UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Activities and Publications Report

PhD Student: Alfredo Nascita

Student DR number: DR995853

PhD Cycle: XXXVII
PhD Cycle Chairman: Prof. Stefano Russo

PhD program student's start date: 01/11/2021
PhD program student's end date: 31/10/2024

Supervisor: Prof. Valerio Persico

e-mail: valerio.persico@unina.it

PhD scholarship funding entity: Università Federico II

General information

Alfredo Nascita received in the year 2021 the Master Science degree in Computer Engineering from the University of Napoli Federico II. He attended a curriculum in Networking Engineering within the PhD program in Information Technology and Electrical Engineering. He received a grant from Università Federico II.

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organization
1st	Network Security	MSc course	6	Prof. Simon Pietro Romano, DIETI	University of Napoli Federico II
1st	Statistical data analysis for science and engineering	Ad hoc course	4	Prof. Roberto Pietrantuono, DIETI	ITEE, University of Napoli Federico II
1st	Imprenditorialità Accademica	Ad hoc course	4	Prof. Pierluigi Rippa, DII	Scuola Politecnica e delle Scienze di Base
1st	Machine Learning for Science and Engineering Research	Ad hoc course	5	Proff. A. Corazza, F. Isgrò, R. Prevete, C. Sansone - DIETI, Dr. G. Pezzulo - CNR	ITEE, University of Napoli Federico II
2nd	On the challenges and impact of Artificial Intelligence in the Insurance domain	Ad hoc course	3	Dr. Lorenzo Ricciardi Celsi, PhD, MBA	ITEE, University of Napoli Federico II
2nd	IoT Data Analysis	Ad hoc course	4	Dr. Raffaele Della Corte, DIETI	ITEE, University of Napoli Federico II
2nd	Using Deep Learning properly	Ad hoc course	4	Dr. Andrea Apicella, DIETI	ITEE, University of Napoli Federico II
3rd	Ethics and AI	External Course	2.4	Prof. Guido Boella (Dipartimento di Informatica Università di Torino) et al.	Italian Society for Ethics of AI (SIpEIA)
3rd	Percorso per il rafforzamento delle competenze sulla progettazione europea	External Course	3.4	Dr. Tommaso FOGLIA, Dr. Federico PORCEDDA. Dr. Veronica ROCCO	Ministero dell'Università e della Ricerca, Ateneo Federico II

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organization
1st	eXplainable AI Summer School (XAISS)	Delft, NL	5	29/08/22 - 02/09/22	University of Delft, Delft, NL
1st	TMA PhD School	Enschede, NL	3,2	27-28/06/22	University of Twente, Enschede, NL
2nd	TMA PhD School	Napoli, IT	2	26-27/06/23	University of Napoli Federico II

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organization
1st	Vehicular Hacking in Akka Technologies	0.3	Dr. Luigi Guida - Luigi Villa	Akka Technologies	ITEE, University of Napoli Federico II
1st	Cyber security in Akka Technologies	0.4	Dr. Luigi Villa, Sara Belluccin, Matteo Pracchia	Akka Technologies	ITEE, University of Napoli Federico II
1st	Threat Hunting Essentials	0.4	Group-IB	Group-IB	ITEE, University of Napoli Federico II
1st	Connecting the dots: Investigating an APT campaign using Splunk	0.4	Dr. Antonio Forzieri	Splunk	ITEE, University of Napoli Federico II
1st	Possible Quantum Machine Learning Approaches in HEP	0.4	Dr. Michele Grossi	CERN, Geneve, Switzerland, Openlab QTI	ITEE, University of Napoli Federico II
1st	Single-cell omics leverage Machine Learning to dissect tumor microenvironment and cancer immuno editing	0.4	Dr. Raoul J.P. Bonnal	IFOM - the FIRC Institute of Molecular Oncology Milan, Italy	ITEE, University of Napoli Federico II
1st	Threat Hunting Use-Cases	0.4	Group-IB	Group-IB	ITEE, University of Napoli Federico II
1st	All roads lead to WebRTC: an introduction to Janus	0.4	Dr. Lorenzo Miniero	Meetecho	ITEE, University of Napoli Federico II
1st	Enel - Digital Innovation e Cyber Security	0.3	ENEL	ENEL	ITEE, University of Napoli Federico II
1st	The quest of quantum advantage with a photonics platform	0.3	Prof. Fabio Sciarrino	UNINA, Dipartimento di Fisica	SSM - Scuola Superiore Meridionale

1st	Computational analysis of cancer genomes	0.2	Nùria Lòpez-Bigas	ICREA Research Professor Institute for Research in Biomedicine Barcelona, Spain	ITEE, University of Napoli Federico II
1st	Project Vāc: Can a Text-to-Speech Engine Generate Human Sentiments?	0.2	Prof. V.K. Gurbani	Illinois Institute of Technology - USA	Dip. Fisica, "Ettore Pancini" - DIETI, Unina
1st	RAILS mid-term workshop	1	Prof. Valeria Vittorini et al.	Università di Napoli Federico II	ITEE, University of Napoli Federico II
1st	Explainable Natural Language Inference	0.3	Dr. Marco Valentino	University of Manchester, Manchester, United Kingdom	ITEE, University of Napoli Federico II
1st	Ciberconflitti e minacce per la pace e la stabilità internazionale - Riflessioni sulla guerra in Ucraina e oltre	0.4	Proff. Simon Pietro Romano, Guglielmo Tamburrini	Università di Napoli Federico II	Gruppo RUniPace, UNINA
1st	IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE Editors	0.3	Dr. Derek Abbott et al.	Electrical and Electronic Engineering at the University of Adelaide, Australia	ITEE, University of Napoli Federico II
1st	Malware Reverse Engineering: Foundations	0.4	Antonio Villani	Cybersecurity Architect at Leonardo's Cybersecurity Division	Prof. Fabio de Gasperi, Università degli Studi di Roma La Sapienza
1st	Towards a Political Philosophy of AI (Picariello Lectures)	0.4	Prof. Mark Coeckelbergh	University of Wien	University of Napoli Federico II, DIETI e Dip. di Fisica
1st	Accelerated Deep Learning via Efficient, Compressed and Managed Communication	0.2	Prof. Marco Canini	King Abdullah University of Science and Technology (KAUST)	ITEE, University of Napoli Federico II

				Thuwal, Saudi Arabia	
2nd	Data mining the output of quantum simulators - from critical behavior to algorithmic complexity	0.2	Dr. Marcello Dalmonte	Abdus Salam ICTP Trieste	University of Napoli Federico II
2nd	Cybercrime and Information Warfare: National and International Actors	0.4	Dr. Pierluigi Paganini	Cibhorus S.r.l.	ITEE, University of Napoli Federico II
2nd	Privacy and data Protection	0.4	Dr. Stefano Mele	Gianni & Origoni	ITEE, University of Napoli Federico II
2nd	Digital Forensics	0.4	Group-IB	Group-IB	ITEE, University of Napoli Federico II
2nd	From Cyber Situational Awareness to Adaptive Cyber Defense: Leveling the Cyber Playing Field	0.4	Prof. Massimiliano Albanese	George Mason University - USA	ITEE, University of Napoli Federico II
2nd	Threat Hunting & Incident Response	0.4	Group-IB	Group-IB	ITEE, University of Napoli Federico II
2nd	Industry 4.0 Fundamentals in Bosch Applications	2	Eng. Martino Bruni	Bosch, Italy	National Doctoral program in Autonomous Systems, in collaboration with Bosch – Centro Studi Componenti per Veicoli and the Decision and Control Laboratory of Politecnico di Bari.
2nd	MLOps: Achieving Operational Velocity with Faster Delivery and Collaboration	0.2	Prof. Tarry Singh	Real.AI & University of Texas at Dallas - USA	ITEE, University of Napoli Federico II

2nd	How to Publish Under the CARE-CRUI Open Access Agreement with IEEE	0.3	Prof. Nino Grizzuti	Università di Napoli Federico II	University of Napoli, Federico II
2nd	Migration of legacy IT infrastructures into the cloud: approaches and strategies	0.4	Ing. Claudio Perrotta	Epsilon S.r.l.	ITEE, University of Napoli Federico II
2nd	Traffic Engineering with Segmented Routing: optimally addressing popular use cases	0.2	Prof. Pascal Merindol	University of Strasbourg - France	ITEE, University of Napoli Federico II
2nd	BGP & Hot-Potato Routing: graceful and optimal convergence in case of IGP events	0.2	Prof. Pascal Merindol	University of Strasbourg - France	ITEE, University of Napoli Federico II
3rd	Robotics Meet AI & 5G - The future is now	0.4	Prof. Bruno Siciliano	Università di Napoli Federico II	University of Napoli Federico II, DIETI
3rd	Media Forensics in the era of generative AII	0.4	Prof. Luisa Verdoliva	Università di Napoli Federico II	University of Napoli Federico II, DIETI

Research activities

Alfredo Nascita's research activities have mainly focused on the explainability of AI-based models for analyzing Internet network traffic. He explored various aspects of the explainability of Deep Learning models, proposing methodologies to understand and improve state-of-the-art approaches. His work has explored the role of inputs derived from network traffic in the decisions of DL models and the reliability of traffic classifier responses through calibration techniques.

Aligned with this central research theme, he investigated explainability approaches for Large Language Models during his internship abroad, focusing on the localization of knowledge in pre-trained and fine-tuned models, particularly in classification tasks.

Additionally, Alfredo Nascita contributed to research on the analysis and design of Class Incremental Learning approaches for analyzing and classifying network traffic generated by mobile applications.

Other research areas he has explored include: (i) Machine and Deep Learning approaches for attack classification and anomaly detection in Internet of Things (IoT) networks, (ii) evaluating the robustness of anomaly detection models in different traffic scenarios using cross-evaluation approaches, (iii) integration of blockchain with Software Defined Networks, and (iv) development of approaches for computing offloading and task migration within Industrial Internet of Things contexts.

Tutoring and supplementary teaching activities

During the three-year PhD Programme, I carried out tutorship and supplementary teaching activities during *Computer Networks* and *Fondamenti di Informatica* courses for Bachelor's Degrees in Computer Engineering and *Internet Data Analysis* course for Master's and Bachelor's Degrees in Computer Engineering.

Details on my tutorship activities are listed in the following:

- Co-supervisor of two Master's theses in Computer Engineering, *Internet Data Analysis* course (16 hours)
- Teaching activities during the *Internet Data Analysis course,* Master's Degree in Computer Engineering, Prof. Pescapé (2 hours)
- Teaching activities and supplementary Teaching Activities during the *Computer Networks* course, Bachelor's Degree in Computer Engineering, Prof. Pescapé (21 hours)
- Laboratory activities during the *Internet Data Analysis* course, Master Degree in Computer Engineering, Prof. Pescapé (14 hours)
- Support: *Porte Aperte Scuola Politecnica e delle Scienze di Base 2023* (2 hours)
- Supplementary teaching activities during the *Computer Networks* and *Fondamenti di Informatica* courses in Bachelor's Degree in Computer Engineering, Prof. Pescapé and Prof. Persico (5 hours)

Credits summary

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	24	10.3	29	0
2nd	11	7.5	40	1.6
3rd	5.8	0.8	53	0.8

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
3rd	Huawei R&D Centre, Paris, France	Jonatan Krolikowski, Senior Research Engineer	15/01/24 - 14/07/24	Research on explainability for Large Language Models. Joint scientific paper preparation

PhD Thesis

Internet network traffic has changed profoundly in recent years, and its analysis today presents new and complex challenges that make traditional approaches ineffective. Nowadays, Deep Learning (DL) approaches represent the most promising strategy for traffic analysis, as they can adapt to the changing nature and heterogeneity of traffic.

Unfortunately, these approaches have limitations in terms of transparency and reliability due to their "black-box" nature. This makes automatic decisions difficult to trust and does not allow their full adoption in real and complex network contexts.

For these reasons, the research area of Explainable AI (XAI) was introduced to shed light on DL models and improve the understanding and interpretability of their results.

This thesis focuses on the explainability of state-of-the-art approaches for Internet traffic analysis to solve different application tasks, such as classifying traffic generated by mobile applications, detecting cyber attacks, and identifying network anomalies.

In particular, several aspects related to explainability are analyzed to understand the functioning of DL models and improve them from different perspectives.

In more detail, this work investigates the role of inputs derived from traffic on model performance and proposes a strategy to select the fundamental inputs for decisions, thus refining the model and improving its training and response times. The reliability of the outputs produced by the traffic classifiers is also analyzed and improved using calibration techniques.

Furthermore, the internal structure of the models is examined to locate the knowledge and the neurons crucial for specific concepts, such as class membership. This enables knowledge manipulation and allows for influencing models' performance without the need for further, particularly burdensome fine-tuning phases, which is especially challenging in the context of Large Language Models.

Additionally, the final chapter analyzes traffic classifiers trained with incremental approaches from different perspectives and through the lens of XAI to understand the reasons for their low performance and derive guidelines for training adaptable and extensible traffic classifiers.

The solutions proposed in this thesis aim to improve the integration of DL models in real-world contexts thanks to an in-depth analysis of their explainability. The developed techniques and methodologies offer new tools to better understand and improve DL models for traffic analysis, making them more transparent, reliable, and suitable for complex and evolving scenarios.

Research products

Research results appear in *6* papers published in international journals (*1* under review), *6* contributions to international conferences (*1* under review), and *1* contribution to national conferences.

List of scientific publications

International journal papers

A. Nascita, A. Montieri, G. Aceto, V. Persico, A. Pescapé, *Improving Performance, Trust, and Feasibility in Multitask Traffic Classification with XAI,* IEEE Transactions on Network and Service Management (TNSM), vol. 20, no. 2, pp. 1267-1289, June 2023, doi: 10.1109/TNSM.2023.3246794

A. Rahman, A. Montieri, D. Kundu, Md R. Karim, Md J. Islam, S. Umme, A. Nascita, A. Pescapé *On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives* - Springer's Journal of Network and Systems Management, Special Issue on Blockchains and Distributed Ledgers in Network and Service Management, vol. 30, p. 7, 2022, doi: 10.1007/s10922-022-09682-4

G. Bovenzi, A. Nascita, L. Yang, A. Finamore, G. Aceto, D. Ciuonzo, A. Pescapé, D. Rossi. *Benchmarking Class Incremental Learning in Deep Learning Traffic Classification*, IEEE Transactions on Network and Service Management (TNSM), vol. 21 (1), pp. 51-69, 2023, doi: 10.1109/TNSM.2023.3287430

W. Qin, H. Chen, L. Wang, Y. Xia, A. Nascita, A. Pescapé, *MCOTM: Mobility-Aware Computation Offloading and Task Migration for Edge Computing in Industrial IoT*, Elsevier Future Generation Computer Systems (FGCS) Journal, vol. 151, pp. 232-241, 2024, doi: 10.1016/j.future.2023.10.004

F. Cerasuolo, A. Nascita, G. Bovenzi, G. Aceto, D. Ciuonzo, A. Pescapé, D. Rossi, *MEMENTO: A Novel Approach for Class Incremental Learning of Encrypted Traffic*, Elsevier Computer Networks, vol. 245, 2024, doi: 10.1016/j.comnet.2024.110374

A. Nascita, G. Aceto, D. Ciuonzo, A. Montieri, V. Persico, and A. Pescapé, *A Survey on Explainable Artificial Intelligence for Internet Traffic Classification and Prediction, and Intrusion Detection*, submitted to IEEE Communications Surveys and Tutorials
(under second review round)

International conference papers

A. Nascita, F, Cerasuolo, D. Di Monda, J. Thern Aberia Garcia, A. Montieri, and A. Pescapè, *Machine and Deep Learning Approaches for IoT Attack Classification*, IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, May 2022, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9797971

G. Bovenzi, F. Cerasuolo, A. Montieri, A. Nascita, V. Persico, A. Pescapé, *A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic,* 2022 IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, July 2022, pp. 1-6, doi: 10.1109/ISCC55528.2022.9912986

C. Guida, A. Nascita, A. Montieri, A. Pescapé, *Cross-Evaluation of Deep Learning-based Network Intrusion Detection Systems*, 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), Marrakesh, Morocco, August 2023, pp. 328-335, doi: 10.1109/FiCloud58648.2023.00055

A. Nascita, F. Cerasuolo, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapé, *Explainable Mobile Traffic Classification: the case of Incremental Learning*, 19th International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2023), Workshop on 'Explainable and Safety Bounded, Fidelitous, Machine Learning for Networking', Paris, France, December 2023, pp. 25–31 doi: 10.1145/3630050.3630178

A. Nascita, R. Carillo, F. Giampetraglia, A. Iacono, V. Persico and A. *Pescapé, Interpretability and Complexity Reduction in Iot Network Anomaly Detection Via XAI*, 2024 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW), Seoul, Korea, Republic of, April 2024, pp. 325-329, doi: 10.1109/ICASSPW62465.2024.10626031

A. Nascita, J. Krolikowski, V. Persico, A. Pescapé, D. Rossi, *[hidden title]*, submitted to the IEEE International Conference on Computer Communications (INFOCOM) 2025 (*under double-blind review process at the date of submission of this document*)

National conference papers

A. Nascita, A. Montieri, G. Aceto, D. Ciuonzo, V. Persico, A. Pescapé, *Can XAI Tools Interpret Traffic Classifiers based on Deep Learning? Secondo Convegno Nazionale CINI sull'Intelligenza Artificiale, Torino, Italy, February 2022.*

Date 14/10/2024

PhD student signature _____

Supervisor signature _____