PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Antonio Emmanuele

Cycle: XXXIX

Training and Research Activities Report

Year: First

Student Signature: Antonio Emmanuele

Tutor: prof. Mario Barbareschi

Tutor Signature: Mario Barbareschi

Co-Tutor: -

Date: October 31, 2024

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX **Author: Antonio Emmanuele**

1. Information:

- **PhD student: Antonio Emmanuele**
- **DR number: DR997187**
- **Date of birth: 04/12/1998**
- **Master Science degree: Computer Engineering**
- **University: Università Federico II di Napoli**
- **Doctoral Cycle: XXXIX**
- **Scholarship type: UNINA**
- **Tutor: Mario Barbareschi**
- **Co-tutor: -**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate
Virtualization technologies and their applications	**Course**	**22**	**5**	**08-10-15-19-24-25-29-31/01/2024 05-07-26/02/2024**	**Dr. Luigi De Simone, DIETI**	**Y**
Strategic Orientation for STEM Research & Writing	**Course**	**24**	**5**	**07-15/12/2023 – 12-19/01 - 09-23/02/2024**	**Dr Chie Shin Fraser, DIETI**	**Y**
IoT Data Analysis	**Course**	**14**	**4**	**08-09-15-16-22-23/02/2024**	**Prof. Raffaele Della Corte, DIETI**	**Y**
Industrial Embedded Systems Design with the ARM Architecture	**Course**	**17**	**4**	**3-7-10-12-13-14-26/06/2024**	**Prof. Mario Barbareschi, DIETI**	**Y**
Using Deep Learning Properly	**Course**	**12**	**4**	**23-25-30/01/2024 01-06-08/02/2024**	**Dr. Andrea Apicella, DIETI**	**Y**
Development of superconducting	**Seminar**	**1**	**0.2**	**24/11/2023**	**Quantum Science and**	**Y**

quantum devices at FBK					**Technologies QST**	
Ensuring Electronic Reliability Against CERN's Radiation Enviromnent	**Seminar**	**2**	**0.4**	**1/12/2023**	**Prof. Francesco Fienga, DIETI**	**Y**
Energy-Efficient Data Science	**Seminar**	**1**	**0.2**	**13/12/2023**	**Prof. Elio Masciari, DIETI**	**Y**
The 14th IEEE international conference on Cloud Computing Technology and Science	**Seminar**	**25**	**5**	**4-6.12.2023**	**-**	**Y**
CSAW 2023 - Puf enabled Security challenge	**Seminar**	**10**	**2**	**9-10.11.2023**	**Ecole d'ingénieur·es en systèmes intelligents cybersécurisés, Valence (France).**	**Y**
AI at The Deep Edge	**Seminar**	**21**	**4,2**	**31.01.2024 – 02.02.2024**	**STMicroelectronics, Arzano NA**	**Y**

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	**0**	**7.8**	**5**	**0**	**12.8**
Bimonth 2	**10**	**4.2**	**5**	**0**	**19.2**
Bimonth 3	**4**	**0**	**5**	**0**	**9**
Bimonth 4	**4**	**0**	**4**	**0**	**8**
Bimonth 5	**4**	**0**	**4**	**0**	**8**
Bimonth 6	**0**	**0**	**5**	**0**	**5**
Total	**22**	**12**	**28**	**0**	**62**
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

My research focuses on two main topics: PUF-based security solutions for Internet of Things systems, and the deployment and interpretation of decision tree-based models at the edge. Both topics are discussed in detail below.

- **PUF-based security solutions for Internet Of Things systems**.

  The Internet of Things (IoT) paradigm is rapidly becoming an essential and pervasive component of modern society by connecting a multitude of devices and enabling data-driven insights. A key factor in the widespread adoption of IoT systems is the use of edge computing, which empowers devices at the edge of networks—often referred to as edge nodes—to perform computation locally, without needing to constantly transmit data to cloud servers. This approach offers several significant advantages such as reduced latency, improved bandwidth and enhanced data privacy. However, the benefits of edge computing come with critical challenges, particularly regarding the security of edge devices.
  Indeed, edge nodes typically operate in unsafe environments, where they can be either physically manipulated or cloned by an attacker, and communicate over unsecure communication channels.
  For these reasons, they must implement robust mechanisms for authentication, to verify the identities edge-nodes; confidentiality, to ensure that sensitive data remains protected from unauthorized access; and attestation, to provide assurance that the device operates as expected and has not been compromised.
  Unfortunately, these mechanisms are challenging to embed in edge devices as they are often microcontrollers with limited computational power, memory capacity, and strict energy constraints, especially when battery-powered. Additionally, such nodes generally lack secure and tamper-resistant memories, making it challenging to safely store cryptographic keys. Therefore, my research focuses on Physical Unclonable Functions (PUFs) a lightweight solution to address the discussed challenges in IoT systems. PUFs leverage intrinsic manufacturing imperfections of circuits to enable device-specific generation of cryptographic keys. In particular, they allow for secure generation and storage of cryptographic material which is directly tied to the unique physical properties of each device, removing the need of secure storage and reducing the computational cost of the previously discussed security mechanisms. Indeed, PUFs enable the authentication of edge devices and facilitate cryptographic key sharing between pairs or groups of these devices without relying on complex mathematical operations, ensuring minimal computational and energy overhead. This year, my work has focused on two main challenges of PUF based security solutions. The first one involves the management of cryptographic keys for groups of IoT nodes. The second one addresses the share of a single hardware PUF in multi-user IoT systems where a single resource is shared between multiple end-users. In such systems, when a PUF is shared, each end user must be isolated from the others. This ensures that if one end user is compromised, the others remain secure.

- **Decision Tree based Machine Learning models**.

  The use of Machine Learning models for classification and regression problems is steadily increasing, with Deep Learning (DL) models like Convolutional Neural Networks (CNNs) being widely adopted for their high accuracy. However, as the trend of shifting computation to the edge grows, these models often prove unsuitable due to their high hardware resource requirements, which edge devices cannot typically meet. Furthermore, as ML becomes more integrated into critical aspects of human life, the demand for interpretability of model predictions is also rising. Unfortunately, most DL models lack interpretability. For these reasons, my research this year has focused on ML models based on Decision Trees. These models represent a set of decision rules in a binary tree, where inference involves a simple tree traversal

rather than complex mathematical operations, keeping computational demands low. During this year, I have worked on hardware accelerator approximation for tree traversal to minimize deployment resources at the edge. Moreover I've developed a framework for their use in public transportation systems. This framework supports both the deployment of DT models on microcontrollers for edge-based inferences and allows for inferences' interpretation through feature attribution techniques.

4. Research products:

- **PUF-based security solutions for Internet Of Things systems**

Title: A Lightweight PUF-based Protocol for Dynamic and Secure Group Key Management in the IoT
Type: Journal article
Journal: IEEE Internet Of Things Journal
Authors: Mario Barbareschi, Valentina Casola, Antonio Emmanuele, Daniele Lombardi
Status: published
Link: https://ieeexplore.ieee.org/abstract/document/10614146
DOI: 10.1109/JIOT.2024.3418207
***Date of Publication*:** 29 July 2024
Abstract: In many Internet of Things (IoT) applications, resource-constrained devices often collaborate in groups for the acquisition, transmission, and management of sensitive information. To uphold the security of these operations, symmetric encryption algorithms are commonly employed due to their efficiency and speed. Nevertheless, establishing a key management mechanism, that accommodates the distinctive features of the IoT domain, remains an ongoing challenge. This article introduces Group-Key PHEMAP, a novel physically unclonable function (PUF)-based protocol for group key management in IoT applications. The proposed protocol relies solely on lightweight operations for group key management and supports dynamic membership without leveraging additional cryptographic keys. We present a formal demonstration for security properties and a comprehensive analysis, regarding both computational and communication costs, as well as scalability property concerning the growing number of devices within the group. Finally, we validate the suitability of our proposal by resorting to the ns-3 network simulator, and, by implementing the protocol on devices representing typical characteristics of those used in IoT applications.

Title: On the adoption of PUF for key agreement scheme in Internet of Things
Type: Workshop article
Workshop: MAL-IoT 2024 : 9th International Workshop on Malicious Software and Hardware in the Internet of Things
Authors: Mario Barbareschi, Valentina Casola, Antonio Emmanuele, Daniele Lombardi
Status: published
Link: https://dl.acm.org/doi/pdf/10.1145/3637543.3654656
DOI: https://doi.org/10.1145/3637543.365465

***Date of Publication*:** 01 July 2024
Abstract: With the rapid proliferation of Internet of Things systems, ensuring secure communication for those applications that need to exchange sensitive and/or critical data is one of the major issues to be faced. Traditional security mechanisms are often impractical due to the constrained resources typically available on IoT devices. On the other hand, Physical Unclonable Functions are emerging as one of the most promising technologies to address security-related challenges. In this manuscript, we propose a novel scheme leveraging PUF-chains to facilitate key agreement between two devices. The scheme employs a trusted third party for secure communications; additionally, it facilitates seamless and continuous modification of the cryptographic key employed, by resulting really suitable in systems for moving target defense. To demonstrate the feasibility of our proposal, we take into account an implementation of the solution on resource-constrained devices, specifically ESP8266, and conducted a thorough analysis in terms of communication and computational costs, time overhead and formal security verification.

Title: Pioneering Virtual Physical Unclonable Functions
Type: Journal article
Journal: IEEE Transaction On Emerging Topics in Computing
Authors: Mario Barbareschi, Antonio Emmanuele, Daniele Lombardi
Status: submitted
Abstract: In recent years, the proliferation of the Internet of Things (IoT) applications is leading to the demand for a more efficient and scalable utilization of computational and sensing resources. Consequently, the multi-user paradigm is being widely adopted, even at the edge, as it allows different users to fairly share the same resources. However, the employment of this paradigm is hindered back by security challenges typical of the IoT. Among available security mechanisms, edge devices are typically equipped with Physical Unclonable Functions (PUFs), due to their lightweight and flexible nature when involved for security primitives and protocols. Unfortunately, PUFs are not designed to be employed in a multi-user environment. In order to address these new challenges, we propose, for the first time, the Virtual-PUFs, namely security primitives that exhibit the characteristics of distinct and independent PUFs. We discuss their mathematical definition and formal properties, as well as their quality metrics and, inherently, virtual enrollment procedures. Additionally, we devise four different virtualization strategies, detailing fundamental security requirements of the hosting platform. Finally, we prototype our solution on a RISC-V core running the Xvisor hypervisor and prove its effectiveness by directly measuring the discussed quality metrics, as well as additional required overhead.

- **Decision Tree based Machine Learning models**.

Title: Designing On-Board Explainable Passenger Flow Prediction
Type: Journal article
Journal: Engineering Applications of Artificial Intelligence.

Authors: Mario Barbareschi, Antonio Emmanuele, Nicola Mazzocca, Franca Rocco di Torrepadula
Status: accepted
Abstract: Nowadays, predicting public transport passenger flow (PF) is essential to optimize service planning and provide information to commuters. However, while current research focuses on enhancing accuracy using advanced models, like recurrent and graph neural networks, other key aspects, such as interpretability and computational efficiency, are often neglected. To fill this gap, we propose a framework to design on-board explainable PF prediction based on eXtreme Gradient Boosting (XGBoost). This framework enhances model interpretability and reduces computational costs, making the resulting PF predictive model suitable for inference on low-end devices. The proposed framework is validated on a real-world dataset from a major Italian city, involving 25 buses. Our results show that the framework achieves performance comparable to Convolutional Neural Networks (CNNs), with only a 0.2% percentage increase in Mean Absolute Percentage Error (MAPE). Additionally, it significantly reduces both inference time and energy consumption, with percentage decrease of 63%. Finally, we present examples to illustrate the interpretability of the predictions using the SHap-ley Additive exPlanation (SHAP) method.

Title: Exploiting Functional Approximation on Decision-Tree based Multiple Classifier Systems
Type: Conference article
Conference: IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC 2024)
Authors: Mario Barbareschi, Salvatore Barone, Antonio Emmanuele and Nicola Mazzocca
Status: accepted
Abstract: Multiple Classifier Systems (MCSs) have been increasingly designed to take advantage of hardware features, such as high parallelism and computational power, to guarantee higher throughput and lower latency. Although the combination of multiple classifiers leads to high classification accuracy, the required area overhead makes the design of a hardware accelerator unfeasible, hindering the adoption of commercial configurable devices. For this reason, in this paper, we exploit the Approximate Computing (AxC) design paradigm to automatically generate approximated hardware implementations of MCSs by trading hardware area overhead off for classification accuracy. In particular, we propose an algorithm that identifies the resiliency source of the model and uses it to introduce approximation with minimum accuracy loss. In order to prove the effectiveness of our solution, we performed numerous experiments on models of various sizes trained on different datasets. The results show that with negligible accuracy loss it is possible to significantly reduce the hardware requirements of a classifier.

Title: Modular Redundancy based approximation of Tree Ensemble Classifiers
Type: Workshop article
Workshop: AxC'24 The 9th Workshop on Approximate Computing

Authors: Antonio Emmanuele, Mario Barbareschi, Salvatore Pappalardo, Alberto Bosio
Status: accepted
Abstract: In recent years, the adoption of edge computing in the Internet of Things has led to the increased deployment of classifiers on edge devices. Among these, tree ensembles are widely adopted at the edge as they are both accurate and resource efficient models when compared to neural networks. However, as the complexity of such models increases, their deployment on typical resource-poor edge devices becomes challenging. For these reasons, we propose a new approximation algorithm for tree ensembles based on the concept of modular redundancy. Our proposal envisions that each class is classified by only a subset of trees in the ensemble, thus allowing both to approximate different trees by removing the leaves related to an unclassified class and to simplify the combining logic among their result.

Title: Modular Redundancy for Efficient Tree Ensemble Approximation in Network Traffic Classification
Type: Conference article
Conference: Design, Automation and Test in Europe Conference, 2025
Authors: Antonio Emmanuele, Mario Barbareschi, Salvatore Pappalardo, Alberto Bosio
Status: submitted
Abstract: Nowadays, the real-time classification of network traffic is becoming an increasingly important task for bandwidth management, service prioritization, and the detection of network intrusions. To this end, tree ensembles, such as Random Forest, have been demonstrated to be highly accurate network traffic classifiers, while also being lightweight models, well-suited for real-time applications. However, as the volume of data grows, the complexity of these models increases, posing a challenge to their use in real-time scenarios. In order to address this challenge, we propose a novel approximation algorithm for tree ensembles based on modular redundancy. Our approach assigns each traffic class to a subset of trees within the ensemble, allowing pruning of leaves related to irrelevant classes and streamlining the logic for combining results. We demonstrate that our proposal reduces computational cost and requirements while maintaining the accuracy required for effective and scalable traffic classification.

5. Conferences and seminars attended

- CSAW 2023 - Puf enabled Security challenge. Ecole d'ingénieur ·es en systèmes intelligents cybersécur isés, Valence (France). 9-10.11.2023.
- The 14th IEEE international conference on Cloud Computing Technology and Science (CLOUDCOM 2023). Napoli, Italy. 4-6 December 2023.
- Conference: IFIP/IEEE International Conference on Very Large Scale Integration(VLSI-SoC 2024). Oct 6-9 2024. Tanger, Morocco. Presented paper.
- Workshop: AxC'24 The 9th Workshop on Approximate Computing. Conference: 2024 International Conference on Computer-Aided Design (ICCAD). October 27-31 2024. Presented paper online (not attended in person).

- Workshop: MAL-IoT 2024 : 9th International Workshop on Malicious Software and Hardware in the Internet of Things. Conference: 21st ACM International Conference on Computing Frontiers (CF' 24). May 7 - 9, 2024, Ischia, Italy. Presented paper.

6. Activity abroad:

Not yet.

7. Activity in partner companies:

-

8. Tutorship

Not yet.