# Nicola Bena
# CURRICULUM VITAE

## Contents

# 1 Personal information

*Surname*: Bena
*Name*: Nicola
*Date of birth*: February 16, 1996

# 2 Short bio

## 2.1 Education

- In *January 2024* he obtained a Ph.D. in Computer Science (XXXVI Cycle) from the Università degli Studi di Milano with the grade *With Honors*.
  Thesis discussed: "Non-Functional Certification of Modern Distributed Systems". Advisor: Prof. Claudio A. Ardagna.
- From *November 2020* to *October 2023*, he attended the Ph.D. in Computer Science (XXXVI Cycle) at the Università degli Studi di Milano.
- In *April 2020*, he obtained a Master's Degree in Computer Security from the Università degli Studi di Milano with a grade of 110/110 and Honors.
  Thesis discussed: "Assurance Verifications in Next-Generation Architectures: A Certification Scheme for DevOps-Based Systems" (title translated from Italian). Advisor: Prof. Claudio A. Ardagna.
- In *October 2018*, he obtained a Bachelor's Degree in Security of Computer Systems and Networks from the Università degli Studi di Milano with a grade of 110/110 and Honors.
  Thesis discussed: "Study and Implementation of an Advanced VPN-Based Architecture for Security Assessment" (title translated from Italian). Advisor: Prof. Marco Anisetti.

## 2.2 Employment history

- Since *August 2025* he is a Tenure-track Assistant Professor at the Department of Computer Science, Università degli Studi di Milano.
- From *June 2020* to *July 2025* he has been working as a postdoctoral research fellow at the Department of Computer Science, Università degli Studi di Milano.
- Since *Gennaio 2022* he is *Secretary* of National Lab on Data Science of the Consorzio Interuniversitario Nazionale per l'Informatica (CINI).
- Since *May 2022* he has been a subject expert in Computer Networks.
- Since *February 2019* to *May 2019* and since *October 2019* to *January 2020* he obtained two external collaboration assignments, Department of Computer Science, Università degli Studi di Milano.
- Since *October 2018* he has been collaborating on the activities of the *SEcure Service-oriented Architectures Research Lab* (SESAR Lab), Department of Computer Science, Università degli Studi di Milano.

# 3 Contracts and research fellowships

- *August 2025* – today: Tenure-track Assistant Professor at the Department of Computer Science, Università degli Studi di Milano.
- *June 2023 – July 2025*: research fellow (postdoc) at the Department of Computer Science, Università degli Studi di Milano, in the context of the PNRR project *Multilayered Urban Sustainability Action (MUSA), Spoke 2 Big Data-Open Data in Life Sciences*.
- *June 2020 – May 2023*: research fellow at the Department of Computer Science, Università degli Studi di Milano, in the context of the project EU Horizon 2020 *Cyber security cOmpeteNce fOr Research anD Innovation* (CONCORDIA).
- *October 2019 – January 2020*: external collaboration assignment at the Department of Computer Science, Università degli Studi di Milano, in the context of the project EU Horizon 2020 *Cyber security cOmpeteNce fOr Research anD Innovation* (CONCORDIA).

- *February 2019 – May 2019*: external collaboration assignment at the Department of Computer Science, Università degli Studi di Milano.

# 4 Teaching activities, supplementary teaching, and student services

## 4.1 Responsibility of courses or modules for undergraduate and graduate students

He has been appointed for the following courses (course name translated from Italian), Università degli Studi di Milano.

- A.A. 2025-26: *Systems and Network Security*, Bachelor's degree in Security of Computer Systems and Networks (12 hours).
- A.A. 2025-26: *Computer Programming*, Bachelor's degree in Security of Computer Systems and Networks (Lab, 48 hours).

## 4.2 University teaching activities

He has held the following seminars as part of undergraduate/master's degree courses at Italian and foreign universities (course name translated from Italian).

- "Anonymity on the Internet: From Cookies to Tor". Lecture part of the course *Computer Networks*, Bachelor's degree in Computer Science, Università degli Studi di Napoli "Parthenope," Naples, Italy, December 2023 (2 hours).
- "Moon Cloud: a Distributed System for Security Assurance". Lecture part of the course *Cloud Computing Technologies*, Master's degree in Computer Science, Università degli Studi di Milano, Milan, Italy, June 2023 (2 hours).
- "Assurance-based Security Governance for ICT systems". Lecture part of the course *Cybersecurity Seminars*, Master's degree in Cybersecurity, Sapienza Università di Roma, Rome, Italy, April 2023 (with M. Anisetti, 2 hours).

## 4.3 University tutoring activities

He has served as a tutor for the following courses in the Bachelor's degree in Security of Systems and Computer Networks, Department of Computer Science, Università degli Studi di Milano (course name translated from Italian).

- A.Y. 2024–25: *Computer Networks (lab)* (48 hours).
- A.Y. 2023–24: *Computer Networks (lab)* (12 hours).
- A.Y. 2021–22: *Computer Networks (lab)* (18 hours).[1]
  [1] Support for hybrid teaching during the COVID-19 pandemic.
- A.Y. 2020–21: *Computer Networks* (8 hours).
- A.Y. 2019–20: *Computer Networks and Computer Networks (lab)* (75 hours)[2]
  [2] Modules delivered synchronously online during the COVID-19 pandemic.
- A.Y. 2019–20: *Model-driven Software Design* (6 CFU, 26 hours).
- A.Y. 2019–20: *Secure Software Design* (lab) (6 CFU, 26 hours).

Activities include *i)* preparation of support materials for students (exercises, handouts, supplementary materials); *ii)* lectures together with the course instructor; *iii)* participation to the commissions of exams.

He has served/serves as a teaching tutor for the following courses in the Bachelor's degree in Security of Systems and Computer Networks (online edition), Department of Computer Science, Università degli Studi di Milano (course name translated from Italian).

- A.Y. 2024–25: *Computer Networks* (12 CFU, 42 hours).
- A.Y. 2023–24: *Computer Networks* (12 CFU, 86 hours).

- A.Y. 2022–23: *Computer Networks* (12 CFU, 86 hours).
- A.Y. 2021–22: *Computer Networks* (12 CFU, 86 hours).
- A.Y. 2020–21: *Computer Networks* (12 CFU, 86 hours).
- A.Y. 2019–20: *Computer Networks* (12 CFU, 86 hours).

Activities include *i)* lessons with individual students on specific topics in synchronous mode; *ii)* correction of exercises and self-assessment exercises for students; *iii)* answering student questions asynchronously; *iv)* participation in exam committees.

### 4.4 Teaching activities in postgraduate specialization schools

He has held the following lectures within postgraduate specialization courses at the Università degli Studi di Milano (lecture titles translated from Italian):

- *January 2025*: "The evolution of supervision: AI at the workplace – certified AI," Advanced course in Data Protection and Data Governance – Employee supervision and personal data protection (2 hours, with C. A. Ardagna, V. Bellandi).
- *November 2024*: "Attacks to data: the new frontier of cybercrime in the era of big data and artificial intelligence," Advanced course in Cybercrime and Digital Investigations – The human factor (2 hours, with C. A. Ardagna)
- *November 2023*: "AI: poisoning attacks and countermeasures," Advanced Course in Cybercrime and Digital Investigations – Artificial Intelligence, attacks, cybercrimes, investigations, and ethical-social aspects (2 hours, with C. A. Ardagna).
- *June 2022*: "The metaverse from a technical and computer science perspective," Advanced Course in Big Data, Artificial Intelligence, and Platforms – Technical and legal aspects related to the use of data and their protection (2 hours, with C. A. Ardagna).
- *December 2021*: "The idea of anonymity and presenting oneself anonymously online," Online Advanced Course in Cybercrime and Digital Investigations – Investigation procedures and removal of digital content. Pornography, intellectual property, hate and terrorism, right to be forgotten, reputation protection (2 hours, with C.A. Ardagna).
- *October 2020*: "Filters and the use of tools such as VPN and Tor," Online Advanced Course in Cybercrime and Digital Investigations – Digital forensics on partner, employee, and professional infidelity and fraud on digital platforms (2 hours, with C.A. Ardagna).

### 4.5 Non-university teaching activities

He has held the following online courses.

- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtual), November 2022 (with M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtual), May 2022 (with M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtual), November 2021 (with M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtual), June 2021 (with M. Anisetti, A. Polimeno).

### 4.6 Supervisor/Co-supervisor of PhD, Master's, and Bachelor's theses

He is currently co-supervising the following PhD theses:

- Aneela Nasim (Università degli Studi di Milano), National PhD Program in Cybersecurity, XL Cycle, thesis entitled "Non-Functional Certification of AI-Based Systems"

He is currently supervising the following bachelor's theses on various topics related to security, assurance evaluation, cloud, and microservices (theses titles translated from Italian).

- Leonardo Vurchio. “Study and Implementation of Secure Boot and Digital Signature System for Building Automation IoT Devices”

He is currently co-supervising the following bachelor’s theses on various topics related to security, assurance evaluation, cloud, and microservices (theses titles translated from Italian).

- Younes Bekkali. “Design and Development of an app for the management of the assurance of distributed systems”.
- Francesco Pertile. “Design of a (Self-)Evaluation Compliance Process to the OWASP Security Requirements”
- Raphael Vauterin. “European Cybersecurity Certification”

He has co-supervised the following bachelor’s theses on various topics related to security, assurance evaluation, cloud, and microservices.

- Riccardo Aldizio. “Design and Implementation of Assurance Evaluations for Machine Learning Models”.
- Riccardo Barone. “Design and Implementation of Pipelines for Security Assurance Data Analysis”.
- Marco A. Bonissi. “Study and Implementation of a Tool for Data Exfiltration Detection”.
- Ruslan Bondaruc. “Study and Implementation of a Next-Generation IDS Based on an Edge Architecture”.
- Carlo Civardi. “Implementation of an IoT Environment for Assurance Activities Simulation”.
- Federico Colombo. “Design and Experimentation of a Certification Scheme for IoT-Based Systems”.
- Matteo dal Grande. “Study and Implementation of a DevSecOps Pipeline”.
- Alex Della Bruna. “Design and Development of an Advanced Distributed System for Security Assurance Verifications”.
- Ez Eddine Ed Daouy. “Study and Implementation of Probes for Log Collection”.
- Veronica Falgiani. “Design and Development of an Agent for Verification of Advanced Network Protocols”
- Simone Farina. “Study and Development of Assurance Probes”.
- Nicolas Ferazzini. “Robustness Evaluation of Machine Learning Models Against Poisoning Attacks”.
- Salvatore Ferrara. “Integrity Assurance for ML Models”.
- Nicolò Grecchi. “Revisiting Trust Management in Open Distributed Systems”.
- Yannick Joly. “Study and Implementation of a Monitoring-Based Security Assurance System: A School Campus Case Study”.
- Giovanni Locatelli. “Study and Implementation of a Hardening Solution for Windows”.
- Nicola Lopatriello. “A Tool for Managing the Lifecycle of Security Assurance Controls”.
- Stefano Maddé. “Study and Development of a Network Probe for Detecting Infected Email Attachments”.
- Jacopo Magagnin. “Analysis of the Publish/Subscribe Model: Architecture, Applications, and Security”.
- Giuseppe Manzo. “A System for Advanced Visualization of Assurance Indicators”.
- Michele Mastroberti. “Firewalls and Encrypted Threats”.
- Melissa Moioli. “A methodology to evaluate the reliability of dronews swarms”.
- Luca Mori. “Design and Implementation of a Risk Management Solution for Machine Learning Models”.
- Paolo Premoli. “Payment Card Industry Data Security Standard”.
- Xhanluka Rama. “Design and Development of a Tool for Automatic Security Report Generation”.
- Davide Righetti. “Explainable AI Techniques”.
- Luca Ruggeri. “Study and Implementation of a System for Automating Penetration Testing Activities”.
- Jacopo Saiani. “Explainability Verifications on ML Models”.
- Victoria Sheng. “Design, Planning, and Development of a Dashboard for Analyzing and Visualizing Security Assurance Process Results”.
- Daniel Simonini. “Study and Implementation of an Authentication System with JWT”.
- Marica Soci. “Design and Development of Security Assurance Probes for Windows-Based Environments”.

- Salvatore Sorvillo. “Data Poisoning in Federated Learning”.
- Christian Vaccarino. “Study and Implementation of Probes for Security Verification of Windows Systems”.

He is currently co-supervising the following master’s theses on various topics related to security, assurance evaluation, cloud, and microservices (theses titles translated from Italian).

- Riccardo Barone. “Studio e implementazione di un sistema di forecasting della compliance”
- Erfan Esfahanian. “Design and Development of a Trust Management System for Modern Service-Based Systems”

He has co-supervised the following master’s theses on various topics related to security, assurance evaluation, cloud, and microservices.

- Ruslan Bondaruc. “An Advanced Security Assurance System for Edge/IoT Environments”.
- Matteo Cavagnino. “Design and Development of an Assurance Methodology for Security Certifications in IoT Systems”
- Andrei Cosmin Cozmei. “Study of Security Solutions in IoT Based on Machine Learning”.
- Alex Fortunato. “Study and Implementation of a System for Assurance of Firewalls and Perimeter Security Devices”
- Marco Luzzara. “Migration of a Spend Analysis Product From an On-Premises Environment to the AWS Cloud”
- Michele Mastroberti. “Assurance Assessments of AI models”
- Emanuele Meroni. “Design and Implementation of a Composite Certification Methodology”
- Paolo G. Panero. “Managing ML-Based Application Non-Functional Behavior: A Multi-Model Approach”
- Marco Pedrinazzi. “A Transparent Certification Scheme Based on Blockchain”. **Candidate thesis of the Department of Computer Science, Università degli Studi di Milano, to the award *premio Tesi di Laurea Magistrale “con.Science 2024”*.**[1]

He has co-supervised and has supported the activities of the following PhD students (visiting students) at the Department of Computer Science, Università degli Studi di Milano, on various topics related to assurance, certification, cloud, and artificial intelligence.

- Kathrin Brecker (Karlsruhe Institute of Technology). The research activity was focused on defining next-generation certification schemes for AI-based applications.

He has co-supervised the following graduate students (visiting students) at the Università degli Studi di Milano on various topics related to security, cloud, and microservices.

- Nicolas Tourette (Université de Bourgogne). “Design and develop probes for host or network scan against malwares or viruses”.

# 5 Research activities at international research centers

- *February – April 2025*: visit at Khalifa University, Abu Dhabi, UAE (as a *visiting scholar*). The research activity, in collaboration with Prof. Chan Yeob Yeun, focused on the robustness evaluation of machine learning models against poisoning attacks.
- *June – August 2023*: visit at LIRIS Lab, INSA Lyon, Lyon, France (as a *visiting scholar*). The research activity, in collaboration with Prof. Chirine Ghedira-Guegan, Prof. Nadia Bennani, and Dr. Genoveva Vargas-Solar, focused on the definition of new methodologies for trust management in modern distributed systems.
- *February – April 2023*: visit at Khalifa University, Abu Dhabi, UAE (as a *visiting scholar*). The research activity, in collaboration with Prof. Chan Yeob Yeun, focused on the definition of new methodologies to improve the robustness of machine learning models against data poisoning attacks.

[1] Translated name: Master’s degree award “con.Science 2024”.

# 6 Research projects activities

## 6.1 Responsibility of/in research projects

Principal Investigator of the following research projects:

- Research projects funded by Università degli Studi di Milano in the context of the call Early Career Development 2025 - Line 8 of the Research Support Plan – PSR - Submeasure A – RTT Research Grant
  *Project Title*: Trustworthy Ai in COllaborative and distributed Scenarios (*TACOS*)
  *Period*: Novembre 2025 – Novembre 2027
  *Budget*: 5000 EUR
  *Activities*: Design of a methodology to support collaborative and trustworthy AI tasks in distributed scenarios.

- Research projects funded to promote the usage of the HPC resources of the University
  *Project Title*: Non-Unctional Assessment of LLM-based applications (*NULLM*)
  *Period*: July 2025 – June 2026
  *Budget*: 25 000 *core hours* on HPC cluster
  *Activities*: Definition of a new-generation certification scheme for applications based on Large Language Models (LLMs).

Work Package leader in the following research projects:

- Research projects funded by Technology Innovation Institute (TII)
  *Project Title*: Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models (*PALM*)
  *Period*: November 2020 – April 2023
  *Operational Unit*: Università degli Studi di Milano (UNIMI)
  *Budget*: 350 000 USD
  *Role*: *Work Package Leader* WP4 "Assurance methodology"
  *Activities*: Definition of a methodology and a prototype to improve the robustness of machine learning models against data poisoning attacks. The activities carried out resulted in the publication of scientific articles [IJ–7, IJ–9] in Section 12.2.2.

## 6.2 Participation in research projects

He has participated/is participating in the following research projects:

- National Recovery and Resilience Plan (PNRR)
  *Project Title*: MUSA: Multilayered Urban Sustainability Action (MUSA), Spoke 2 Big Data-Open Data in Life Sciences
  *Period*: September 2022 – August 2025
  *Operational Unit*: Università degli Studi di Milano (UNIMI)
  *Activities*: Design and development of a 5G-enabled cloud-edge digital architecture for the secure storage and exchange of big data for life sciences and to support clinical studies. The activities carried out resulted in the publication of scientific articles [IJ–3, IJ–4, IJ–5, IJ–6, IC–3, IC–5, IC–6, IC–7, IC–8] in Section 12.2.2.

- Grandi Sfide d'Ateneo (GSA) – Line 6 – Strategic Line 4: Cybersecurity/Cloud
  *Period*: 2022 – 2024
  *Project Title*: Sovereign Edge-Hub: A Cloud-Edge Architecture for Digital Sovereignty in Life Sciences (*SOV-EDGE-HUB*)
  *Activities*: Requirements gathering and analysis, design and development of the university's cloud/edge infrastructure with particular reference to non-functional aspects. The activities carried out resulted in the publication of the scientific article [IJ–2, IJ–3, IJ–4, IC–6] in Section 12.2.2.

- EU Horizon 2020 Program (SU-ICT – Boosting the effectiveness of the Security Union)
  *Project Title*: Cyber security cOmpeteNce fOr Research anD Innovation (CONCORDIA)
  *Period*: January 2019 – December 2023
  *Operational Unit*: Università degli Studi di Milano (UNIMI)

*Activities*: Definition of a series of threat reports presenting *i)* the evolution of IT security threats and vulnerabilities, *ii)* gaps and challenges in the IT security domain, and *iii)* available security countermeasures. The activities carried out resulted in the publication of scientific articles [IJ−8, IJ−10, IC−9, IC−11, IC−12, IC−13, IC−14, IC−15] and outreach articles [OP−1, OP−2] in Section 12.2.2.

In the context of his research has contributed/contributes to the research activities of the following projects:

- Research projects funded by Laboratoire d'InfoRmatique en Image et Systèmes d'information (Transversal Actions Program of the LIRIS Lab)
  *Project Title*: A fairness approach to deal with data and models in federated learning verifying an intersectional, diverse, and inclusive analytics (*FRIENDLY*)
  *Period*: January 2024 – December 2025
  *Activities*: Definition of a certification-based trust management methodology for modern distributed systems. The activities carried out resulted in the publication of the scientific articles [IC−4, IJ−5] in Section 12.2.2.

- EU Horizon 2020 Program
  *Project Title*: Intelligent Management of Processes, Ethics and Technology for Urban Safety (*IMPETUS*)
  *Period*: September 2020 – August 2022
  *Activities*: Requirements gathering and analysis, and design of the data lake infrastructure for the definition and execution of analytics to ensure *urban safety* in a smart city scenario.

# 7 Participation to national and international research groups

He participates in the activities of the following research groups:

- *Critical Information Infrastructures*, Karlsruhe Institute of Technology, Karlsruhe, Germany.
- *Laboratoire d'InfoRmatique en Image et Systèmes d'information (LIRIS)*, CNRS, INSA Lyon, Université Claude Bernard Lyon 1, Université Lumière Lyon 2, Ecole Centrale de Lyon, Lyon, France.
- *Center for Cyber-Physical Systems (C2PS)*, Khalifa University, Abu Dhabi, UAE.
- *SEcure Service-oriented Architectures Research Lab (SESAR)*, Università degli Studi di Milano, Milan, Italy.

He participates as *member* in the activities of the following consortiums:

- National Lab on Data Science of the Consorzio Interuniversitario Nazionale per l'Informatica (CINI)
- National Lab on Cybersecurity of the Consorzio Interuniversitario Nazionale per l'Informatica (CINI)

# 8 Presentations at conferences, workshops, and seminars

He has participated in the following panels at international conferences and workshops:

- "Navigating Time and Space: Diverse Perspective on Building Scientific Careers", at the conference ACS/IEEE 21st International Conference on Computer Systems and Applications (*ACS/IEEE AICCSA 2024*), Sousse, Tunisia, October 2024.

He has presented, as speaker, the following works at international conferences and workshops:

- N. Bena, M. Pedrinazzi, M. Anisetti, O. Hasan, L. Brunie, "A Transparent Certification Scheme Based on Blockchain for Service-Based Systems," in *2024 IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, China, July 2024.
- M. Anisetti, C. A. Ardagna, N. Bena, V. Giandomenico, G. Gianini, "Lightweight Behavior-Based Malware Detection," in *15th International Conference on Management of Digital Systems (MEDES 2023)*, Heraklion, Greece, May 2023.
- M. Anisetti, C. A. Ardagna, N. Bena, "Certification Meets Modern Service-Based Systems: Connecting Service and Certificate Life Cycle," in *Italian Conference on Cybersecurity (ITASEC 2023)*, Bari, Italy, May 2023.

- M. Anisetti, C. A. Ardagna, N. Bena, "A Multi-Dimensional Certification Scheme for Modern Services," in *First Conference on System and Service Quality (QualITA 2022)*, Milan, Italy, November 2022.
- C. A. Ardagna, N. Bena, R. M. de Pozuelo, "Bridging the Gap Between Certification and Software Development," in *17th International Conference on Availability, Reliability and Security (ARES 2022)*, Vienna, Austria, August 2022.
- N. Bena, R. Bondaruc, A. Polimeno, "Security Assurance in Modern IoT Systems," in *4th Workshop on Connected Intelligence for IoT and Industrial IoT Applications (C3IA)*, part of *2022 IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring)*, Helsinki, Finland, June 2022.
- M. Anisetti, C.A. Ardagna, N. Bena, R. Bondaruc, "Towards an Assurance Framework for Edge and IoT Systems," in *2021 IEEE International Conference on Edge Computing (IEEE EDGE 2021)*, Guangzhou, China, December 2021.
- M. Anisetti, C.A. Ardagna, N. Bena, A. Foppiani, "An Assurance-Based Risk Management Framework for Distributed Systems," in *2021 IEEE International Conference on Web Services (IEEE ICWS 2021)*, Chicago, IL, USA, September 2021.
- M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "Stay Thrifty, Stay Secure: A VPN-Based Assurance Framework for Hybrid Systems," in *17th International Conference on Security and Cryptography (SECRYPT 2020)*, Paris, France, July 2020 (**winner of the "Best Student Paper Award"**).

He has held the following invited seminars at international research centers/universities:

- "Trustworthy AI: Assurance, Certification, and Security", Khalifa University, Abu Dhabi, UAE, March 2025.
- "Assurance in Modern ICT Systems: From Theory to Practice". Shandong University of Technology, China, August 2023 (with M. Anisetti).
- "Distributed Systems Certification: From Services to Machine Learning". INSA Lyon, Lyon, France, June 2023.
- "Distributed Systems Certification: From Services to Machine Learning". Khalifa University, Abu Dhabi, UAE, March 2023.

He has held the following seminars/presentations:

- "Trustworthy AI: Assurance, Certification, and Security." IRIXYS Young Scientists' Workshop, Università degli Studi di Milano, Milan, Italy, October 2025.
- "Trustworthy Machine Learning-Based Applications: A Certification-Based Approach". Poster session at Third General Meeting MUSA, Bocconi University, Milan, Italy, May 2024.
- "A digital platform for data analytics pipeline management in the cloud-edge continuum". Second General Meeting MUSA, Politecnico di Milano, Milan, Italy, November 2023.
- "Security and Privacy of the Data Lake Architecture". PhD Day Hub, Università degli Studi di Milano, Milan, Italy, October 2022.
- "Bridging the Gap Between Certification and Software Development". CONCORDIA WP1 Meeting, Munich, Germany, June 2022.
- "An Assurance-Based Risk Management Framework for Distributed Systems". CONCORDIA T1.1 Meeting, July 2021.
- "Moon Cloud: a Platform for Cybersecurity". Open Day, Department of Computer Science, Università degli Studi di Milano, Milan, February 2020 (with M. Anisetti, A. Polimeno).
- "Moon Cloud: Security Governance and Compliance Verification". Open Day, Department of Computer Science, Università degli Studi di Milano, Milan, February 2019 (with P. Ceravolo).

# 9 Awards, recognitions, and certifications

## 9.1 Awards and recognitions

- **Winner of the "Best Student Paper Award"** at the international conference "17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)".
  Title of the article: "Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems".
  Co-authors: M. Anisetti, C.A. Ardagna, E. Damiani.

### 9.2 Certifications

- In *June 2015* he obtained the certification “EUCIP IT Administrator – module Information Security”

## 10 Professional and service activity

### 10.1 Participation to editorial boards of international journals

*Review editor* of the following international journals:

- *Frontiers in Big Data*, *SJR: Q2.*

Co-editor (guest editor) of the following special issues in international journals:

- Special Issue on “Towards the Next Frontier in Data Management: Data Spaces and Data Governance,” Data Science and Engineering, *SJR: Q1* (with S. Distefano, L. Romano, A. Tzouganatou)

### 10.2 Editorial activities

He has carried out reviews of works submitted to the following international journals as a *reviewer*:

- *Discover Artificial Intelligence*
- *Data Mining and Knowledge Discovery*
- *Expert Systems with Applications*
- *Discover Computing*
- *IEEE Internet of Things Journal*
- *International Journal of Data Science and Analytics*
- *International Journal of Machine Learning and Cybernetics*
- *ACM Transactions on Intelligent Systems and Technology*
- *Data and Knowledge Engineering*
- *IEEE Transactions on Affective Computing*
- *Scientific Reports*
- *Engineering Applications of Artificial Intelligence*
- *Journal of Medical Internet Research*
- *Journal of Hardware and Systems Security*
- *Cluster Computing*
- *PeerJ Computer Science*
- *Frontiers in Artificial Intelligence*
- *PLOS ONE*
- *International Journal of Intelligent Systems*
- *ACM Computing Surveys*
- *IEEE Transactions on Artificial Intelligence*
- *Computers in Biology and Medicine*
- *SN Computer Science*
- *IEEE Transactions on Cloud Computing*
- *Computers and Electrical Engineering*
- *IEEE Transactions on Network and Service Management*
- *Journal of Reliable Intelligent Environments*
- *IEEE Transactions on Services Computing*
- *Computers & Security*
- *IEEE Access*

- *Annals of Telecommunications*
- *Mobile Information Systems*

He has performed review activities for *Qeios* and for monograph proposals submitted to John Wiley and Sons publisher.

## 10.3 Organization of international conferences

Program Chair for the following conferences and workshops:

- *5th Italian Conference on Big Data and Data Science (ITADATA 2026)*, Bari, Italia, Novembre 2025 (co-chair con S. Distefano, A. Longo, G. Pio).
- *4th Italian Conference on Big Data and Data Science (ITADATA 2025)*, Turin, Italy, September 2025 (co-chair with R. Esposito, R. Torlone, M. Ceci).
- *3rd Italian Conference on Big Data and Data Science (ITADATA 2024)*, Pisa, Italy, September 2024 (co-chair with M. Natilli, G. Stilo, C. Diamantini, L. Romano).
- *ICWS Workshop on Services Regulation & Governance (SRG 2024)*, workshop part of *IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, China, July 2024 (co-chair with L. Kuang, Y. Watanabe, T. Zhao).
- *2nd Italian Conference on Big Data and Data Science (ITADATA 2023)*, Napoli, Italy, September 2023 (co-chair with B. Di Martino, A. Maratea, A. Sperduti).

Chair of *Special Sessions* for the following conferences and workshops:

- *Data Science: Multidisciplinary Perspectives to Tame the Data Revolution.* Special session at *The International Joint Conference on Neural Networks (IJCNN 2025)*, Roma, Italy, June – July 2025 (co-chair with E. Di Nardo, A. Ciaramella, C. A. Ardagna).

Member of the Organizing Committee of the following conferences and workshops:

- *3rd International Conference on Machine Intelligence and Digital Applications (MIDA 2026)*, Xi'an, China, April 2026
- *2nd International Conference on Machine Intelligence and Digital Applications (MIDA 2025)*, Ningbo, China, April 2025.

Member of the Program Committee of the following conferences and workshops:

- *3rd International Conference on Communication, Information and Digital Technologies (CIDT 2026)*, Singapore, September 2026.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2026)*, Sidney, Australia, July 2026.
- *41st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2026)*, Perth, Australia, June 2026.
- *2nd Workshop on Large Language Models for Service-Oriented Architectures and Systems Design (LLM-SOA 2026)*, workshop part of *38th International Conference on Advanced Information Systems Engineering (CAiSE 2026)*, Verona, Italy, June 2026.
- *11th International Conference on Cyber Security and Information Engineering (ICCSIE 2026)*, Xining, China, May 2026.
- *Seventeenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2026)*, April 2026, Lisbon, Portugal.
- *1st International Workshop on Distributed AI and Pervasive Computing Systems (DAPCS-2026)*, workshop part of *40th International Conference on Advanced Information Networking and Applications (AINA-2026)*, Wellington, New Zealand, March 2026.
- *The 41th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2026)*, Thessaloniki, Greece, March 2026.
- *2026 8th International Symposium on Computational and Business Intelligence (ISCBI 2026)*, Bali, Indonesia, February 2026.

- *24th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2025)*, Guiyang, China, November 2025.
- *2025 ICA3PP Workshop on Smart Education Powered by Parallel and Distributed Processing (SmartEduPP 2025)*, workshop part of ICA3PP 2025, Zhengzhou, China, October–November 2025.
- *2025 International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2025)*, Zhengzhou, China, October–November 2025.
- *The European Workshop on Trustworthy AI (TRUST-AI)*, workshop part of ECAI 2025, Bologna, Italy, October 2025.
- *3rd Workshop on Advancements in Federated Learning (WAFL)*, workshop part of ECML-PKDD 2025, Porto, Portugal, September 2025.
- *13th Workshop on New Frontiers in Mining Complex Patterns (NFMCP 2025)*, workshop part of ECML-PKDD 2025, Porto, Portugal, September 2025.
- *IEEE 6th International Conference on Computer Science and Communication Technology (IEEE ICCSCT 2025)*, Wuhan, China, August 2025.
- *2025 IEEE CSR Workshop on Synthetic Data Generation for a Cyber-Physical World (SDGCP 2025)*, workshop part of IEEE CSR 2025, Chania, Greece, August 2025.
- *2025 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2025)*, Chania, Greece, August 2025.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2025)*, Helsinki, Finland, July 2025.
- *International Workshop on Trustworthiness and Reliability in Neurosymbolic AI (TRNS-AI 2025)* workshop part of IJCNN 2025, Rome, Italy, June–July 2025.
- *2025 3rd International Conference on Communications, Computing and Artificial Intelligence (CCCAI 2025)*, Xi'an, China, June 2025.
- *2nd International Conference on Communication, Information and Digital Technologies (CIDT 2025)*, Singapore, June 2025.
- *Sixteenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2025)*, April 2025, Valencia, Spain.
- *15th International Conference on Cloud Computing and Services Science (CLOSER 2025)*, Porto, Portugal, April 2025.
- *The 40th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2025)*, Catania, March–April 2025.
- *2025 7th International Symposium on Computational and Business Intelligence (ISCBI 2025)*, Macau, China, February 2025.
- *2025 7th International Conference on Software Engineering and Computer Science (CSECS 2025)*, Taicang, China, January 2025.
- *22nd IEEE International Conference on Embedded and Ubiquitous Computing (IEEE EUC 2024)*, Sanya, China, December 2024
- *27th IEEE International Conference on Computational Science and Engineering 2024 (IEEE CSE 2024)*, Sanya, China, December 2024
- *23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2024)*, Sanya, China, December 2024
- *2024 IEEE International Conference on High Performance Computing and Communications (IEEE HPCC 2024)*, Wuhan, China, December 2024.
- *21st IEEE International Conference on Ubiquitous Intelligence and Computing (IEEE UIC 2024)*, Denarau Island, Fiji, December 2024.
- *25th International Web Information Systems Engineering conference (WISE 2024)*, Doha, Qatar, December 2024.
- *7th International Conference on Machine Learning for Networking (MLN'2024)*, Reims, France, November 2024.
- *2024 6th International Conference on Advanced Information Science and System (AISS 2024)*, Sanya, China, November 2024.

- *12th Workshop on New Frontiers in Mining Complex Patterns (NFMCP 2024)*, workshop part of ECML-PKDD 2024, Vilnius, Lithuania, September 2024.
- *2024 IEEE CSR Workshop on Synthetic Data Generation for a Cyber-Physical World (SDG 2024)*, workshop part of IEEE CSR 2024, London, United Kingdom, September 2024.
- *2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2024)*, London, United Kingdom, September 2024.
- *6th International Conference on Science of Cyber Security (SciSec 2024)*, Copenhagen, Denmark, August 2024.
- *8th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2024) During SMARTCOMP 2024, (IEEE BITS 2024)*, workshop part of IEEE SMARTCOMP 2024, Osaka, Japan, June – July 2024.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2024)*, July 2024, Shenzhen, China.
- *A Human-Centric Perspective of Explainability, Interpretability and Resilience in Computer Vision*, special session at *IEEE International Joint Conference on Neural Networks (IEEE IJCNN 2024)*, June – July 2024, Yokohama, Japan.
- *2024 5th International Conference on Computing, Networks and Internet of Things (CNIOT 2024)*, May 2024, Tokyo, Japan.
- *2024 International Conference on Communication, Information and Digital Technologies (ICCIDT 2024)*, May 2024, Wuhan, China.
- *14th International Conference on Cloud Computing and Services Science (CLOSER 2024)*, May 2024, Angers, France.
- *Fifteenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2024)*, April 2024, Venice, Italy.
- *21th IEEE International Symposium on Parallel and Distributed Processing with Applications (IEEE ISPA 2023)*, December 2023, Wuhan, China.
- *14th IEEE International Conference On Cloud Computing Technology And Science (CloudCom 2023)*, December 2023, Naples, Italy.
- *22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023)*, Exeter, United Kingdom, November 2023.
- *2023 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2023)*, Venice, Italy, July – August 2023.
- *IEEE Cloud Summit 2023*, Baltimore, MD, USA, July 2023.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2023)*, Chicago, IL, USA, July 2023.
- *7th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2023) During SMARTCOMP 2023, (IEEE BITS 2023)*, workshop part of IEEE SMARTCOMP 2023, Nashville, TN, USA, June 2023.
- *International Workshop on AI-driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP 2023)*, workshop part of IEEE INFOCOM 2023, New York, USA. May 2023.
- *4th International Conference on Computing, Networks and Internet of Things (CNIOT 2023)*, Xiamen, China, May 2023.
- *13th International Conference on Cloud Computing and Services Science (CLOSER 2023)*, Prague, Czech Republic, April 2023.
- *IEEE Global Communications Conference (IEEE GLOBECOM 2022)*, Rio de Janeiro, Brazil, December 2022.
- *5th International Conference on Machine Learning for Networking (MLN'2022)*, Paris, France, November 2022.
- *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUSTCOM 2022)*, Wuhan, China, October 2022.
- *2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022)*, Virtual, July 2022.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2022)*, Barcelona, Spain, July 2022.
- *6th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2022) During SMARTCOMP 2022, (IEEE BITS 2022)*, workshop part of IEEE SMARTCOMP 2022, Espoo, Finland, June 2022.
- *3rd International Conference on Computing, Networks and Internet of Things (CNIOT 2022)*, Qingdao, China, May 2022.
- *12th International Conference on Cloud Computing and Services Science (CLOSER 2022)*, Virtual, April 2022.

- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2021)*, Chicago, IL, USA, September 2021.
- *5th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2021) During SMARTCOMP 2021, (IEEE BITS 2021)*, workshop part of IEEE SMARTCOMP 2021, Irvine, CA, USA, August 2021.
- *2nd International Conference on Computing, Networks and Internet of Things (CNIOT 2021)*, Beijing, China, May 2021.
- *3rd International Conference on Machine Learning for Networking (MLN'2020)*, Paris, France, November 2020.

He has carried out reviews of works submitted to the following international conferences as a *sub-reviewer*:

- *IEEE International Conference on Web Services ICWS 2025*, Helsinki, Finland, July 2025.
- *40th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2025)*, Maribor, Slovenia, May 2025.
- *The 7th International Conference on Attacks and Defenses for Internet-of-Things (ADIoT 2024)*, Hangzhou, China, December 2024.
- *20th International Conference on Information Systems Security (ICISS 2024)*, Jaipur, India, December 2024.
- *International Conference on Security for Information Technology and Communications (SecITC 2024)*, Bucharest, Romania, November 2024.
- *39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024)*, Edinburgh, United Kingdom, June 2024.
- *18th International Conference on Information Systems Security (ICISS 2022)*, Tirupati, India, December 2022.
- *37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2022)*, Copenhagen, Denmark, June 2022.
- *37th ACM/SIGAPP Symposium on Applied Computing (ACM SAC 2022)*, Brno, Czech Republic, April 2022.
- *14th IEEE/ACM International Conference on Utility and Cloud Computing (IEEE/ACM UCC 2021)*, Leicester, United Kingdom, December 2021.
- *6th International Conference on Systems, Control and Communications (ICSCC 2021)*, Chongqing, China, October 2021.
- *36th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2021)*, Oslo, Norway, June 2021.
- *19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)*, Guangzhou, China, December 2020 – January 2021.
- *International Conference on Security and Privacy in Digital Economy (SPDE 2020)*, Quzhou, China, October – November 2020.
- *2020 IEEE International Conference on Cloud Computing (IEEE CLOUD 2020)*, Beijing, China, October 2020.
- *11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019)*, Sydney, Australia, December 2019.

He was *publication chair* of the following conferences:

- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milan, Italy, September 2022.

He was *publicity chair* of the following conferences:

- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2024)*, Shenzhen, China, July 2024.
- *IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, China, July 2024.
- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milan, Italy, September 2022.
- *Big Data and Data Science for Next-Generation Distributed Systems (BDDS 2022)*, workshop part of *IEEE World Congress on Computational Intelligence (IEEE WCCI 2022)*, Padua, Italy, July 2022.
- *IEEE World Congress on Services (IEEE SERVICES 2022)*, Barcelona, Spain, July 2022.
- *IEEE World Congress on Services (IEEE SERVICES 2021)*, Chicago, IL, USA, September 2021.

He was *session chair* for the following conferences:

- *4th Italian Conference on Big Data and Data Science (ITADATA 2025)*, Turin, Italy, September 2025.
- *3rd Italian Conference on Big Data and Data Science (ITADATA 2024)*, Pisa, Italy, September 2024.
- *IEEE International Conference on Web Services (IEEE ICWS 2022)*, Barcelona, Spain, July 2022.

### 10.4 Evaluation activity

He has been *evaluator* in the context of national competitive selection procedures for:

- Research projects of "Deutsche Forschungsgemeinschaft" (*German Research Foundation*) [2025]

### 10.5 Service activity

- Since *September 2023* he is chair of the organization of the seminar series "Tales on Data Science and Big Data Science" of the National Lab on Data Science of CINI (co-chair with G. Ruffo).
- Since *January 2022* he is *Secretary* of the National Lab on Data Science of Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

## 11 Other activities: third mission and technology transfer

### 11.1 Third mission

He has carried out the following activities for the third mission:

- Practical lecture "AI: Attacks and Defenses," and presentation of the degree courses offered by the Department of Computer Science, Università degli Studi di Milano, at high school ITIS E. Majorana, Seriate (BG), Italy, March 21, 2024.
- "Multi-Dimensional Certification of Artificial Intelligence". Part of *Building Bridges through Multidisciplinary Cooperation: Perspective Approaches for Inclusive Artificial Intelligence*, Milan, May 2023.
- "Moon Cloud: Security Governance and Compliance Verification". Milan Digital Week, Milan, March 2019.

### 11.2 Technology Transfer

He has contributed/contributes to the following technology transfer activities:

- Since *November 2018*, he has been collaborating with Moon Cloud srl, an innovative startup and spin-off of the Università degli Studi di Milano, for the evaluation and monitoring of IT system security.

# 12 Scientific publications

## 12.1 Description of the research activities

The research activity has mainly focused on the security of modern distributed systems, with particular reference to assurance evaluation and the definition of certification techniques for applications *i)* deployed in cloud-edge environments and service architectures, and *ii)* based on Machine Learning (ML) models. The research activity has also contributed to the definition and development of new trust management techniques for distributed systems. Below is a classification of the topics covered by the research, briefly describing the problems addressed and the main results obtained. The bibliographic entries refer to the list of publications reported in Section 12.2.2 and are classified according to the following convention: IJ (International Journals), IC (International Conferences and Workshops), IS (In Submission).

**Assurance and certification of applications in modern distributed systems.** Modern distributed systems are characterized by a highly complex structure with interdependencies between different services. The service lifecycle is highly automated and characterized by frequent releases and deployments; applications are dynamically created by continuously composing and replacing these services according to functional requirements. In this scenario, it becomes essential to ensure that these applications also support a set of non-functional requirements. The research activity, within the research projects *CONCORDIA*, *SOV-EDGE-HUB*, and *MUSA*, has focused on *i)* the definition of new certification schemes [IC−6, IC−7, IJ−10]; *ii)* the definition of methodologies to facilitate the adoption of certification by reducing its costs [IC−9] and removing assumptions that make existing certification schemes inapplicable [IC−5]; and *iii)* the use of certification in real case studies [IJ−8, IC−10, IC−11, IC−12, IC−13, IC−14, IC−15].
Regarding research line *i)*, in [IC−7], the main deficiencies of existing certification techniques in relation to modern distributed systems were analyzed. Subsequently, a manifesto was defined to guide certification research in the coming years, identifying the macro-areas of research to be developed and their temporal placement in the short, medium, and long term, along with related research lines that can contribute to research in the identified macro-areas. In [IJ−10], a new certification scheme was defined that expands the scope of non-functional verification compared to traditional certification schemes. The issued certificates are *multi-dimensional* and evaluate different aspects (*dimensions*) that impact the non-functional property of the service/application under examination. These dimensions include, for example, the software artifacts and the development process used for the implementation of the service/application. This latter dimension, in particular, has never been considered before in the literature. Multi-dimensional certificates provide a more accurate picture of the service/application under examination and contribute to the management of its lifecycle. This work was further extended in [IC−6], addressing the problem of *continuous* certification. The scheme in [IC−6] defines a new certificate lifecycle capable of following and semi-automatically adapting to the evolution of the service/application under examination. This lifecycle reduces the impact of the service/application evolution on the validity of the certificate itself, minimizing the costs of maintaining the certification. To achieve this, the proposed solution relies on an ML algorithm.
Regarding research line *ii)*, in [IC−9], a methodology based on multi-objective genetic algorithms was defined to facilitate the integration of certification within the software development cycle. Indeed, certification has always been an activity performed at the end of the development process, introducing high costs and inefficiencies. The proposed methodology is based on the definition of the properties to be certified at development time; these properties will guide the software implementation. In [IC−5], numerous unrealistic assumptions regarding the use of certification were removed, related to the need to blindly trust the numerous involved actors. The literature has long recognized the problematic nature of these assumptions, but no valid technical solution has been provided. The proposed solution consists of adopting a blockchain to support the removal of the *blind trust* assumption. In this regard, the actors and their actions are mapped into constructs for the blockchain, and new constructs are defined to increase the transparency of the certification process.
Regarding research line *iii)*, in [IC−13] a risk management process integrated with assurance and certification activities was defined. The integration of assurance allows for more accurate results, providing a *risk posture* that is more adherent to reality. Continuing with what was defined in [IC−9], in [IC−10] the integration of assurance controls within a DevSecOps pipeline of Big Data analytics was proposed, introducing assurance checks at every stage of the pipeline. In [IJ−8] a methodology was defined to guide the *deployment* of Big Data pipelines based on non-functional requirements. The requirements are compared with the properties of the services to be recruited in the pipeline, and a monitoring process continuously evaluates that these requirements are supported by the chosen services. If not, new services are re-negotiated with the providers to ensure that the pipeline meets the set requirements. In [IC−11, IC−12] the requirements to support the certification scheme in research line *i)*

were identified, focusing on the peculiarities of the (IoT-)edge-cloud paradigm, characterized by high component volatility; the corresponding *assurance framework* was then implemented. The same problem was addressed in [IC–14, IC–15], focusing on the need for automation and the peculiarities of hybrid systems, where the private components of the systems to be verified still play an important role and need to be evaluated while limiting the impact on the systems themselves.

**Assurance and certification of ML-based applications.** The growing spread of ML-based applications and their increasing use in critical contexts introduces an ever-pressing need for assurance and certification techniques capable of verifying their non-functional properties. The research activity, carried out within the research project *MUSA* and in the context of the collaboration with Khalifa University (research project *PALM*), has focused on the definition and practical application of certification schemes for ML-based applications.
First, in [IJ–6], the peculiarities of ML-based applications and their impact on existing certification techniques were analyzed, identifying the main research challenges in this regard. Subsequently, a first adaptation of the multi-dimensional certification scheme in [IJ–10] was proposed. The scheme focuses on three relevant dimensions for ML: dataset, training process, and ML model; the scheme has been further refined in [IC–1].
Subsequently, the research activity focused on verifying the property of *robustness* against *training time* (*poisoning*) attacks [IJ–7, IJ–2, IS–2] and *inference time* attacks [IC–8, IJ–4]. Regarding robustness at training time, in [IJ–7] a technique was defined to improve the robustness of ML models against data poisoning attacks. The technique consists of replacing the base ML model with an *ensemble* of models, each trained on a disjoint portion of the training dataset. The quality of the proposed technique was validated against poisoning attacks in an extensive experimental setting using *random forest* models. In [IJ–2], an advanced technique for the same purpose was defined. It is based on an ensemble, where the training set of each model of the ensemble is defined on the basis of a *risk index* computed for each data point in the training set. The quality of the proposed technique was validated against *semi-targeted* poisoning attacks in an extensive experimental setting.
Regarding robustness at inference time, in [IC–8] a new approach for malware detection based on ML was presented. The malware detector proposes an innovative low-invasive approach, collecting data from the system to be analyzed without requiring any access privileges. The malware detector was subsequently certified in [IJ–4], along with two existing approaches in the literature, for non-functional properties accuracy, privacy, and robustness. For this purpose, the certification scheme defined in [IJ–6] was used. The property of robustness was finally studied in specific contexts, such as the processing of electroencephalography signals [IJ–9].
Finally, in [IJ–3], a new methodology for the run-time management of ML-based application has been introduced. The methodology is based on dynamic Multi-Armed Bandit (MAB), which evaluates the behavior of the ML-based application with respect to a given non-functional property. A worsening in such behavior triggers a model substitution process ensuring the stability of the application non-functional behavior.

**Trust management.** Trust management is the process by which two parties (typically a user and a service) establish a trust relationship before conducting a transaction. It has been a widely investigated research area since the early 2000s, but then relatively lost importance. However, the advent of applications often distributed among multiple providers and, more generally, involving various parties with conflicting interests, is increasingly demanding a rethinking of trust management techniques. In [IJ–5], in the context of collaboration with the inter-university LIRIS laboratory in Lyon (research project *FRIENDLY*), the peculiarities of modern applications and their impact on existing trust management techniques were analyzed. Based on the identified challenges, a *research roadmap* was defined, identifying a series of macro-research actions distributed over the short, medium, and long term. In [IC–4, IC–2], the roadmap has been further refined and preliminary instantiated in the context of fair resource allocation in federated learning tasks [IC–4] and, more in general, data science pipelines [IC–2].

## 12.2 Publications

Data retrieved from the Google Scholar profile `https://scholar.google.com/citations?user=dTTH3GgAAAAJ`

- Data retrieved on November 22nd, 2025.
- *h-index*: 11
- *Total number of citations*: 231

Data retrieved from the SCOPUS profile `https://www.scopus.com/authid/detail.uri?authorId=57344643500`

- Data retrieved on November 22nd, 2025.

- *h-index*: 8
- *Total number of citations*: 138

### 12.2.1 Summary of the publications

The research activity resulted in several publications listed in Section 12.2.2 and classifiable as follows.

- **5 Edited Volumes** [CV–1, . . . , CV–5]
- **10 peer-reviewed publications in International Journals** [IJ–1, . . . , IJ–10] of which
  - 9 with SJR *Q1*
  - 1 with SJR *Q2*
- **15 peer-reviewed publications in proceedings of International Conferences and Workshops** [IC–1, . . . , IC–15]
- **3 Book Chapters** [BC–1, . . . , BC–3]
- **1 Ph.D Thesis** [PT–1]
- **2 Other Publications** [OP–1, OP–2]
- **2 Papers In Submission** [IS–1, IS–2]

### 12.2.2 Publications list

**Edited books**

CV–1 N. Bena, M. Ceci, R. Esposito, R. Torlone, A. Della Bruna, C. A. Ardagna, M. Polato, L. Romano (eds.), "Proceedings of the 4th Italian Conference on Big Data and Data Science (ITADATA 2025)", CEUR-Workshop, 2026.

CV–2 N. Bena, C. Diamantini, M. Natilli, L. Romano, G. Stilo, V. Pansanella, C. A. Ardagna, A. Monreale, R. Trasarti (eds.), "Proceedings of the 3rd Italian Conference on Big Data and Data Science (ITADATA 2024)", arXiv, 2025.

CV–3 N. Bena, C. Diamantini, M. Natilli, L. Romano, G. Stilo, V. Pansanella, C. A. Ardagna, A. Monreale, R. Trasarti, V. Cesare, G. Mittone, E. De Rubeis, A. Vecchiato (eds.), "Workshop Scientific HPC in the pre-Exascale era (part of ITADATA 2024) Proceedings", arXiv, 2025.

CV–4 N. Bena, B. Di Martino, A. Maratea, A. Sperduti, E. Di Nardo, A. Ciaramella, R. Montella, C. A. Ardagna (eds.), "Proceedings of the 2nd Italian Conference on Big Data and Data Science (ITADATA 2023)," CEUR-Workshop, 2023.

CV–5 M. Anisetti, A. Bonifati, N. Bena, C. A. Ardagna, D. Malerba (eds.), "Proceedings of the 1st Italian Conference on Big Data and Data Science (ITADATA 2022)," CEUR-Workshop, 2022.

**Papers in international journals**

IJ–1 K. Brecker, S. Lins, N. Bena, C. A. Ardagna, M. Anisetti, A. Sunyaev, "AI Impermanence: Achilles' Heel for AI Assessment?" *IEEE Access*, vol. 13, 2025. *DOI: 10.1109/ACCESS.2025.3631309*

IJ–2 N. Bena, M. Anisetti, E. Damiani, C. Y. Yeun, C. A. Ardagna, "Protecting Machine Learning from Poisoning Attacks: a Risk-Based Approach," *Computers & Security*, vol. 155, 2025. *DOI: 10.1016/j.cose.2025.104468*

IJ–3 M. Anisetti, C. A. Ardagna, N. Bena, E. Damiani, P. G. Panero, "Continuous Management of Machine Learning-Based Application Behavior," in *IEEE Transactions on Services Computing*, vol. 18, no. 1, 2025. *DOI: 10.1109/TSC.2024.3486226*

IJ–4 N. Bena, M. Anisetti, G. Gianini, C. A. Ardagna, "Certifying Accuracy, Privacy, and Robustness of ML-Based Malware Detection," in *SN Computer Science*, vol. 5, 2024. *DOI: 10.1007/s42979-024-03024-8*

IJ–5 C. A. Ardagna, N. Bena, N. Bennani, C. Ghedira-Guegan, N. Grecchi, G. Vargas-Solar, "Revisiting Trust Management in the Data Economy: A Road Map," in *IEEE Internet Computing*, vol. 28, no. 4, 2024. *DOI: 10.1109/MIC.2024.3398403*

IJ–6 M. Anisetti, C. A. Ardagna, N. Bena, E. Damiani, "Rethinking Certification for Trustworthy Machine-Learning-Based Applications," in *IEEE Internet Computing*, vol. 27, no. 6, 2023. *DOI: 10.1109/MIC.2023.3322327*

IJ–7 M. Anisetti, C. A. Ardagna, A. Balestrucci, N. Bena, E. Damiani, C. Y. Yeun, "On the Robustness of Random Forest Against Untargeted Data Poisoning: An Ensemble-Based Approach," in *IEEE Transactions on Sustainable Computing*, vol. 8, no. 4, 2023. *DOI: 10.1109/TSUSC.2023.3293269*

IJ–8 C. A. Ardagna, N. Bena, C. Hebert, M. Krotsiani, C. Kloukinas, G. Spanoudakis, "Big Data Assurance: An Approach Based on Service-Level Agreements," in *Big Data*, vol. 11, no. 3, 2023. *DOI: 10.1089/big.2021.0369*

IJ–9 Z. Zhang, S. Umar, Y. Al Hammadi, S. Yoon, E. Damiani, C. A. Ardagna, N. Bena, C. Y. Yeun, "Explainable Data Poison Attacks on Human Emotion Evaluation Systems based on EEG Signals," in *IEEE Access*, vol. 11, 2023. *DOI: 10.1109/ACCESS.2023.3245813*

IJ–10 M. Anisetti, C. A. Ardagna, N. Bena, "Multi-Dimensional Certification of Modern Distributed Systems," in *IEEE Transactions on Services Computing*, vol. 16, no. 3, 2023. *DOI: 10.1109/TSC.2022.3195071*

### Papers in proceedings of internal conferences and workshops

IC–1 M. Anisetti, C. A. Ardagna, N. Bena, A. Nasim, "Towards the Assessment of Trustworthy AI: A Catalog-Based Approach." In *Proc. of TRUST-AI 2025*, Bologna, Italy, October 2025. *URL: https://ceur-ws.org/Vol-4132/short42.pdf*

IC–2 G. Vargas-Solar, J.-L. Zechinelli-Martini, C. A. Ardagna, N. Bena, N. Bennani, B. Catania, J. A. Espinosa-Oviedo, C. Ghedira-Guegan, A. Mauri, "Techno/Ecofeminism in Action: Fair and Responsible Resource Allocation for Sustainable Data Science Pipelines". In *Proc. of EDBT/ICDT-WS 2025*, Barcelona, Spain, March 2025. *URL: https://ceur-ws.org/Vol-3946/DARLI-AP-15.pdf*

IC–3 M. Anisetti, C. A. Ardagna, N. Bena, E. Damiani, C. Y. Yeun, S. Yoon, "Trusting Data Updates to Drone-based Model Evolution". In *Proc. of GENZERO 2024*, Abu Dhabi, UAE, November 2024. *DOI: 10.1007/978-981-95-1050-4_10*

IC–4 G. Vargas-Solar, N. Bennani, J. A. Espinosa-Oviedo, A. Mauri, J.-L. Zechinelli-Martini, B. Catania, C. A. Ardagna, N. Bena. "Decolonizing Federated Learning: Designing Fair and Responsible Resource Allocation". In *Proc. of ACS/IEEE 21st International Conference on Computer Systems and Applications (ACS/IEEE AICCSA 2024)*, Sousse, Tunisia, October 2024. *DOI: 10.1109/AICCSA63423.2024.10912594*

IC–5 N. Bena, M. Pedrinazzi, M. Anisetti, O. Hasan, L. Brunie, "A Transparent Certification Scheme Based on Blockchain for Service-Based Systems," In *Proc. of 2024 IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, China, July 2024 (**Acceptance factor 19.56%**)

IC–6 M. Anisetti, C. A. Ardagna, N. Bena, "Continuous Certification of Non-Functional Properties Across System Changes," in *Proc. of the 21st International Conference on Service-Oriented Computing (ICSOC 2023)*, Roma, Italia, November – December 2023 (**Acceptance factor 17%**). *DOI: 10.1007/978-3-031-48421-6_1*

IC–7 C. A. Ardagna, N. Bena, "Non-Functional Certification of Modern Distributed Systems: A Research Manifesto," in *Proc. of 2023 IEEE International Conference on Software Services Engineering (IEEE SSE 2023)*, Chicago, IL, USA, July 2023 *(invited paper)*. *DOI: 10.1109/SSE60056.2023.00020*

IC–8 M. Anisetti, C. A. Ardagna, N. Bena, V. Giandomenico, G. Gianini, "Lightweight Behavior-Based Malware Detection," in *Proc. of the 15th International Conference on Management of Digital Systems (MEDES 2023)*, Heraklion, Greece, May 2023. *DOI: 10.1007/978-3-031-51643-6_17*

IC–9 C. A. Ardagna, N. Bena, R. M. de Pozuelo, "Bridging the Gap Between Certification and Software Development," in *Proc. of the 17th International Conference on Availability, Reliability and Security (ARES 2022)*, Vienna, Austria, August 2022 (**Acceptance factor 20.33%**). *DOI: 10.1145/3538969.3539012*

IC–10 M. Anisetti, N. Bena, F. Berto, G. Jeon, "A DevSecOps-based Assurance Process for Big Data Analytics," in *Proc. of 2022 IEEE International Conference on Web Services (IEEE ICWS 2022)*, Barcelona, Spain, July 2022. *DOI: 10.1109/ICWS55610.2022.00017*

IC–11 N. Bena, R. Bondaruc, A. Polimeno, "Security Assurance in Modern IoT Systems," in *Proc. of 2022 IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring)*, Helsinki, Finland, June 2022. *DOI: 10.1109/VTC2022-Spring54318.2022.9860757*

IC–12 M. Anisetti, C.A. Ardagna, N. Bena, R. Bondaruc, "Towards an Assurance Framework for Edge and IoT Systems," in *Proc. of 2021 IEEE International Conference on Edge Computing (IEEE EDGE 2021)*, Guangzhou, China, December 2021. *DOI: 10.1109/EDGE53862.2021.00015*

IC–13 M. Anisetti, C.A. Ardagna, N. Bena, A. Foppiani, "An Assurance-Based Risk Management Framework for Distributed Systems," in *Proc. of 2021 IEEE International Conference on Web Services (IEEE ICWS 2021)*, Chicago, IL, USA, September 2021 (**Acceptance factor 23.7%**). *DOI: 10.1109/ICWS53863.2021.00068*

IC–14 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "An Assurance Framework and Process for Hybrid Systems," in *Proc. of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)*, Paris, France, July 2020. *DOI: 10.1007/978-3-030-90428-9_4*

IC–15 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "Stay Thrifty, Stay Secure: A VPN-Based Assurance Framework for Hybrid Systems," in *Proc. of the 17th International Conference on Security and Cryptography (SECRYPT 2020)*, Paris, France, July 2020 (**winner of the prize "Best Student Paper Award"**). *DOI: 10.5220/0009822600980109*

### Chapters in books/encyclopedias

BC–1 C.A. Ardagna, N. Bena, "Location Information (privacy of)," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021. *DOI: 10.1007/978-3-642-27739-9_755-2*

BC–2 C.A. Ardagna, N. Bena, "Privacy-Aware Languages," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021. *DOI: 10.1007/978-3-642-27739-9_881-2*

BC–3 C.A. Ardagna N. Bena, "XML-Based Access Control Languages," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021. *DOI: 10.1007/978-3-642-27739-9_833-2*

### Ph.D Thesis

PT–1 N. Bena, "Non-Functional Certification of Modern Distributed Systems," Ph.D Thesis in Computer Science, Advisor: Prof. Claudio A. Ardagna, Co-advisor: Prof. Marco Anisetti, Università degli Studi di Milano, January 2024

### Other publications

OP–1 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, J. Sessa, "Countermeasures and Research Actions," in *CONCORDIA blog*, 2022. `https://www.concordia-h2020.eu/blog-post/countermeasures-and-research-actions/`

OP–2 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, J. Sessa, "Threats, Gaps and Challenges in the Era of COVID-19," in *CONCORDIA blog*, 2021. `https://www.concordia-h2020.eu/blog-post/threats-gaps-and-challenges-in-the-era-of-covid-19/`

### Papers in submission

IS–1 N. Bena, M. Anisetti, E. Damiani, A. Della Bruna, C. Y. Yeun, C. A. Ardagna, "A Certification Scheme for Large Language Models-Based Applications" (submitted to *ACM Transactions on Intelligent Systems and Technology*), 2025

IS–2 M. Ramirez Aguilar, S.-K. Kim, S. Yoon, E. Damiani, H. Al Hamadi, C. A. Ardagna, N. Bena, A. Almahmoud, C. Y. Yeun, “Blockchain in the Context of Poisoning Attacks and Defenses: A Survey” (submitted to *ACM Computing Surveys*), 2023

Date: February 5, 2026 Location: Milan