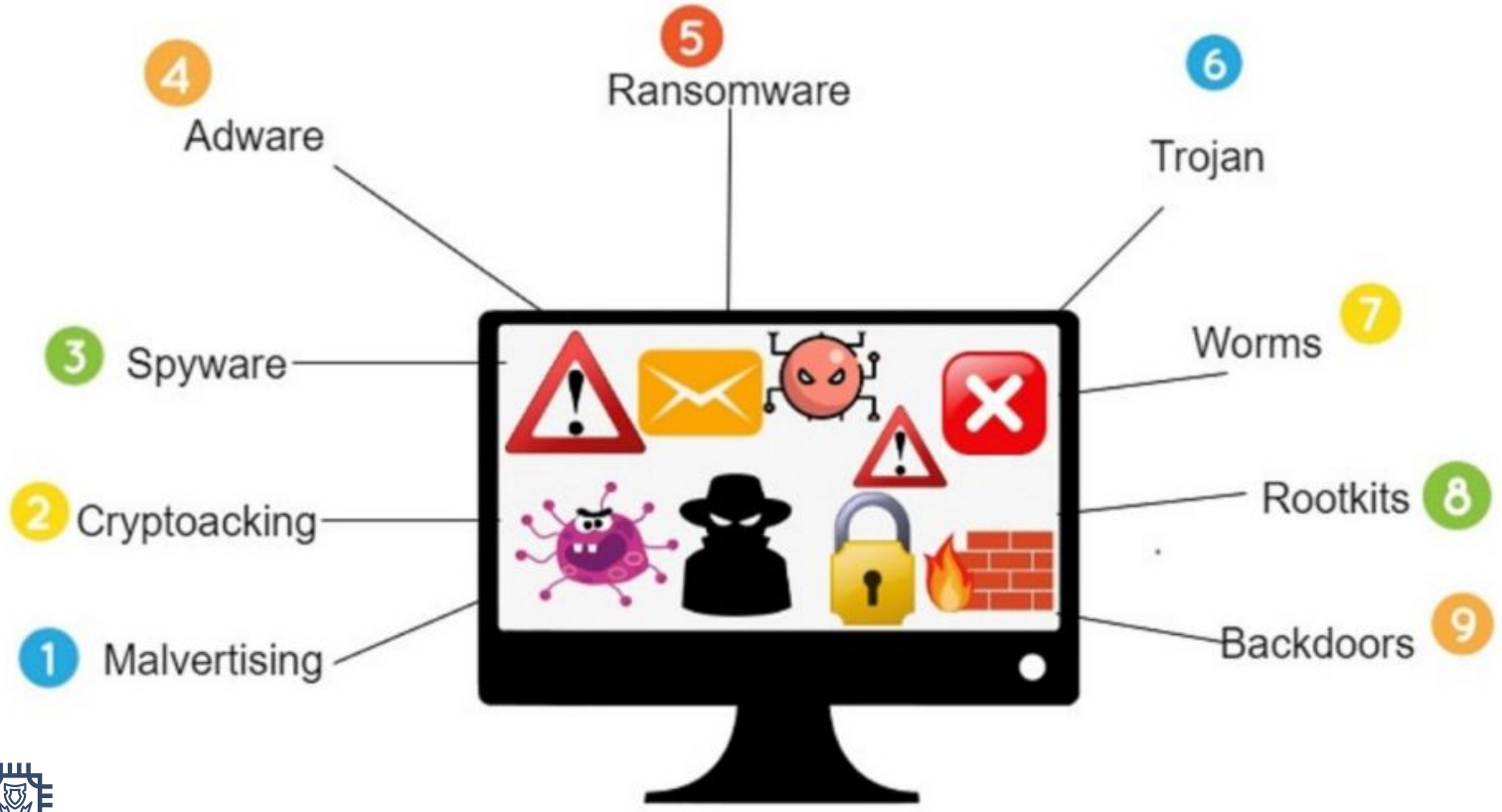
- Ransomware:

  Description: Ransomware targeting IoT devices can lock users out of their systems or devices until a ransom is paid.

  Impact: For instance, ransomware attacks on smart medical devices can have severe consequences, potentially endangering patients' lives.

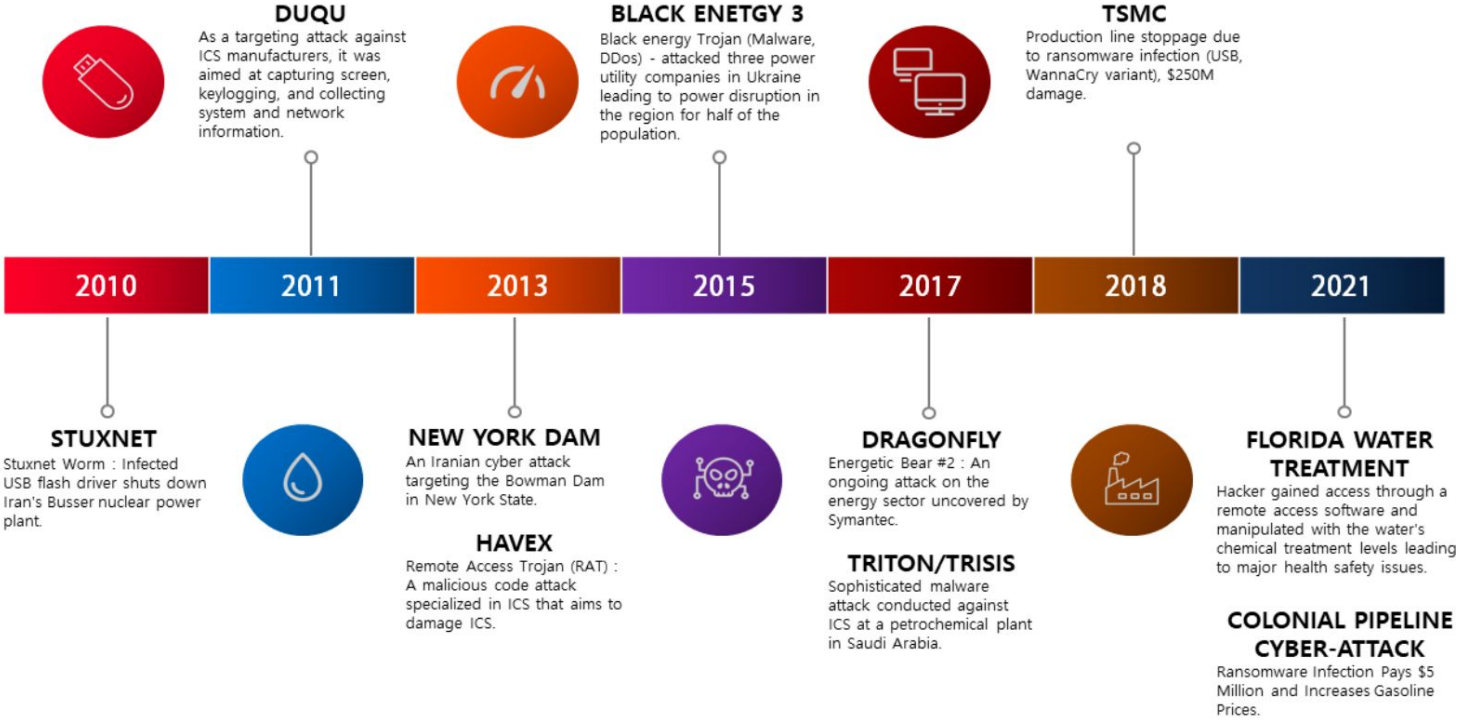
- Spyware
- Worms and Viruses

Malware Types[1]



[1] Akhtar, M.S.; Feng, T. "Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time". Symmetry,2022

Timeline of international industrial cyber attacks [1]



[1] Kim, "IIoT Malware Detection Using Edge Computing and Deep Learning for Cybersecurity in Smart Factories" , Applied Sciences, 2022

Planning

- Context
- **State of the art**
- PhD Objective
- Methodology And Results

Hardware Performance Counters [1]

Counter Name	Purpose
Cycle Counter	Increment after each CPU cycle
Load And Store Counter	Increment each time a load and store instruction is executed
Instruction Cycle Counter	Increment on each additional cycle required to execute a multi-cycle instruction
Exception Counter	Increments on each entry or return from an exception
Fold Instruction Counter	Increment on zero cycles instructions like If-Then and some NOPs
Sleep Counter	Increment on cycles associated with power saving mode

[1] "ARMv7-M Architecture Reference Manual" , C1.8.6, DWT Register Summary

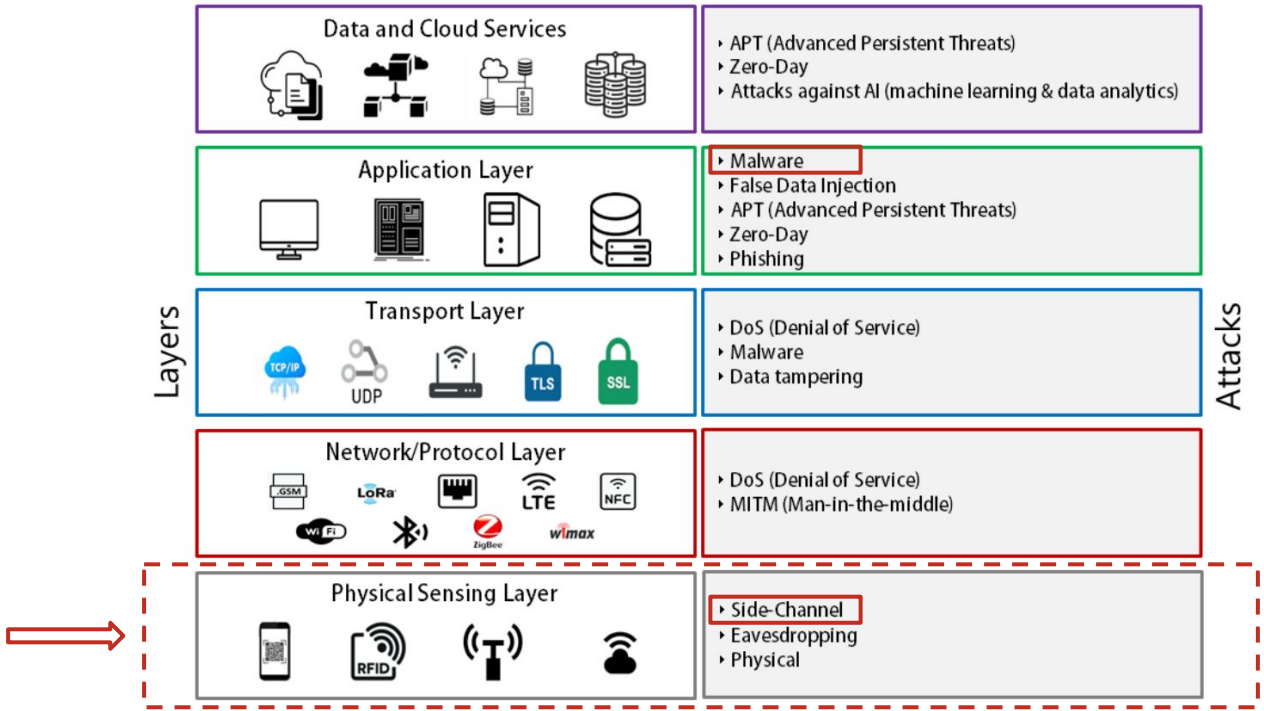
State of the art

Detection by	Paper name
HPC + AI + Hardware Architecture	Ozsoy, "**Hardware-Based Malware Detection Using Low-Level Architectural Features**". IEEE Transactions on Computers. 2016
HPC + AI	Zhou, "**Hardware Performance Counters Can Detect Malware: Myth or Fact?**". Association for Computing Machinery. 2018
	Sayadi, "**Customized Machine Learning-Based Hardware-Assisted Malware Detection in Embedded Devices**". IEEE International Conference On Trust. 2018
	Pan, "**Hardware-Assisted Malware Detection using Machine Learning**". Design, Automation & Test in Europe Conference & Exhibition (DATE). 2021
EM + AI	Pham, "**Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification**". Association for Computing Machinery. 2021
Power + AI	Hernandez Jimenez, "**Malware Detection Using Power Consumption and Network Traffic Data**". 2nd International Conference on Data Intelligence and Security (ICDIS). 2019

Malware Detection by Power Consumption [1]

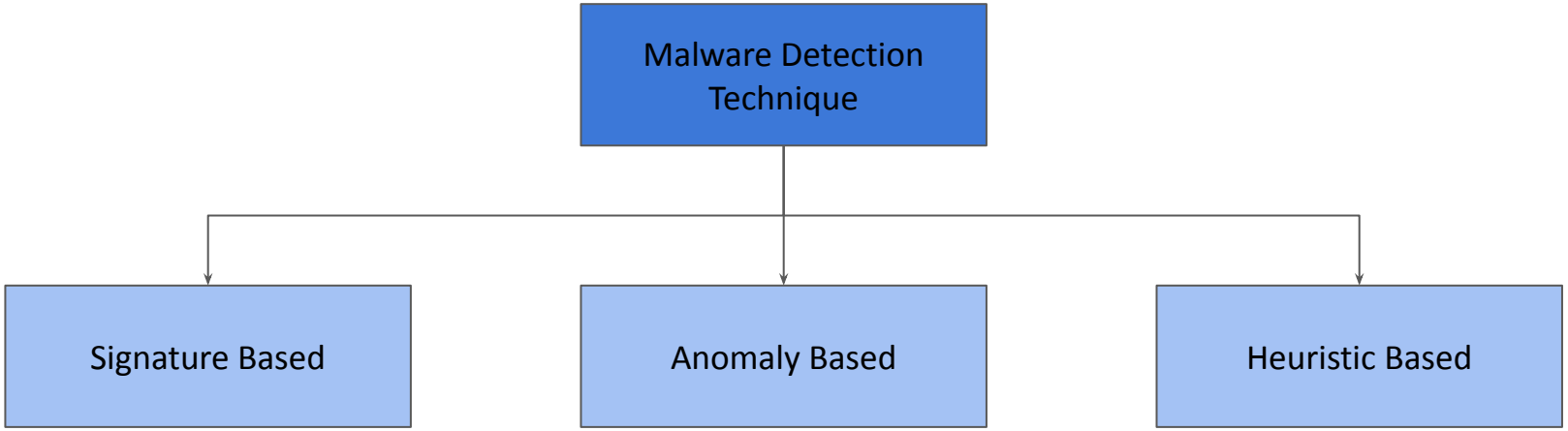
[1] Pham, “Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification”. Association for Computing Machinery. 2021

Smartfactory cyberattack structure diagram [1]



[1] Kim, "IIoT Malware Detection Using Edge Computing and Deep Learning for Cybersecurity in Smart Factories" , Applied Sciences, 2022

Malware detection Technique [1]

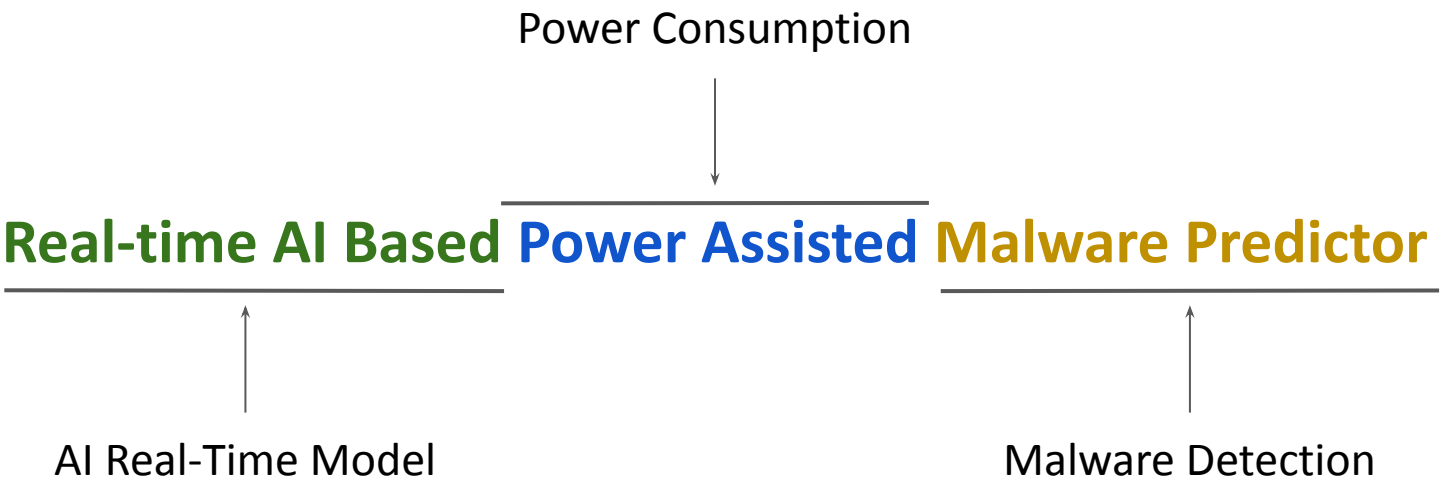


[1] Hossain Faruk ,"Malware Detection and Prevention using Artificial Intelligence Techniques", IEEE International Conference on Big Data (Big Data), 2021

Planning

- Context
- State of the art
- **PhD Objective**
- Methodology And Results

RAI-PAMP Project Objective



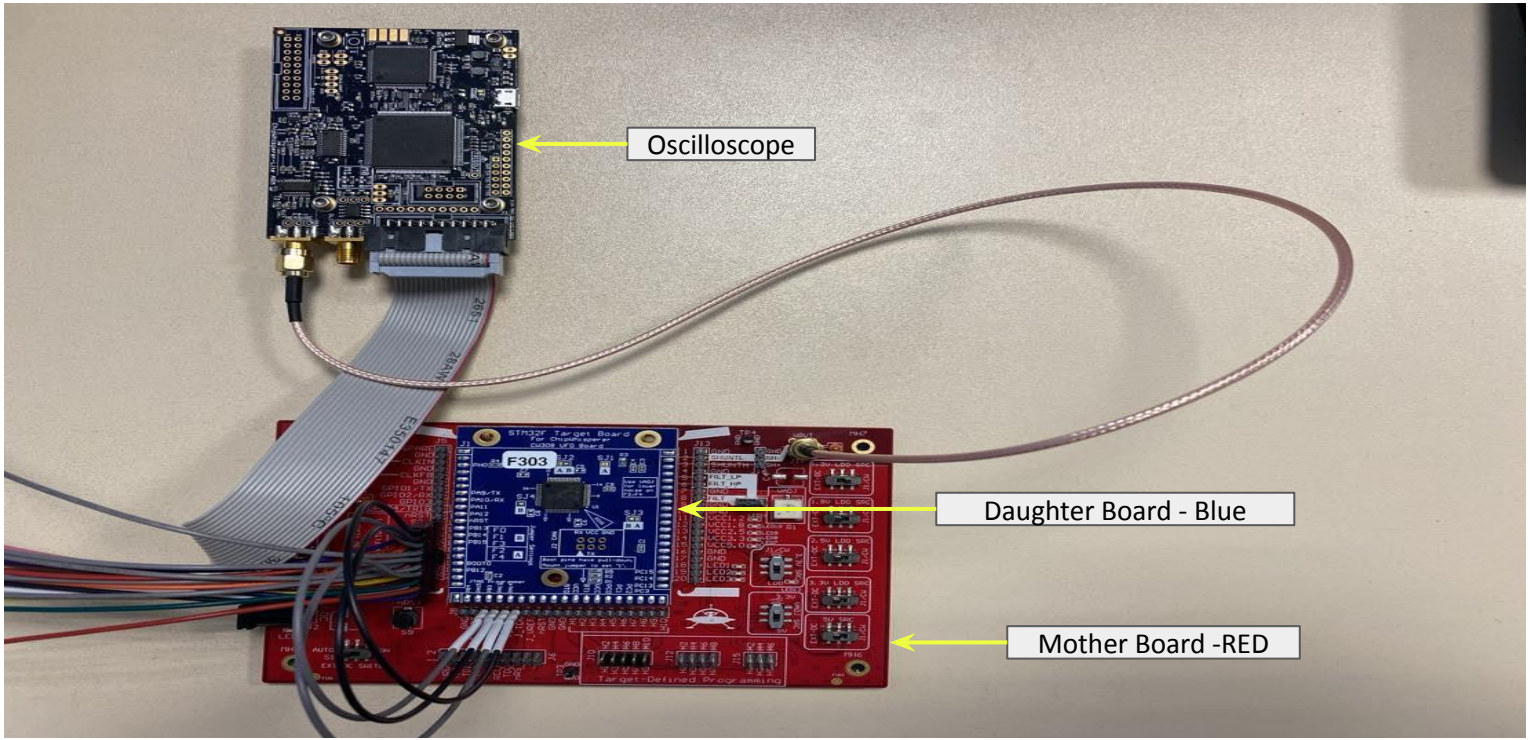
Planning

- Context
- State of the art
- PhD Objective
- **Methodology And Results**

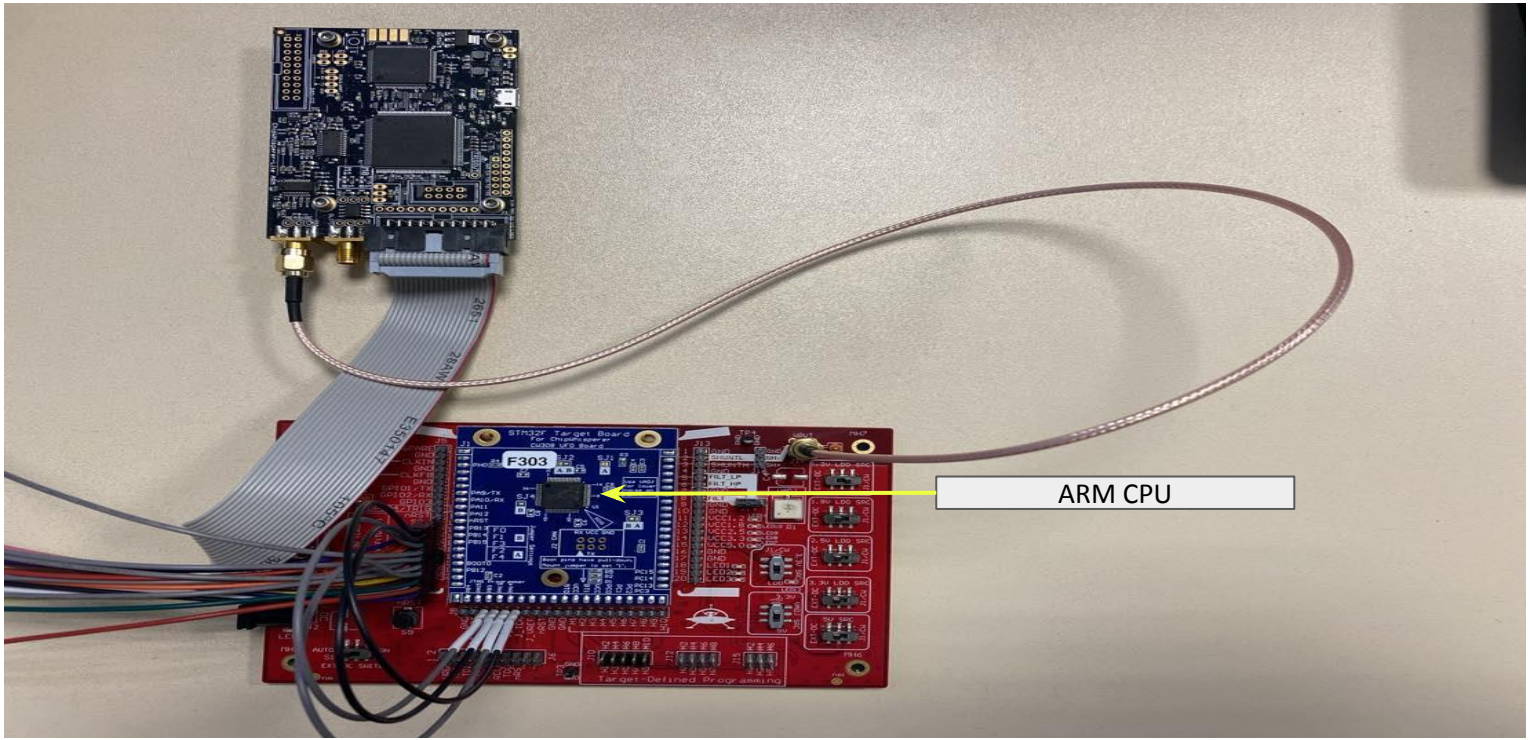
Methodology :

1. Data Collection
2. Data Analyses
3. Feature Selection
4. Model Selection

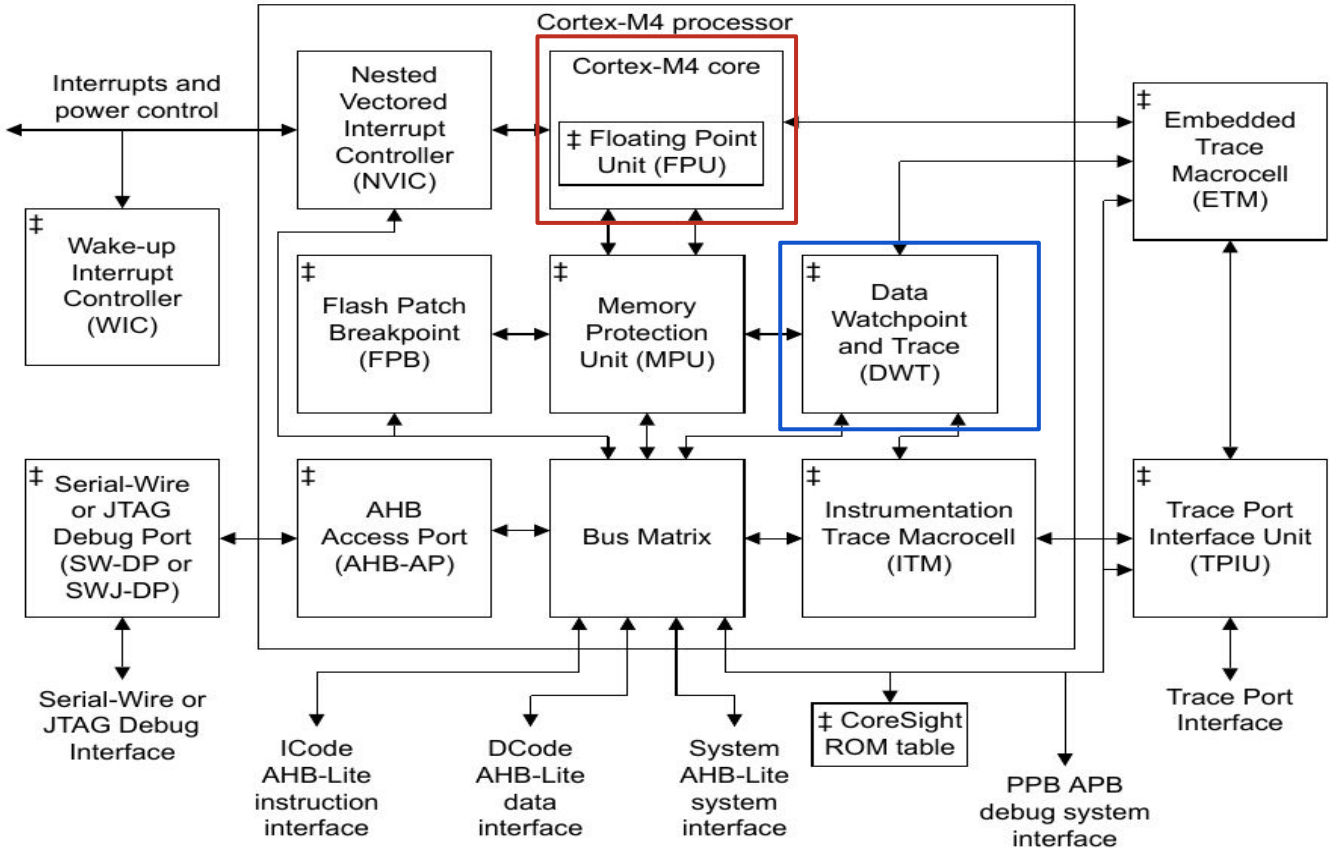
CW 308 With STM32F303



ARM CPU



ARM Cortex-M4 CPU Block Diagram



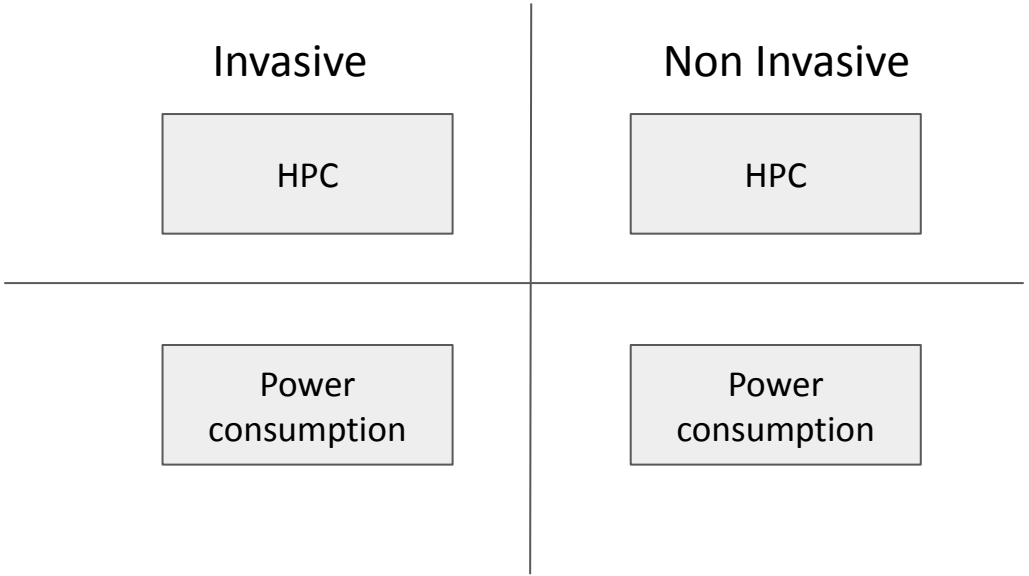
Hardware Performance Counters [1]

Counter Name	Purpose
Cycle Counter	Increment after each CPU cycle
Load And Store Counter	Increment each time a load and store instruction is executed
Instruction Cycle Counter	Increment on each additional cycle required to execute a multi-cycle instruction
Exception Counter	Increments on each entry or return from an exception
Fold Instruction Counter	Increment on zero cycles instructions like If-Then and some NOPs
Sleep Counter	Increment on cycles associated with power saving mode

[1] "ARMv7-M Architecture Reference Manual" , C1.8.6, DWT Register Summary

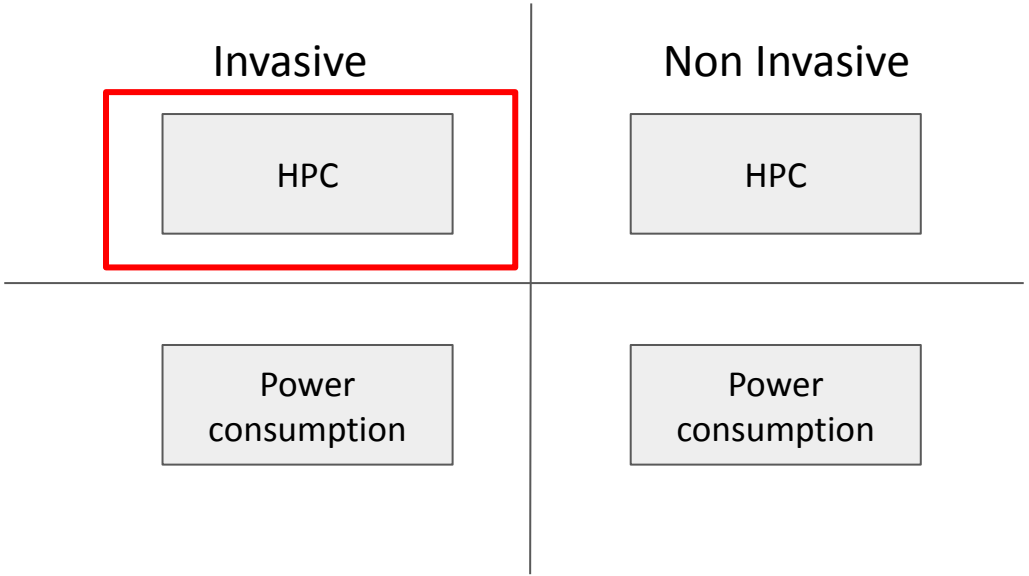
Methodology

Invasive : With interruptions
Non Invasive : Without interruptions



Methodology

Invasive : With interruptions
Non Invasive : Without interruptions



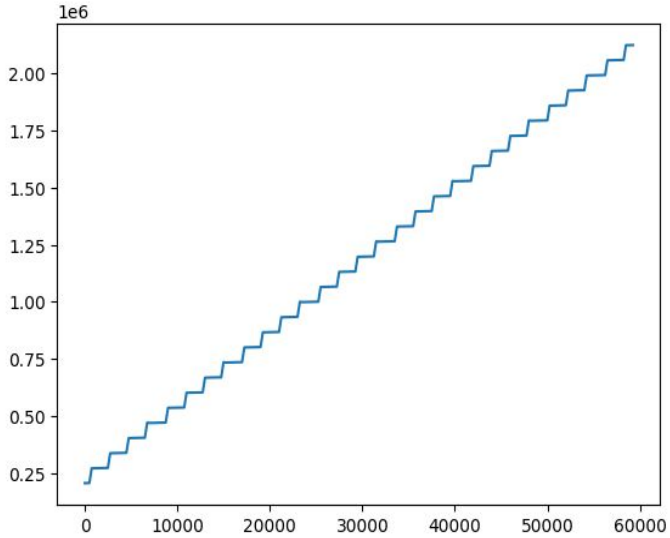
Counter results with interruption (Invasive)

- Bubble Sort

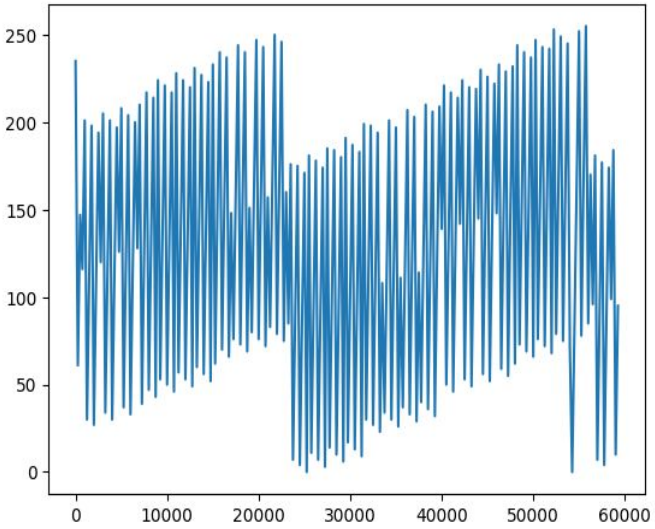
Bubble Sort						
	Timestamps/Cycles	Cycle counter	Load and Store	Instruction cycle counter	Exception counter	Fold Counter
	0	207409	235	248	0	0
	250	207659	61	13	0	0
	500	207909	147	33	0	0
	750	272159	116	55	0	0
	1000	272409	201	76	0	0
	1250	272659	30	97	0	0
	1500	272909	112	158	0	0
	1750	273159	198	178	0	0
	2000	273409	27	200	0	0
	2250	273659	109	222	0	0
	2500	273909	194	242	0	0
	2750	338159	120	6	0	0
	3000	338409	205	26	0	0
	3250	338659	34	49	0	0
	3750	338909	116	70	0	0

Counter results with interruption (Invasive)

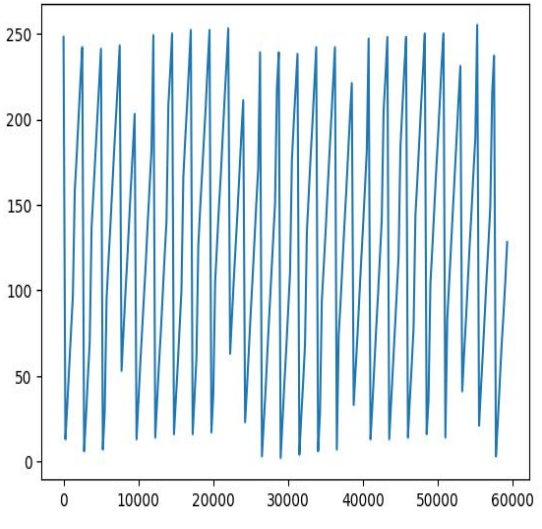
- Bubble Sort



Cycle counter



Load and Store counter



Instruction counter

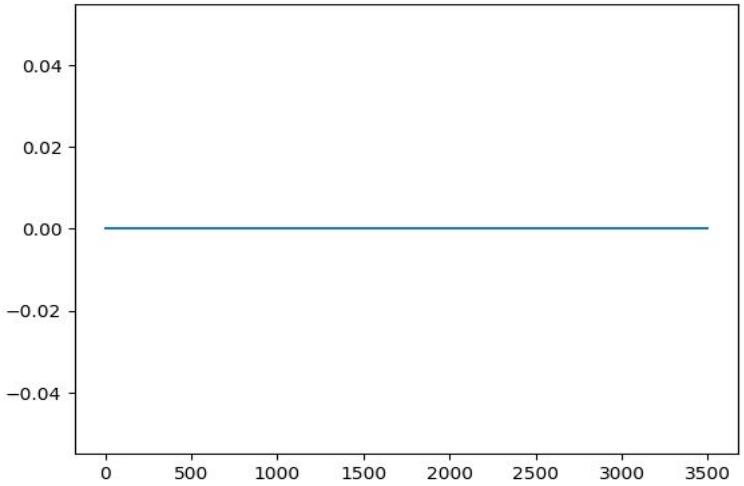
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

LPSS
In Silicon, We Innovate

Counter results with interruption (Invasive)

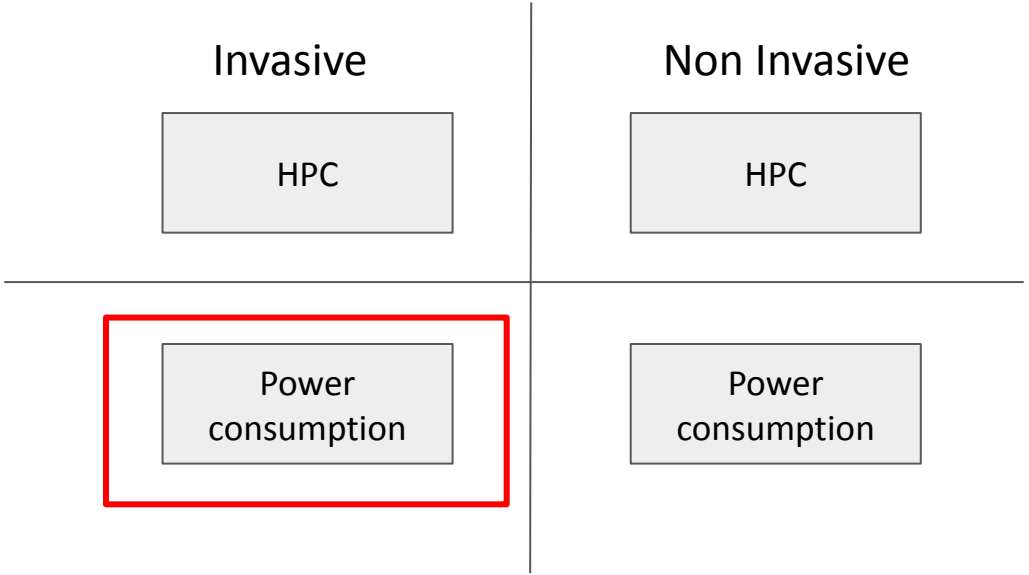
- Bubble Sort

  For both Exception & FOLD counter



Methodology

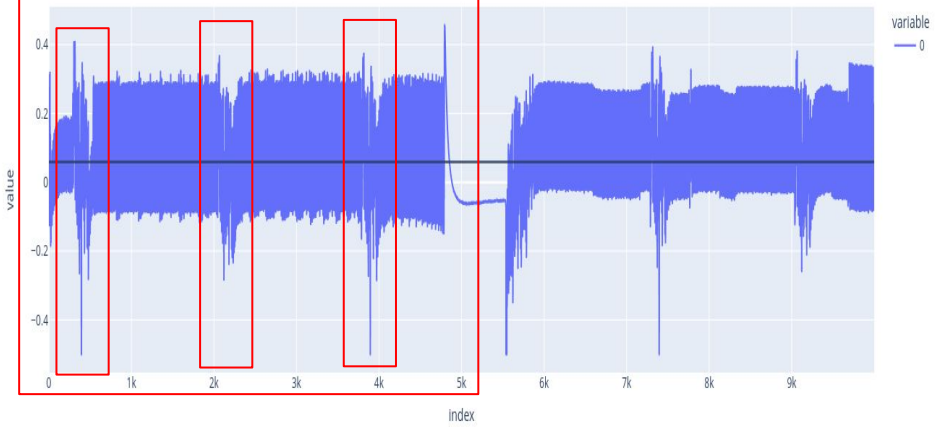
Invasive : With interruptions
Non Invasive : Without interruptions



Power Consumption (Invasive)

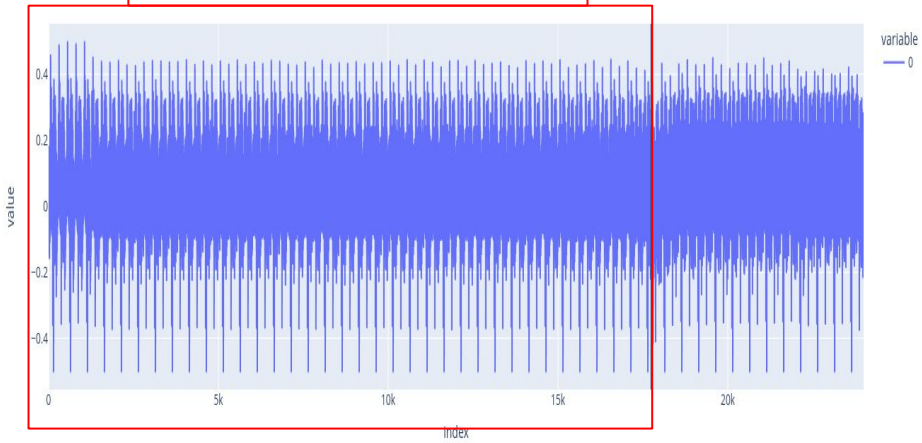
- Using CW-lite with a trigger, we can set a point at which we begin to measure the power of our system.
- We set our sampling rate equal to CPU frequency so we take a sample after each cycle.
- Adding to that a Cycle Counter measurement to have an extract window for our power measurement

1750 cycle



Bubble Sort WorkLoad / Fcpu = 8MHZ / CYC = 4302 /iteration 30

250 cycle

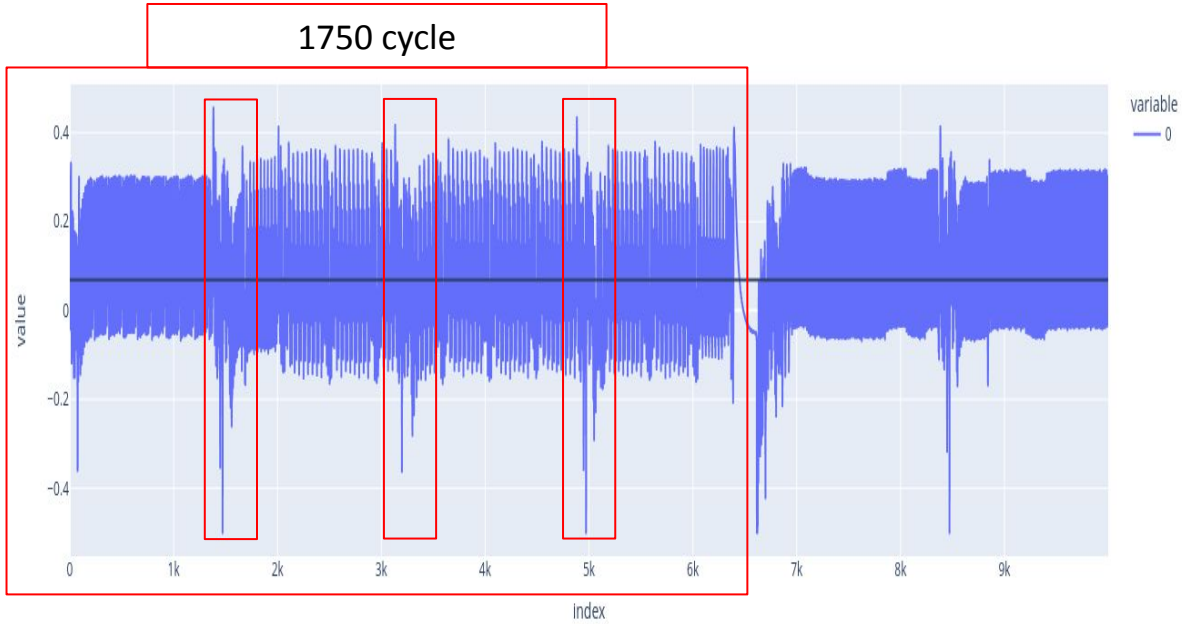


Bubble Sort WorkLoad / Fcpu = 8MHZ / CYC = 17748 /iteration 30

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

LPSS
In Silicon, We Innovate

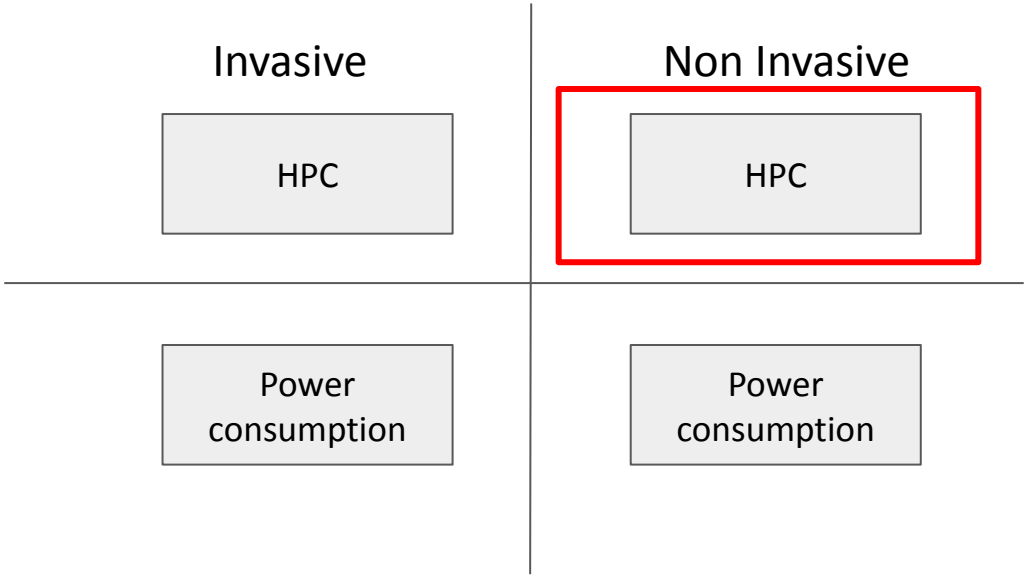
Power Consumption (Invasive)



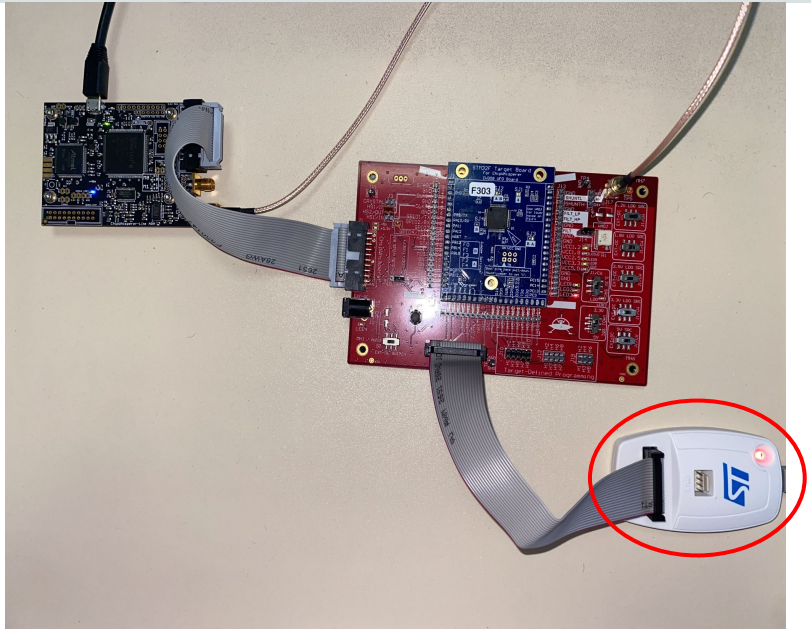
Matrix WorkLoad / Fcpu = 8MHZ/ CYC = 5804/iteration 10

Methodology

Invasive : With interruptions
Non Invasive : Without interruptions



Non Invasive Method (Without interruption)

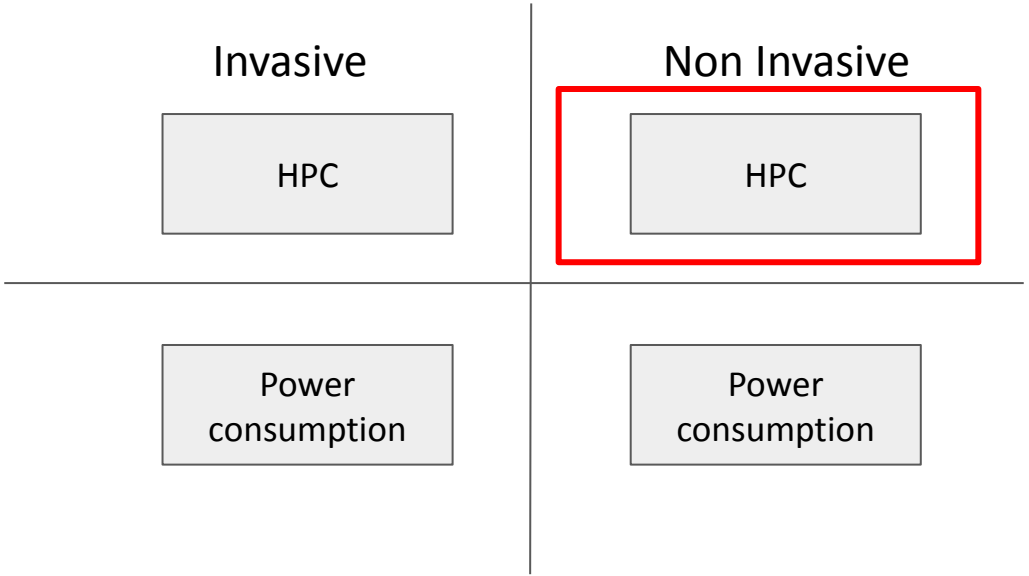


Testbed

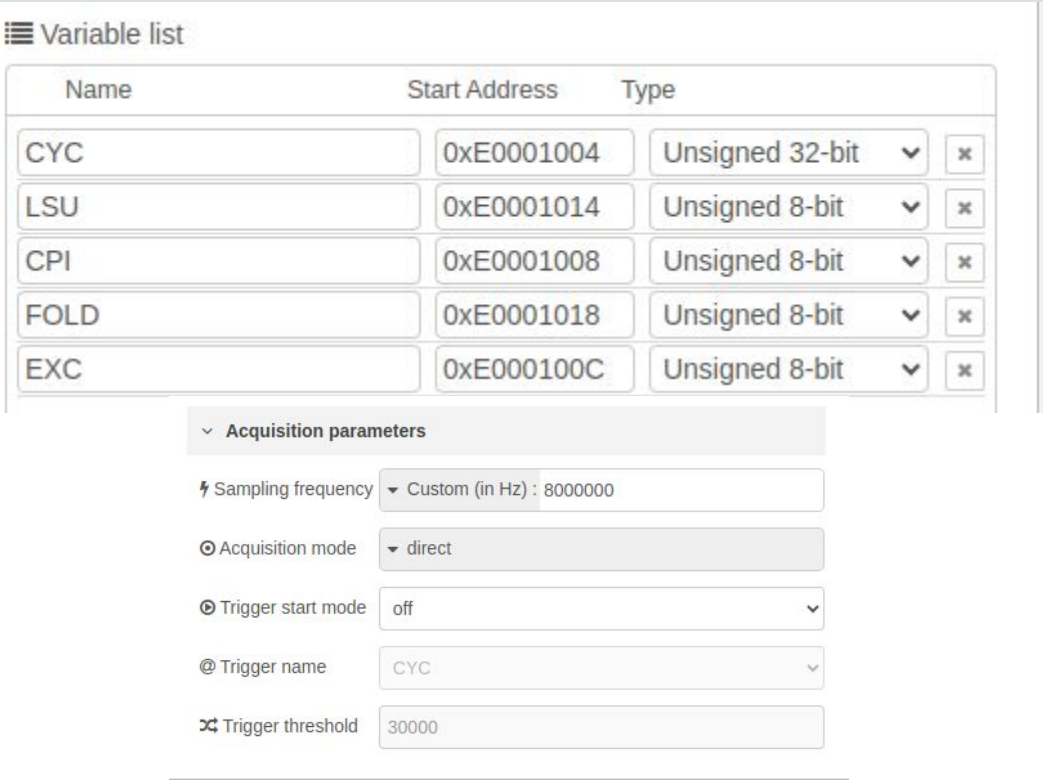
ST-Link V2 debugger

Methodology

Invasive : With interruptions
Non Invasive : Without interruptions



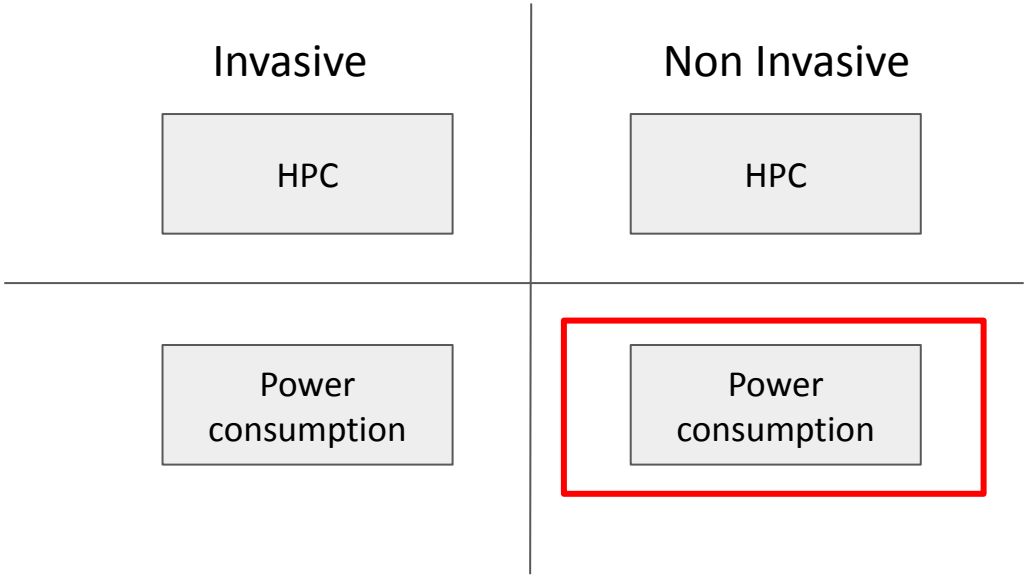
Methodology (Without interruption)



STM32 Cube Monitor

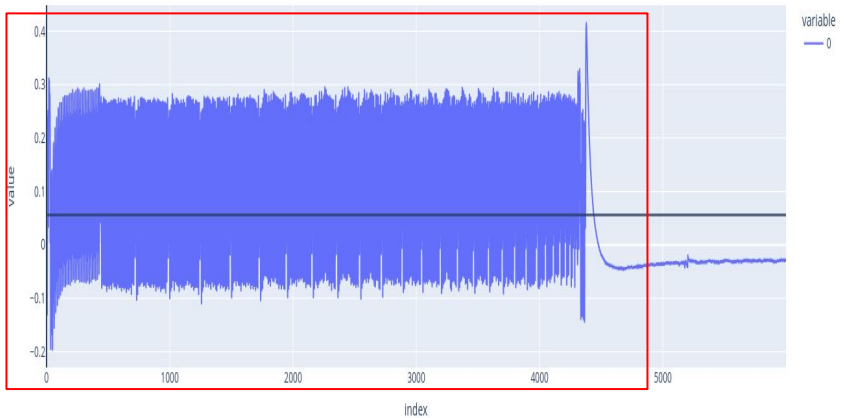
Methodology

Invasive : With interruptions
Non Invasive : Without interruptions

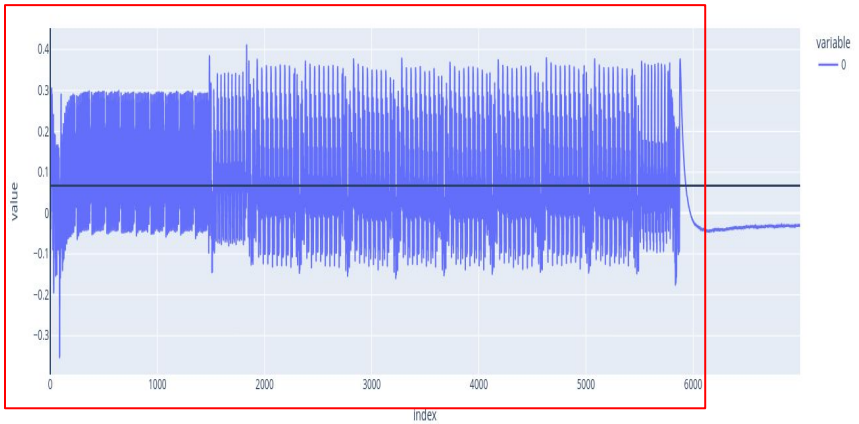


Power Consumption (Without interruption)

- Using CW-lite with a trigger, we can set a point at which we begin to measure the power of our system.
- We set our sampling rate equal to CPU frequency so we take a sample after each cycle.
- Adding to that a Cycle Counter measurement to have an extract window for our power measurement



Bubble Sort WorkLoad / Fcpu = 8MHZ / Mean 527.0163 / CYC = 4302 /iteration 30

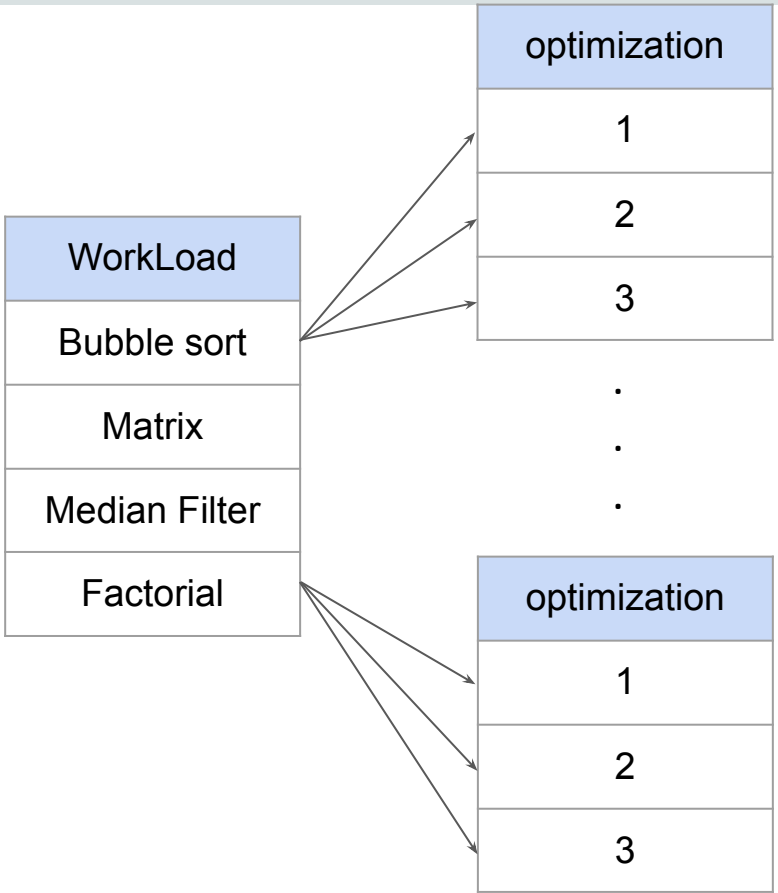


Matrix WorkLoad / Fcpu = 8MHZ/Mean 528.5005/ CYC = 5804/iteration 10

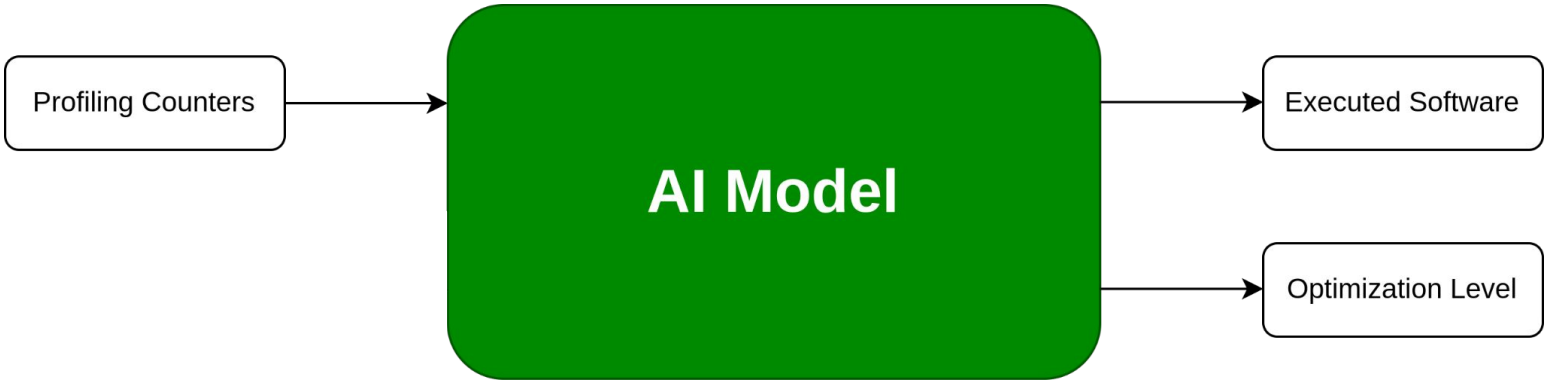
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

LPSS
In Silicon, We Innovate

AI Classification



Workload classification using Profiling Counters



Proposed AI Model

Used Model : MLP , SVM

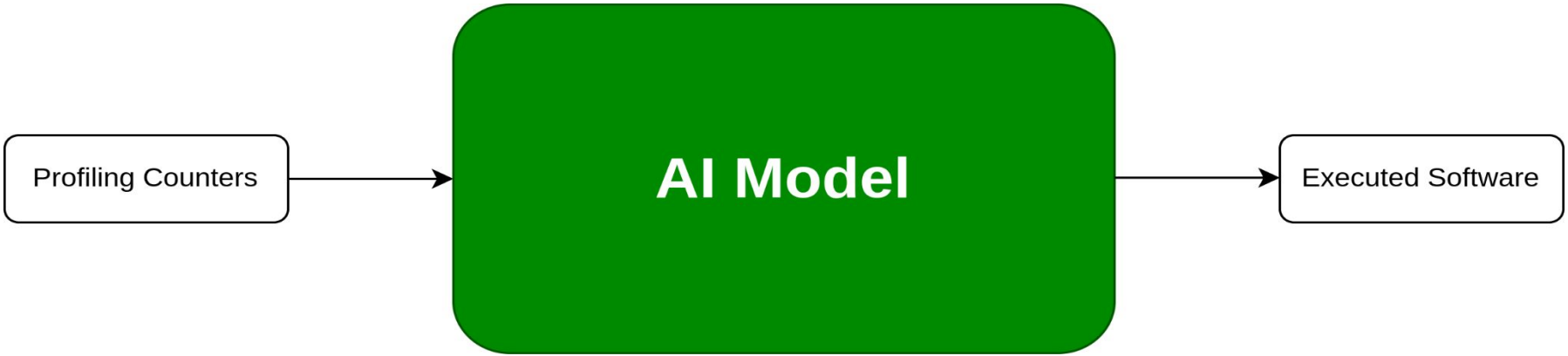
Preliminary Results

Model	Training Accuracy	Validation Accuracy
MLP	58 - 66	62.5
SVM	/	70

AI Classification

WorkLoad
Bubble sort
Matrix
Median Filter
Factorial

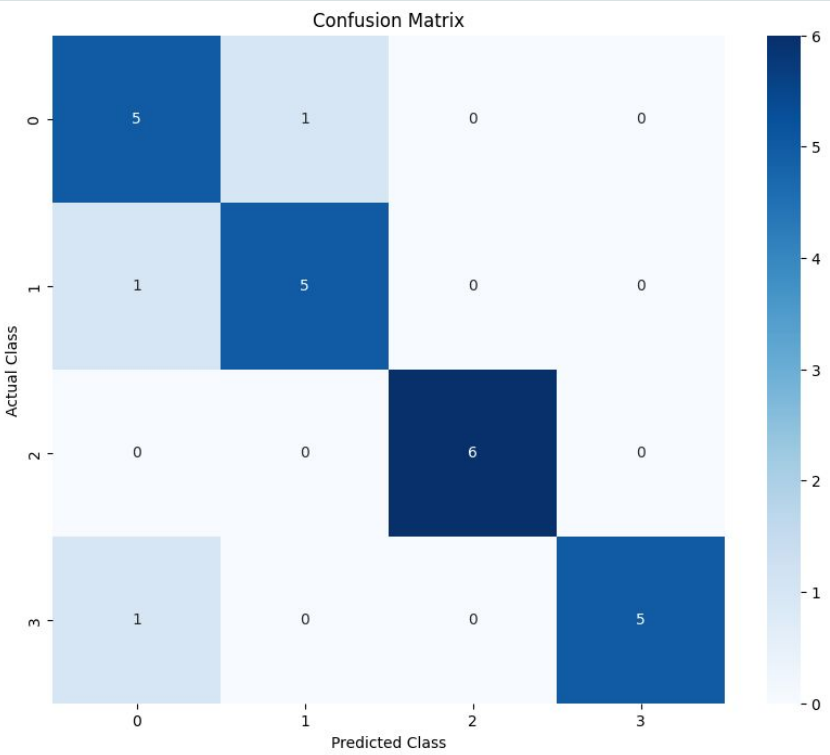
Workload classification using Profiling Counters



Proposed AI Model

Used Model : MLP , SVM

Preliminary Results



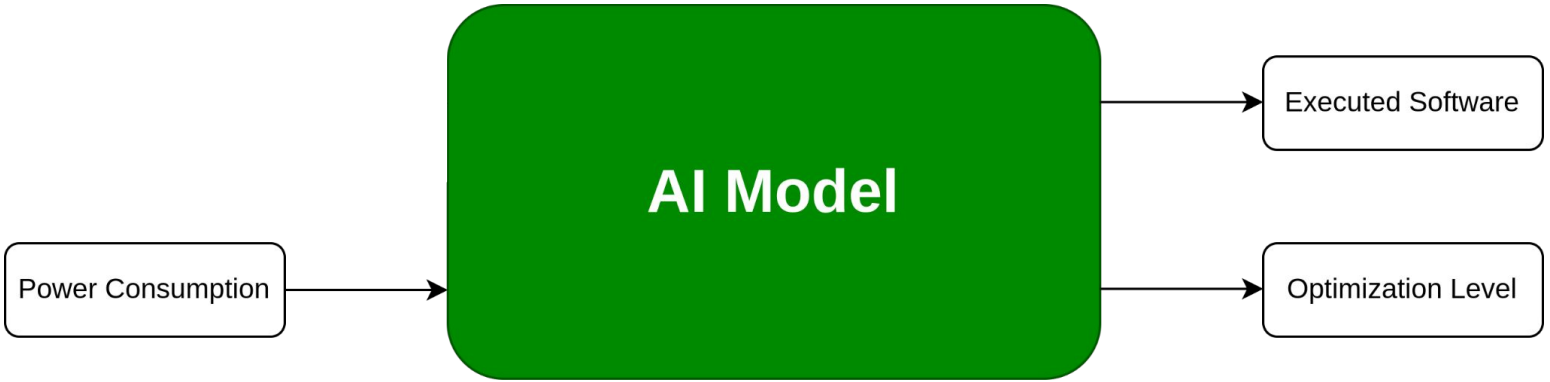
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

LPSS
In Silicon, We Innovate

Preliminary Results

Model	Training Accuracy	Validation Accuracy
MLP	91	87.5
SVM	/	75

Workload classification using Power Consumption



Proposed AI Model

Used Model : CNN + LSTM

Thanks for your intention