PERSONAL INFORMATION

Giuseppina Andresini

Work address	Dipartimento di Informatica, Università degli Studi di Bari Aldo Moro, via Orabona 4, 70125 Bari, Italy
Phone	+39 080 5442203
E-mail	giuseppina.andresini@uniba.it
Google Scholar	scholar.google.com/citations?user=dWNTRHcAAAAJ
Scopus Author ID	57204829656
Nationality	Italian

WORK EXPERIENCE

Oct 2025 - today

Tenure-track Assistant Professor (RTD-B), Computer Science

SSD INFO-01/A. Department of Computer Science, University of Bari Aldo Moro, Bari (Italy).

Feb 2023 - Oct 2025

Fixed-term Assistant Professor (RTD-A), Computer Engineering

SSD ING-INF/05 (now IINF-05/A). Department of Computer Science, University of Bari Aldo Moro, Bari (Italy). Position funded by the PNRR project FAIR – Future Artificial Intelligence Research, on “Understandability of AI systems to improve robustness of decision models”.

Nov 2021 - Feb 2023

Postdoctoral Research Fellow, Computer Engineering

SSD ING-INF/05 (now IINF-05/A). Department of Computer Science, University of Bari Aldo Moro, Bari (Italy). Research topic: “Synthesis of Artificial Intelligence techniques to support cyber-defence”.

EDUCATION AND TRAINING

Mar 2022

PhD in Computer Science and Mathematics (XXXIV cycle)

University of Bari Aldo Moro (Italy). Thesis: “Innovative Machine Learning techniques for Cybersecurity”. University PhD scholarship. The thesis received the con.Scienze Prize 2021–2022 as best PhD thesis in Computer Science.

2018

MSc in Computer Science, 110/110 cum laude

University of Bari Aldo Moro (Italy). Thesis in Data Mining on the discovery and characterisation of macroscopic changes in complex data.

PHD PROGRAMMES

PhD Board

2026 - today — **Member of the PhD Board** (Collegio dei Docenti), PhD Programme in Computer Science, University of Bari Aldo Moro (XLII cycle)

PhD courses

Jun 2026 — **Bridging Adversarial Learning and Data-Centric AI for Robust AI** (15 hours, 1 CFU), PhD School in Computer Science and Mathematics, University of Bari Aldo Moro (XLI cycle)

Jun 2025 — **Artificial Intelligence Techniques for Remote Sensing** (8 hours, 1 CFU), PhD School in Computer Science and Mathematics, University of Bari Aldo Moro (XL cycle)

Jan 2024 — **Transparency and Explainability in Artificial Intelligence** (30 hours, 4 CFU), competenze trasversali course for PhD students, University of Bari Aldo Moro

Nov - Dec 2023 — **Understanding Symbiotic AI Systems to Improve Robustness of Models** (31 hours, 3 CFU, in English), PhD School in Computer Science and Mathematics, University of Bari Aldo Moro (XXXIX cycle)

Jun 2022 — **Advanced Machine Learning for Cyber Defence** (16 hours, 2 CFU, in English), PhD School in Computer Science and Mathematics, University of Bari Aldo Moro (XXXVII cycle)

Co-supervision of PhD students

XXXVIII cycle — **Dr. Luca De Rose** (supervisor: Prof. Annalisa Appice), PhD in Computer Science and Mathematics, University of Bari Aldo Moro (Computer Science curriculum)
Thesis topic: “Leveraging XAI in Defensive Adversarial Learning”.

XXXIX cycle — **Dr. Vito Recchia** (supervisor: Prof. Annalisa Appice), PhD in Computer Science and Mathematics, University of Bari Aldo Moro (Computer Science curriculum)
Thesis topic: “Data-Centric AI approaches in Symbiotic AI”.

PhD evaluation committees and thesis review

2025 - today — **Member of the evaluation committee** of PhD candidate Dr. Flavia Fazio (“Numerical Algorithms for Remote Sensing Image Processing”, XLI cycle), PhD in Computer Science and Mathematics, University of Bari Aldo Moro

RESEARCH INTERESTS

Main research activity is in **Artificial Intelligence**, in particular **Machine Learning, Deep Learning, Adversarial Learning and eXplainable AI (XAI)**, and their applications to **Cybersecurity** (malware detection, network intrusion detection, review spam detection) and **Remote Sensing** (change detection, semantic segmentation of satellite images, forest health monitoring).

PUBLICATIONS

Co-author of **45 publications** (2018–2026): **17 papers in international journals** (e.g., Information Sciences, Expert Systems with Applications, Future Generation Computer Systems, Knowledge-Based Systems, Computers & Security, Machine Learning, Data Mining and Knowledge Discovery, IEEE JSTARS), **4 book chapters** and **24 papers in conference and workshop proceedings** (e.g., AISec@ACM CCS, ECML-PKDD, Discovery Science, IEEE EuroS&P Workshops, ACM SAC, IEEE IGARSS).
A full list is available at: Google Scholar profile

BIBLIOMETRIC INDEXES

Scopus: Citations: 1200, H-index: 17 (October 2026)
Google Scholar: Citations: 1683, H-index: 20, i10-index: 26 (October 2026)

HONOURS AND AWARDS

2026 — Winner of the ISCRA-C call (CINECA) with project VISERION: 68,000 hours on the Leonardo-Booster supercomputer

2024 — Winner of the ERC SEEDS UniBa call with project AI-CREED (12th out of 77 applications)

2024 — Winner of the ISCRA-C call (CINECA) with project GARRETT: 80,000 hours on the Leonardo-Booster supercomputer

2023 — con.Scienze Prize 2021–2022 for the best PhD thesis in Computer Science, awarded by the National Conference of Presidents and Directors of University Science and Technology Structures

2022 — Best paper award, the 7th IEEE Cyber Science and Technology Congress (CyberSciTech 2022), for “An XAI-based adversarial training approach for cyber-threat detection”

RESEARCH PROJECTS

Principal Investigator

2026 — **VISERION** “adVanclng SEcuRe and explaInable reasONing for trustworthy AI” – ISCRA-C, CINECA (68,000 hours on Leonardo-Booster)

2024 - 2025 — **AI-CREED** “Enhancing Robustness in Artificial Intelligence for Cybersecurity through Explainability and Adversarial Learning” – ERC SEEDS UniBa (€10,000)

2024 — **GARRETT** “Graph neurAl netwoRks for cybeR thrEaT deTection” – ISCRA-C, CINECA (80,000 hours on Leonardo-Booster), with Prof. Annalisa Appice (co-PI) and Dr. Giuseppe Fiameni (NVIDIA AI Technology Center Italy)

Participant / collaborator

2023 - 2026 — **PNRR FAIR** – Future Artificial Intelligence Research (PE00000013), Spoke 6 “Symbiotic AI”, WP 6.4 “Understandability of AI Systems”

2023 - 2026 — **EU SWIFTT** – Satellites for Wilderness Inspection and Forest Threat Tracking (Grant Agreement 101082732)

2019 - 2021 — **PON TALIsMan** – Tecnologie di Assistenza personALizzata per il Miglioramento della quAlità della vitA (ARS01_01116), PON R&I 2014–2020

INTERNATIONAL COLLABORATIONS

Mar 2021 - Jul 2021 — **Research internship** (4 months, remote due to COVID-19) at S2Lab – Systems Security Research Lab, King’s College London (UK), supervised by Prof. Lorenzo Cavallaro

Nov 2022 — **Visiting researcher** at the DM2L team, LIRIS lab, INSA Lyon (France), with Prof. Céline Robardet

2022 - today — **Research collaboration** with Dr. Dino Ienco, INRAE UMR TETIS, University of Montpellier (France)

SCIENTIFIC RESPONSIBILITIES

Organisation of scientific events

2026 **PhD Forum Chair** – European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2026), Naples (I)

2026 **Program Co-Chair** – 28th International Symposium on Methodologies for Intelligent Systems (ISMIS 2026), Lyon (France)

2026 **Program Co-Chair** – 1st International Workshop on Secure and Trustworthy AI (STAI), co-located with ECML PKDD 2026

2026 **Workshop Chair** – 5th Italian Conference on Big Data and Data Science (ITADATA 2026), Bari (Italy)

2021 - 2024 **Program Co-Chair** – International Workshop on Machine Learning for Cybersecurity (MLCS), co-located with ECML PKDD (4 editions)

2023 **Organising Committee** – 3rd International Joint Conference on Learning & Reasoning (IJCLR 2023), Bari (Italy)

2023 **Local Co-Chair** – 9th International School on Deep Learning (DeepLearn 2023 Spring), Bari (Italy)

Editorial activities

2026 - today **Associate Editor** – International Journal of Data Science and Analytics (Springer); Discover Artificial Intelligence (Springer)

2024 - today **Editorial Board Member** – Machine Learning Journal (Springer)

2021 - 2024 **Guest Editor** of the special issues “Explainable AI for Secure Applications” (Machine Learning, Springer) and “AI meets Cybersecurity” (Journal of Intelligent Information Systems, Springer); co-editor of the Springer proceedings of the ECML PKDD 2021 and 2022 International Workshops

Program committees, invited talks and tutorials

Program committee member of international conferences including IJCAI, ICDE, VLDB (PVLDB Review Board), ECAI, ECML PKDD, Discovery Science, ACM SAC, IJCNN, IGARSS and the World Conference on XAI, and of workshops including AISec@ACM CCS and XAISec@IEEE EuroS&P. Reviewer for several international journals (e.g., IEEE TKDE, Information Sciences, ESWA, Computers & Security, DAMI, Machine Learning, EAAI).

Invited speaker at TAIC@ITASEC 2025 and MACLEAN@ECML PKDD 2024; **tutorial** “XAI in Cybersecurity” at ITADATA 2023; **lecturer** at the 3rd European Summer School on Artificial Intelligence (ESSAI 2025) and at the SERICS Summer School on Technology and Politics in Cybersecurity (2025).