

Nicola Bena

CURRICULUM VITAE

Indice

1 Informazioni personali	1
2 Breve biografia	1
2.1 Titoli di studio	1
2.2 Posizioni	1
3 Contratti e assegni di ricerca	1
4 Attività di didattica, didattica integrativa, e servizio agli studenti	2
4.1 Attività di didattica frontale a livello universitario	2
4.2 Attività di tutoraggio a livello universitario	2
4.3 Attività di didattica nell'ambito di scuole di specializzazione post-laurea	3
4.4 Attività di didattica non universitaria	3
4.5 Relatore/correlatore di tesi di laurea magistrale e triennale	3
5 Attività di ricerca presso qualificati istituti internazionali	5
6 Attività progettuale	5
6.1 Responsabilità di/in progetti di ricerca	5
6.2 Partecipazione a progetti di ricerca	5
7 Partecipazione a gruppi di ricerca nazionali e internazionali	6
8 Presentazioni a conferenze, workshop e seminari	6
9 Premi, riconoscimenti e certificazioni	8
9.1 Premi e riconoscimenti	8
9.2 Certificazioni	8
10 Attività professionale e di servizio	8
10.1 Partecipazione a comitati editoriali di riviste internazionali	8
10.2 Attività editoriali	8
10.3 Organizzazione di conferenze internazionali	9
10.4 Attività di servizio	12
11 Altre attività: terza missione e trasferimento tecnologico	12
11.1 Terza missione	12
11.2 Trasferimento tecnologico	12
12 Pubblicazioni scientifiche	13
12.1 Descrizione dell'attività di ricerca	13
12.2 Pubblicazioni	14
12.2.1 Specchietto riassuntivo delle pubblicazioni	15
12.2.2 Elenco delle pubblicazioni	15

1 Informazioni personali

Cognome: Bena

Nome: Nicola

2 Breve biografia

2.1 Titoli di studio

- Nel *Gennaio 2024* ha conseguito il Dottorato di Ricerca in Informatica (XXXVI Ciclo) presso l'Università degli Studi di Milano con giudizio *Con Lode*.
Tesi discussa: "Non-Functional Certification of Modern Distributed Systems". Relatore: Prof. Claudio A. Ardagna.
- Da *Novembre 2020* a *Ottobre 2023* ha frequentato il Dottorato di Ricerca in Informatica (XXXVI Ciclo) presso l'Università degli Studi di Milano.
- Nell'*Aprile 2020* ha conseguito la Laurea Magistrale in Sicurezza Informatica presso l'Università degli Studi di Milano con la votazione di 110/110 e Lode.
Tesi discussa: "Verifiche di Assurance in Architetture di Nuova Generazione: Uno Schema di Certificazione per Sistemi Basati su DevOps". Relatore: Prof. Claudio A. Ardagna.
- Nell'*Ottobre 2018* ha conseguito la Laurea Triennale in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università degli Studi di Milano con la votazione di 110/110 e Lode.
Tesi discussa: "Studio ed implementazione di una architettura avanzata basata su VPN per Security Assessment". Relatore: Prof. Marco Anisetti.

2.2 Posizioni

- Da *Giugno 2020* lavora come assegnista di ricerca presso il Dipartimento di Informatica, Università degli Studi di Milano.
- Da *Gennaio 2022* è Segretario del Laboratorio Nazionale di Data Science del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).
- Da *Maggio 2022* è cultore della materia in Reti di calcolatori.
- Da *Febbraio 2019* a *Maggio 2019* e da *Ottobre 2019* a *Gennaio 2020* ha ottenuto due incarichi di collaborazione esterna, Dipartimento di Informatica, Università degli Studi di Milano.
- Da *Ottobre 2018* collabora alle attività del laboratorio *SEcure Service-oriented Architectures Research Lab* (SESAR Lab), Dipartimento di Informatica, Università degli Studi di Milano.

3 Contratti e assegni di ricerca

- *Giugno 2023 – Maggio 2025*: assegnista di ricerca presso il Dipartimento di Informatica, Università degli Studi di Milano, nell'ambito del progetto PNRR *Multilayered Urban Sustainability Action (MUSA)*, *Spoke 2 Big Data-Open Data in Life Sciences* (MUSA).
- *Giugno 2020 – Maggio 2023*: assegnista di ricerca presso il Dipartimento di Informatica, Università degli Studi di Milano, nell'ambito del progetto EU Horizon 2020 *Cyber security cOmpeteNce fOr Research and Innovation* (CONCORDIA).
- *Ottobre 2019 – Gennaio 2020*: contratto di collaborazione esterna presso il Dipartimento di Informatica, Università degli Studi di Milano, nell'ambito del progetto EU Horizon 2020 *Cyber security cOmpeteNce fOr Research and Innovation* (CONCORDIA).
- *Febbraio 2019 – Maggio 2019*: contratto di collaborazione esterna presso il Dipartimento di Informatica, Università degli Studi di Milano.

4 Attività di didattica, didattica integrativa, e servizio agli studenti

4.1 Attività di didattica frontale a livello universitario

Ha tenuto i seguenti seminari nell'ambito di corsi di Laurea triennale/magistrale presso università italiane ed estere.

- “Anonimato in Rete: Dai Cookie a Tor”. Lezione nell'ambito dell'insegnamento di *Reti di Calcolatori*, corso di Laurea triennale in Informatica, Università degli Studi di Napoli “Parthenope,” Napoli, Dicembre 2023 (2 ore).
- “Moon Cloud: a Distributed System for Security Assurance”. Lezione nell'ambito dell'insegnamento *Cloud Computing Technologies*, corso di Laurea magistrale in Informatica, Università degli Studi di Milano, Milano, Giugno 2023 (2 ore).
- “Assurance-based Security Governance for ICT systems”. Lezione nell'ambito dell'insegnamento *Cybersecurity Seminars*, corso di Laurea magistrale in Cybersecurity, Sapienza Università di Roma, Roma. Aprile 2023 (con M. Anisetti, 2 ore).

4.2 Attività di tutoraggio a livello universitario

Ha svolto attività come docente tutor per i seguenti insegnamenti della Laurea Triennale in Sicurezza dei Sistemi e delle Reti Informatiche, Dipartimento di Informatica, Università degli Studi di Milano:

- A.A. 2024–25: *Reti di calcolatori (laboratorio)* (48 ore).
- A.A. 2023–24: *Reti di calcolatori (laboratorio)* (12 ore).
- A.A. 2021–22: *Reti di calcolatori (laboratorio)* (18 ore).¹
- A.A. 2020–21: *Reti di calcolatori* (8 ore).
- A.A. 2019–20: *Reti di calcolatori e reti di calcolatori (laboratorio)*. (75 ore).²
- A.A. 2019–20: *Progettazione model-driven del software* (6 CFU, 26 ore).
- A.A. 2019–20: *Progettazione di software sicuro (laboratorio)* (6 CFU, 26 ore).

¹Supporto all'erogazione ibrida dell'insegnamento in periodo pandemico COVID-19.

²Moduli erogati in modalità sincrona online in periodo pandemico COVID-19.

Le attività includono *i)* preparazione di materiale di supporto per gli studenti (esercizi, dispense, materiale di approfondimento); *ii)* lezioni frontali assieme al docente titolare dell'insegnamento; *iii)* partecipazione alle commissioni degli esami di profitto.

Ha svolto/svolge attività di tutor didattico nell'ambito dei seguenti insegnamenti del corso di laurea in Sicurezza dei Sistemi e delle Reti Informatiche (edizione online), Dipartimento di Informatica, Università degli Studi di Milano:

- A.A. 2024–25: *Reti di calcolatori* (12 CFU, 42 ore).
- A.A. 2023–24: *Reti di calcolatori* (12 CFU, 86 ore).
- A.A. 2022–23: *Reti di calcolatori* (12 CFU, 86 ore).
- A.A. 2021–22: *Reti di calcolatori* (12 CFU, 86 ore).
- A.A. 2020–21: *Reti di calcolatori* (12 CFU, 86 ore).
- A.A. 2019–20: *Reti di calcolatori* (12 CFU, 86 ore).

Le attività svolte includono *i)* lezioni di recupero con singoli studenti su argomenti specifici in modalità sincrona; *ii)* correzione di esercitazioni e esercizi di auto-valutazione degli studenti; *iii)* risposta a quesiti degli studenti in maniera asincrona; *iv)* partecipazione alle commissioni degli esami di profitto.

4.3 Attività di didattica nell'ambito di scuole di specializzazione post-laurea

Ha tenuto i seguenti insegnamenti all'interno dei corsi di perfezionamento dell'Università degli Studi di Milano:

- *Novembre 2024*: "Attacchi ai dati: la nuova frontiera del cybercrime nell'era dei big data e dell'intelligenza artificiale" Corso di Perfezionamento in Criminalità Informatica e Investigazioni Digitali – Il fattore umano (2 ore, con C. A. Ardagna)
- *Novembre 2023*: "AI: poisoning attacks and countermeasure," Corso di Perfezionamento in Criminalità Informatica e Investigazioni Digitali – Intelligenza Artificiale, attacchi, crimini informatici, investigazioni e aspetti etico-sociali (2 ore, con C. A. Ardagna).
- *Giugno 2022*: "Il metaverso da un punto di vista tecnico e informatico," Corso di perfezionamento in Big Data, Artificial Intelligence e Piattaforme – Aspetti tecnici e giuridici connessi all'utilizzo dei dati e alla loro tutela (2 ore, con C. A. Ardagna).
- *Dicembre 2021*: "L'idea di anonimato e il presentarsi in rete anonimi," Corso di Perfezionamento Online in Criminalità Informatica e Investigazioni Digitali – Le procedure di investigazione e di rimozione dei contenuti digitali. Pornografia, proprietà intellettuale, odio e terrorismo, oblio, tutela della reputazione (2 ore, con C.A. Ardagna).
- *Ottobre 2020*: "I filtri e l'utilizzo di strumenti quali VPN e Tor," Corso di Perfezionamento Online in Criminalità Informatica e Investigazioni Digitali – La digital forensics sulle infedeltà del partner, del dipendente, del professionista e sulle frodi nelle piattaforme digitali (2 ore, con C.A. Ardagna).

4.4 Attività di didattica non universitaria

Ha tenuto i seguenti corsi online.

- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Novembre 2022 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Maggio 2022 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Novembre 2021 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Giugno 2021 (con M. Anisetti, A. Polimeno).

4.5 Relatore/correlatore di tesi di laurea magistrale e triennale

Segue in qualità di correlatore, le seguenti tesi triennali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- Riccardo Aldizio. "Design e Implementazione di Valutazioni di Assurance per Modelli Basati su Machine Learning".
- Melissa Moioli. "Una metodologia per la valutazione di affidabilità di flotte di droni".
- Raphael Vauterin. "Interfaccia grafica per la configurazione ed il deployment di pipeline MUSA nel continuum".

Ha seguito, in qualità di correlatore, le seguenti tesi triennali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- Riccardo Barone. "Design e implementazione di pipeline per l'analisi dei dati di assurance di sicurezza".
- Marco A. Bonissi. "Studio e realizzazione di uno strumento per il rilevamento di exfiltration di dati".
- Ruslan Bondaruc. "Studio e realizzazione di un IDS di nuova generazione basato su un'architettura edge".
- Carlo Civardi. "Implementazione di un ambiente IoT per la simulazione di attività di assurance".
- Federico Colombo. "Design e Sperimentazione di uno Schema di Certificazione per Sistemi Basati su IoT".
- Matteo dal Grande. "Studio e implementazione di una pipeline di DevSecOps".

- Alex Della Bruna. "Design e Sviluppo di un Sistema Distribuito Avanzato per Verifiche di Security Assurance".
- Ez Eddine Ed Daouy. "Studio ed implementazione di sonde per la collezione di log".
- Nicolas Ferazzini. "Valutazione di Robustezza di Modelli di Machine Learning rispetto ad Attacchi di Poisoning".
- Salvatore Ferrara. "Assurance di integrità per modelli ML".
- Nicolò Grecchi. "Revisting Trust Management in Open Distributed Systems".
- Yannick Joly. "Studio e implementazione di un sistema di security assurance basato su monitoraggio: Un caso di studio Campus Scolastico".
- Giovanni Locatelli. "Studio e realizzazione di una soluzione di hardening per Windows".
- Nicola Lopatriello. "Un tool per la gestione del ciclo di vita di controlli di security assurance".
- Stefano Maddé. "Studio e sviluppo di una sonda di rete per rilevazione di allegati e-mail infetti".
- Jacopo Magagnin. "Analisi del Modello Publish/Subscribe: Architettura, Applicazioni e Sicurezza".
- Michele Mastroberti. "I firewall e le minacce criptate".
- Luca Mori. "Design and implementation of a risk management solution for machine learning models".
- Paolo Premoli. "Payment Card Industry Data Security Standard".
- Khanluka Rama. "Design e sviluppo di uno strumento per la generazione automatica di report di sicurezza".
- Davide Righetti. "Tecniche di Explainable AI".
- Luca Ruggeri. "Studio ed implementazione di un sistema per l'automazione di attività di penetration testing".
- Jacopo Saiani. "Verifiche di explainability su modelli di ML".
- Victoria Sheng. "Design, progettazione e sviluppo di una dashboard per l'analisi e la visualizzazione dei risultati di un processo di security assurance".
- Daniel Simonini. "Studio ed implementazione di un sistema di autenticazione con JWT".
- Marica Soci. "Design e sviluppo di probe di assurance di sicurezza per ambienti basati su Windows".
- Salvatore Sorvillo. "Data poisoning in federated learning".
- Christian Vaccarino. "Studio ed implementazione di sonde per la verifica di sicurezza di sistemi Windows".

Segue, come correlatore, le seguenti tesi magistrali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- Michele Mastroberti. "Valutazioni di assurance di modelli di machine learning".
- Paolo G. Panero. "Managing ML-Based Application Non-Functional Behavior: A Multi-Model Approach".

Ha seguito, come correlatore, le seguenti tesi magistrali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- 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. "Studio di soluzioni di sicurezza in ambito IoT basate su Machine Learning".
 - Alex Fortunato. "Studio ed Implementazione di un Sistema per l'Assurance di Firewall e Dispositivi di Sicurezza Perimetrale".
 - Marco Luzzara. "Migration of a Spend Analysis Product From an On-Premises Environment to the AWS Cloud".
 - Emanuele Meroni. "Design ed implementazione di una metodologia di certificazione composta".
 - Marco Pedrinazzi. "A Transparent Certification Scheme Based on Blockchain".
- Tesi candidata del Dipartimento di Informatica, Università degli Studi di Milano al *premio Tesi di Laurea Magistrale "con.Scienze 2024"*.**

Segue/ha seguito e supporta/ha supportato le attività dei seguenti dottorandi (visiting student) presso il Dipartimento di Informatica dell'Università degli Studi di Milano nell'ambito di diverse tematiche inerenti all'assurance, alla certificazione, alla cloud, e all'intelligenza artificiale.

- Kathrin Brecker (Karlsruhe Institute of Technology). L'attività di ricerca è rivolta alla definizione di schemi di certificazione di nuova generazione per applicazioni basate su AI.

Ha seguito, in qualità di co-supervisore, i seguenti laureandi (visiting student) presso l'Università degli Studi di Milano nell'ambito di diverse tematiche inerenti alla sicurezza, alla cloud, ai microservizi.

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

5 Attività di ricerca presso qualificati istituti internazionali

- *Febbraio – Aprile 2025*: visiterà la Khalifa University, Abu Dhabi, UAE (come *visiting scholar*). L'attività di ricerca, in collaborazione con il Prof. Chan Yeob Yeun, sarà rivolta alla valutazione di robustezza di modelli di machine learning rispetto ad attacchi di poisoning. Viene allegata la lettera di invito del Prof. Chan Yeob Yeun in **Appendice A** del presente curriculum vitae.
- *Giugno – Agosto 2023*: ha visitato il LIRIS Lab, INSA Lyon, Lione, Francia (come *visiting scholar*). L'attività di ricerca, in collaborazione con la Prof.ssa Chirine Ghedira-Guegan, Prof.ssa Nadia Bennani, Dr.ssa Genoveva Vargas-Solar, è stata rivolta alla definizione di nuove metodologie per il trust management in sistemi distribuiti moderni.
- *Febbraio – Aprile 2023*: ha visitato la Khalifa University, Abu Dhabi, UAE (come *visiting scholar*). L'attività di ricerca, in collaborazione con il Prof. Chan Yeob Yeun, è stata rivolta alla definizione di nuove metodologie per migliorare la robustezza dei modelli di machine learning ad attacchi di data poisoning.

6 Attività progettuale

6.1 Responsabilità di/in progetti di ricerca

Work Package leader nei seguenti progetti di ricerca:

- Progetti di ricerca finanziati da Technology Innovation Institute (TII)
Titolo progetto: Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models (PALM)
Periodo: Novembre 2020 – Aprile 2023
Unità operativa: Università degli Studi di Milano (UNIMI)
Finanziamento: 350 000 USD
Ruolo: Work Package Leader WP4 "Assurance methodology"
Attività: Definizione di una metodologia e un prototipo per migliorare la robustezza dei modelli di machine learning ad attacchi di data poisoning. Le attività svolte sono risultate nella pubblicazione degli articoli scientifici [RI-5, RI-7] in Sezione 12.2.2.

6.2 Partecipazione a progetti di ricerca

Ha partecipato/partecipa ai seguenti progetti di ricerca:

- Piano Nazionale di Ripresa e Resilienza (PNRR)
Titolo progetto: MUSA: Multilayered Urban Sustainability Action (MUSA), Spoke 2 Big Data-Open Data in Life Sciences
Periodo: Settembre 2022 – Agosto 2025
Unità operativa: Università degli Studi di Milano (UNIMI)
Attività: Design e sviluppo di un'architettura digitale cloud-edge abilitata dal 5G per lo storage e lo scambio sicuro di big data per scienze della vita e a supporto di studi clinici. Le attività svolte sono risultate nella pubblicazione degli articoli scientifici [RI-1, RI-2, RI-3, RI-4, CI-1, CI-3, CI-4, CI-5, CI-6] in Sezione 12.2.2.

- Grandi Sfide di Ricerca (GSA) – Linea 6 – Strategic Line 4: Sicurezza informatica/Cloud
Periodo: 2022 – 2024
Titolo progetto: Sovereign Edge-Hub: Un’Architettura Cloud-Edge per la Sovranità Digitale nelle Scienze della Vita (SOV-EDGE-HUB)
Attività: Raccolta e analisi dei requisiti, design e sviluppo dell’infrastruttura cloud-edge di ateneo con particolare riferimento ad aspetti non-funzionali. Le attività svolte sono risultate nella pubblicazione degli articoli scientifici [RI-1, RI-2, CI-4] in Sezione 12.2.2.
- Programma EU Horizon 2020 (SU-ICT - Boosting the effectiveness of the Security Union)
Titolo progetto: Cyber security cOmpeteNce fOr Research andN Innovation (CONCORDIA)
Periodo: Gennaio 2019 – Dicembre 2023
Unità operativa: Università degli Studi di Milano (UNIMI)
Attività: Definizione di una serie di threat report che presentano *i)* l’evoluzione delle minacce e vulnerabilità di sicurezza IT, *ii)* i gap e challenge nel dominio della sicurezza IT, e *iii)* le contromisure di sicurezza disponibili. Le attività svolte sono risultate nella pubblicazione degli articoli scientifici [RI-6, RI-8, CI-7, CI-9, CI-10, CI-11, CI-12, CI-13] e degli articoli divulgativi [AP-1, AP-2] in Sezione 12.2.2.

Nell’ambito della sua ricerca ha contribuito/contribuisce alle attività di ricerca dei seguenti progetti:

- Progetti di ricerca finanziati da Laboratoire d’InfoRmatique en Image et Systèmes d’information (Transversal Actions Program of the LIRIS Lab)
Titolo progetto: A fairness approach to deal with data and models in federated learning verifying an intersectional, diverse, and inclusive analytics (FRIENDLY)
Periodo: Gennaio 2024 – Dicembre 2025
Attività: Definizione di una metodologia di trust management basata su certificazione per sistemi distribuiti moderni. Le attività svolte sono risultate nella pubblicazione degli articoli scientifici [CI-2, RI-3] in Sezione 12.2.2.
- Program EU Horizon 2020
Titolo progetto: Intelligent Management of Processes, Ethics and Technology for Urban Safety (IMPETUS)
Periodo: Settembre 2020 – Agosto 2022
Attività: Raccolta e analisi dei requisiti, e design di una piattaforma per la definizione ed esecuzione di pipeline di analisi dati che migliorino la sicurezza e la safety di una smart city.

7 Partecipazione a gruppi di ricerca nazionali e internazionali

Partecipa alle attività dei seguenti gruppi di ricerca:

- *Critical Information Infrastructures*, Karlsruhe Institute of Technology, Karlsruhe, Germania.
- *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, Lione, Francia.
- *Center for Cyber-Physical Systems (C2PS)*, Khalifa University, Abu Dhabi, UAE.
- *SEcure Service-oriented Architectures Research Lab (SESAR)*, Università degli Studi di Milano, Milano, Italia.

Partecipa come afferente alle attività dei seguenti consorzi:

- Laboratorio Nazionale di Data Science del Consorzio Interuniversitario Nazionale per l’Informatica (CINI)
- Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l’Informatica (CINI)

8 Presentazioni a conferenze, workshop e seminari

Ha partecipato ai seguenti panel presso conferenze e workshop internazionali:

- “Navigating Time and Space: Diverse Perspective on Building Scientific Careers”, presso la conferenza ACS/IEEE 21st International Conference on Computer Systems and Applications (ACS/IEEE AICCSA 2024), Sousse, Tunisia, Ottobre 2024.

Ha presentato, come relatore, i seguenti lavori a conferenze e workshop internazionali:

- 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, Cina, Luglio 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, Grecia, Maggio 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, Italia, Maggio 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)*, Milano, Novembre 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, Agosto 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)*, parte di *2022 IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring)*, Helsinki, Finlandia, Giugno 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, Cina, Dicembre 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, Settembre 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)*, Parigi, Francia, Luglio 2020 (**vincitore del premio “Best Student Paper Award”**).

Ha tenuto i seguenti seminari invitati presso centri di ricerca/università internazionali:

- “Assurance in Modern ICT Systems: From Theory to Practice”. Shandong University of Technology, Cina, Agosto 2023 (con M. Anisetti).
- “Distributed Systems Certification: From Services to Machine Learning”. INSA Lyon, Lione, Francia, Giugno 2023.
- “Distributed Systems Certification: From Services to Machine Learning”. Khalifa University, Abu Dhabi, UAE, Marzo 2023.

Ha tenuto i seguenti seminari/presentazioni all’interno di progetti di ricerca ed eventi nazionali:

- “Trustworthy Machine Learning-Based Applications: A Certification-Based Approach”. Poster session presso Terzo General Meeting MUSA, Università Bocconi, Milano, Italia, Maggio 2024.
- “A digital platform for data analytics pipeline management in the cloud-edge continuum”. Secondo General Meeting MUSA, Politecnico di Milano, Milano, Italia, Novembre 2023.
- “Security and Privacy of the Data Lake Architecture”. PhD Day Hub, Università degli Studi di Milano, Milano, Ottobre 2022.
- “Bridging the Gap Between Certification and Software Development”. CONCORDIA WP1 Meeting, Universität der Bundeswehr, Monaco, Germania, Giugno 2022.
- “An Assurance-Based Risk Management Framework for Distributed Systems”. CONCORDIA T1.1 Meeting, Virtuale, Luglio 2021.
- “Moon Cloud: una Piattaforma per la Cybersecurity”. Giornata aperta, Dipartimento di Informatica, Università degli Studi di Milano, Milano, Febbraio 2020 (con M. Anisetti, A. Polimeno).
- “Moon Cloud: Governance di Sicurezza e Verifica di Conformità”. Giornata aperta, Dipartimento di Informatica, Università degli Studi di Milano, Milano, Febbraio 2019 (con P. Ceravolo).

9 Premi, riconoscimenti e certificazioni

9.1 Premi e riconoscimenti

- **Vincitore del premio “Best Student Paper Award”** presso la conferenza internazionale “17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)”.
Titolo dell’articolo: “Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems”.
Coautori: M. Anisetti, C.A. Ardagna, E. Damiani.
- *Member IEEE*

9.2 Certificazioni

- A *Giugno 2015* ha conseguito la certificazione “EUCIP IT Administrator – modulo Sicurezza Informatica”, rilasciata da Associazione Italiana per l’Informatica e il Calcolo Automatico (AICA).

10 Attività professionale e di servizio

10.1 Partecipazione a comitati editoriali di riviste internazionali

Review editor delle seguenti riviste internazionali:

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

Co-editore (guest editor) delle seguenti special issue su riviste internazionali:

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

10.2 Attività editoriali

Ha svolto, in qualità di *reviewer*, revisioni di lavori sottomessi alle seguenti riviste internazionali:

- *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.*

Ha svolto attività di revisione per *Qeios* e per proposte di monografie sottomesse a John Wiley and Sons publisher.

10.3 Organizzazione di conferenze internazionali

Program Chair per le seguenti conferenze e workshop:

- *4th Italian Conference on Big Data and Data Science (ITADATA 2025)*, Torino, Italia, Settembre 2025.
- *3rd Italian Conference on Big Data and Data Science (ITADATA 2024)*, Pisa, Italia, Settembre 2024 (co-chair con M. Natilli, G. Stilo, C. Diamantini, L. Romano).
- *ICWS Workshop on Services Regulation & Governance (SRG 2024)*, workshop parte di *IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, Cina, Luglio 2024 (co-chair con L. Kuang, Y. Watanabe, T. Zhao).
- *2nd Italian Conference on Big Data and Data Science (ITADATA 2023)*, Napoli, Italia, Settembre 2023 (co-chair con B. Di Martino, A. Maratea, A. Sperduti).

Special Session Chair per le seguenti conferenze e workshop:

- *Data Science: Multidisciplinary Perspectives to Tame the Data Revolution*. Special session presso *The International Joint Conference on Neural Networks (IJCNN 2025)*, Roma, Italia, Giugno – Luglio 2025 (co-chair con E. Di Nardo, A. Ciaramella, C. A. Ardagna).

Membro del Comitato Organizzatore delle seguenti conferenze e workshop:

- *2nd International Conference on Machine Intelligence and Digital Applications (MIDA 2025)*, Ningbo, Cina, Aprile 2025

Membro del Comitato di Programma delle seguenti conferenze e workshop:

- *IEEE 6th International Conference on Computer Science and Communication Technology (IEEE ICCSCT 2025)*, Wuhan, Cina, Agosto 2025.
- *2025 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2025)*, Chania, Grecia, Agosto 2025.
- *2nd International Conference on Communication, Information and Digital Technologies (CIDT 2025)*, Singapore, Giugno 2025.
- *15th International Conference on Cloud Computing and Services Science (CLOSER 2025)*, Porto, Portogallo, Aprile 2025.
- *The 40th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2025)*, Catania, Marzo–Aprile 2025.
- *2025 7th International Symposium on Computational and Business Intelligence (ISCBI 2025)*, Macao, Cina, Febbraio 2025.
- *2025 7th International Conference on Software Engineering and Computer Science (CSECS 2025)*, Taicang, Cina, Gennaio 2025.
- *22nd IEEE International Conference on Embedded and Ubiquitous Computing (IEEE EUC 2024)*, Sanya, Cina, Dicembre 2024
- *27th IEEE International Conference on Computational Science and Engineering 2024 (IEEE CSE 2024)*, Sanya, Cina, Dicembre 2024
- *23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2024)*, Sanya, Cina, Dicembre 2024
- *2024 IEEE International Conference on High Performance Computing and Communications (IEEE HPCC 2024)*, Wuhan, Cina, Dicembre 2024.
- *21st IEEE International Conference on Ubiquitous Intelligence and Computing (IEEE UIC 2024)*, Denarau Island, Figi, Dicembre 2024.
- *25th International Web Information Systems Engineering conference (WISE 2024)*, Doha, Qatar, Dicembre 2024.
- *7th International Conference on Machine Learning for Networking (MLN'2024)*, Reims, Francia, Novembre 2024.
- *2024 6th International Conference on Advanced Information Science and System (AISS 2024)*, Sanya, Cina, Novembre 2024.

- *12th Workshop on New Frontiers in Mining Complex Patterns (NFMCP 2024)*, workshop parte di ECML-PKDD 2024, Vilnius, Lituania, Settembre 2024.
- *2024 IEEE CSR Workshop on Synthetic Data Generation for a Cyber-Physical World (SDG 2024)*, workshop parte di IEEE CSR 2024, Londra, Regno Unito, Settembre 2024.
- *2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2024)*, Londra, Regno Unito, Settembre 2024.
- *6th International Conference on Science of Cyber Security (SciSec 2024)*, Copenhagen, Danimarca, Agosto 2024.
- *8th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2024) During SMART-COMP 2024, (IEEE BITS 2024)*, workshop parte di IEEE SMARTCOMP 2024, Osaka, Giappone, Giugno – Luglio 2024.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2024)*, Luglio 2024, Shenzhen, Cina.
- *A Human-Centric Perspective of Explainability, Interpretability and Resilience in Computer Vision*, special session presso *IEEE International Joint Conference on Neural Networks (IEEE IJCNN 2024)*, Giugno – Luglio 2024, Yokohama, Giappone.
- *2024 5th International Conference on Computing, Networks and Internet of Things (CNIOT 2024)*, Maggio 2024, Tokyo, Giappone.
- *2024 International Conference on Communication, Information and Digital Technologies (ICCIDT 2024)*, Maggio 2024, Wuhan, Cina.
- *14th International Conference on Cloud Computing and Services Science (CLOSER 2024)*, Maggio 2024, Angers, Francia.
- *Fifteenth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2024)*, Aprile 2024, Venezia, Italia.
- *21th IEEE International Symposium on Parallel and Distributed Processing with Applications (IEEE ISPA 2023)*, Dicembre 2023, Wuhan, Cina.
- *14th IEEE International Conference On Cloud Computing Technology And Science (CloudCom 2023)*, Dicembre 2023, Napoli, Italia.
- *22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023)*, Exeter, Regno Unito, Novembre 2023.
- *2023 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2023)*, Venezia, Italia, Luglio – Agosto 2023.
- *IEEE Cloud Summit 2023*, Baltimora, MD, USA, Luglio 2023.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2023)*, Chicago, IL, USA, Luglio 2023.
- *7th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2023) During SMART-COMP 2023, (IEEE BITS 2023)*, workshop parte di IEEE SMARTCOMP 2023, Nashville, TN, USA, Giugno 2023.
- *International Workshop on AI-driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP 2023)*, workshop parte di IEEE INFOCOM 2023, New York, USA. Maggio 2023.
- *4th International Conference on Computing, Networks and Internet of Things (CNIOT 2023)*, Xiamen, Cina, Maggio 2023.
- *13th International Conference on Cloud Computing and Services Science (CLOSER 2023)*, Praga, Repubblica Ceca, Aprile 2023.
- *IEEE Global Communications Conference (IEEE GLOBECOM 2022)*, Rio de Janeiro, Brasile, Dicembre 2022.
- *5th International Conference on Machine Learning for Networking (MLN'2022)*, Parigi, Francia, Novembre 2022.
- *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUST-COM 2022)*, Wuhan, Cina, Ottobre 2022.
- *2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022)*, Virtuale, Luglio 2022.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2022)*, Barcellona, Spagna, Luglio 2022.

- *6th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2022) During SMART-COMP 2022, (IEEE BITS 2022)*, workshop parte di IEEE SMARTCOMP 2022, Espoo, Finlandia, Giugno 2022.
- *3rd International Conference on Computing, Networks and Internet of Things (CNIOT 2022)*, Qingdao, Cina, Maggio 2022.
- *12th International Conference on Cloud Computing and Services Science (CLOSER 2022)*, Virtuale, Aprile 2022.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2021)*, Chicago, IL, USA, Settembre 2021.
- *5th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2021) During SMART-COMP 2021, (IEEE BITS 2021)*, workshop parte di IEEE SMARTCOMP 2021, Irvine, CA, USA, Agosto 2021.
- *2nd International Conference on Computing, Networks and Internet of Things (CNIOT 2021)*, Pechino, Cina, Maggio 2021.
- *3rd International Conference on Machine Learning for Networking (MLN'2020)*, Parigi, Francia, Novembre 2020.

Ha svolto, in qualità di *sub-reviewer*, revisioni di lavori sottomessi alle seguenti conferenze internazionali:

- *The 7th International Conference on Attacks and Defenses for Internet-of-Things (ADIoT 2024)*, Hangzhou, Cina, Dicembre 2024.
- *20th International Conference on Information Systems Security (ICISS 2024)*, Jaipur, India, Dicembre 2024.
- *International Conference on Security for Information Technology and Communications (SecITC 2024)*, Bucharest, Romania, Novembre 2024.
- *39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024)*, Edimburgo, Regno Unito, Giugno 2024.
- *18th International Conference on Information Systems Security (ICISS 2022)*, Tirupati, India, Dicembre 2022.
- *37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2022)*, Copenhagen, Danimarca, Giugno 2022.
- *37th ACM/SIGAPP Symposium on Applied Computing (ACM SAC 2022)*, Brno, Repubblica Ceca, Aprile 2022.
- *14th IEEE/ACM International Conference on Utility and Cloud Computing (IEEE/ACM UCC 2021)*, Leicester, Regno Unito, Dicembre 2021.
- *6th International Conference on Systems, Control and Communications (ICSCC 2021)*, Chongqing, Cina, Ottobre 2021.
- *36th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2021)*, Oslo, Norvegia, Giugno 2021.
- *19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)*, Guangzhou, Cina, Dicembre 2020 – Gennaio 2021.
- *International Conference on Security and Privacy in Digital Economy (SPDE 2020)*, Quzhou, Cina, Ottobre – Novembre 2020.
- *2020 IEEE International Conference on Cloud Computing (IEEE CLOUD 2020)*, Pechino, Cina, Ottobre 2020.
- *11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019)*, Sidney, Australia, Dicembre 2019.

È stato *publication chair* delle seguenti conferenze:

- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milano, Italia, Settembre 2022.

È stato *publicity chair* delle seguenti conferenze:

- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2024)*, Shenzhen, Cina, Luglio 2024.
- *IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, Cina, Luglio 2024.
- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milano, Italia, Settembre 2022.
- *Big Data and Data Science for Next-Generation Distributed Systems (BDDS 2022)*, workshop parte di *IEEE World Congress on Computational Intelligence (IEEE WCCI 2022)*, Padova, Italia, Luglio 2022.
- *IEEE World Congress on Services (IEEE SERVICES 2022)*, Barcellona, Spagna, Luglio 2022.

- *IEEE World Congress on Services (IEEE SERVICES 2021)*, Chicago, IL, USA, Settembre 2021.

È stato *session chair* delle seguenti conferenze:

- *3rd Italian Conference on Big Data and Data Science (ITADATA 2024)*, Pisa, Italia, Settembre 2024.
- *IEEE International Conference on Web Services (IEEE ICWS 2022)*, Barcellona, Spagna, Luglio 2022.

10.4 Attività di servizio

- Da *Settembre 2023* è responsabile dell'organizzazione della serie di seminari "Tales on Data Science and Big Data Science" erogata dal Laboratorio Nazionale di Data Science del CINI (co-responsabile con G. Ruffo).
- Da *Gennaio 2022* è *Segretario* del Laboratorio Nazionale di Data Science del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

11 Altre attività: terza missione e trasferimento tecnologico

11.1 Terza missione

Ha svolto le seguenti attività per la terza missione:

- Lezione pratica "AI: Attacchi e Difese," e presentazione dei corsi di laurea erogati dal Dipartimento di Informatica, Università degli Studi di Milano, presso ITIS E. Majorana, Seriate (BG), Italia, 21 Marzo 2024.
- "Multi-Dimensional Certification of Artificial Intelligence". Parte di *Building Bridges through Multidisciplinary Cooperation: Perspective Approaches for Inclusive Artificial Intelligence*, Milano, Maggio 2023.
- "Moon Cloud: Governance di Sicurezza e Verifica di Conformità". Milano Digital Week, Milano, Marzo 2019.

11.2 Trasferimento tecnologico

Ha contribuito/contribuisce alle seguenti attività di trasferimento tecnologico:

- Da *Novembre 2018* collabora con Moon Cloud srl, startup innovativa e spin-off dell'Università degli Studi di Milano per la valutazione e il monitoraggio della sicurezza dei sistemi IT.

12 Pubblicazioni scientifiche

12.1 Descrizione dell'attività di ricerca

L'attività di ricerca si è concentrata principalmente sui temi della sicurezza dei sistemi distribuiti moderni, con particolare riferimento alla valutazione di assurance e alla definizione di tecniche di certificazione per applicazioni *i)* erogate in ambienti cloud-edge e architetture a servizi, e *ii)* basate su modelli di Machine Learning (ML). L'attività di ricerca ha inoltre contribuito alla definizione e sviluppo di nuove tecniche di trust management per sistemi distribuiti. Di seguito viene riportata una classificazione degli argomenti interessati dalla ricerca descrivendo brevemente i problemi affrontati e i principali risultati ottenuti. Le entrate bibliografiche si riferiscono alla lista di pubblicazioni riportata in Sezione 12.2.2 e sono classificate secondo la seguente convenzione: RI (Riviste Internazionali), CI (Conferenze e Workshop Internazionali), IS (In Sottomissione).

Assurance e certificazione di applicazioni in sistemi distribuiti moderni. I sistemi distribuiti moderni sono caratterizzati da una struttura a elevata complessità con interdipendenze tra i diversi servizi. Il ciclo di vita dei servizi è altamente automatizzato e caratterizzato da rilasci e deployment frequenti; le applicazioni sono create dinamicamente componendo e sostituendo continuamente tali servizi in accordo a requisiti funzionali. In questo scenario, diventa fondamentale poter garantire che tali applicazioni supportino anche un insieme di requisiti non-funzionali. L'attività di ricerca, svolta all'interno dei progetti di ricerca *CONCORDIA*, *SOV-EDGE-HUB*, e *MUSA*, si è concentrata su *i)* la definizione di nuovi schemi di certificazione [CI-4, CI-5, RI-8]; *ii)* la definizione di metodologie per facilitare l'adozione della certificazione riducendone i costi [CI-7] e rimuovendo assunzioni che rendono gli schemi di certificazione esistenti inapplicabili [CI-3]; e *iii)* l'utilizzo della certificazione in casi di studio reali [RI-6, CI-8, CI-9, CI-10, CI-11, CI-12, CI-13].

Per quanto riguarda il punto *i)*, in [CI-5] sono state analizzate le principali deficienze delle tecniche di certificazione esistenti in relazione ai sistemi distribuiti moderni. Successivamente, è stato definito un manifesto che mira a guidare la ricerca sulla certificazione nei prossimi anni, individuando le macro-aree di ricerca da sviluppare e la loro collocazione temporale nel breve, medio, e lungo termine, unitamente a linee di ricerca affini che possono contribuire alla ricerca nelle macro-aree individuate. In [RI-8] è stato definito un nuovo schema di certificazione che espande lo scopo della verifica non-funzionale rispetto agli schemi di certificazione tradizionali. I certificati rilasciati sono *multi-dimensionali* e valutano diversi aspetti (*dimensioni*) che impattano le proprietà non-funzionali del servizio/applicazione sotto esame. Tali dimensioni includono, ad esempio, gli artefatti software e il processo di sviluppo usato per l'implementazione del servizio/applicazione. I certificati multi-dimensionali consentono di fornire un'immagine più accurata del servizio/applicazione sotto esame e contribuiscono alla gestione del relativo ciclo di vita. Tale lavoro è stato ulteriormente esteso in [CI-4], affrontando il problema della certificazione *continua*. Lo schema in [CI-4], infatti, definisce un nuovo ciclo di vita del certificato in grado di seguire e adattarsi in maniera semi-automatica all'evoluzione del servizio/applicazione sotto esame. Tale ciclo di vita riduce l'impatto dell'evoluzione del servizio/applicazione sulla validità del certificato stesso, minimizzando i costi di mantenimento della certificazione. Per fare ciò, la soluzione proposta si avvale di algoritmi di machine learning (ML).

Per quanto riguarda il punto *ii)*, in [CI-7] è stata definita una metodologia basata su algoritmi genetici multi-obiettivo per facilitare l'integrazione della certificazione all'interno del ciclo di sviluppo software. Infatti, la certificazione è tradizionalmente un'attività eseguita al termine del processo di sviluppo, introducendo alti costi e inefficienze. La metodologia proposta si basa sulla definizione delle proprietà da certificare a tempo di sviluppo; tali proprietà guideranno l'implementazione del software rendendolo certificabile *by design*. In [CI-3] sono state rimosse numerose assunzioni irrealistiche riguardo l'uso della certificazione, legate alla necessità di fidarsi ciecamente dei numerosi attori coinvolti. La letteratura ha da tempo riconosciuto la problematicità di tali assunzioni, senza però fornire alcuna soluzione tecnica valida. La soluzione proposta consiste nell'adozione di una blockchain che supporti la rimozione dell'assunzione di *blind trust*. A questo proposito, gli attori e le loro azioni sono mappati in costrutti per la blockchain e nuovi costrutti sono definiti per incrementare la trasparenza del processo di certificazione.

Per quanto riguarda il punto *iii)*, in [CI-11] è stato definito un processo di gestione del rischio integrato con attività di assurance e certificazione. L'integrazione dell'assurance consente di ottenere risultati più accurati, fornendo una *risk posture* maggiormente aderente alla realtà. Proseguendo con quanto definito in [CI-7], in [CI-8] è stata proposta l'integrazione di controlli di assurance all'interno di una pipeline DevSecOps di analitiche Big Data, introducendo verifiche di assurance in ogni fase della pipeline. In [RI-6] è stata definita una metodologia per guidare il *deployment* di pipeline Big Data sulla base di requisiti non-funzionali. I requisiti sono confrontati con le proprietà dei servizi da reclutare nella pipeline, e un processo di monitoraggio valuta continuamente che

tali requisiti siano supportati dai servizi scelti. In caso negativo, nuovi servizi sono ri-negoziati con i provider per garantire che la pipeline soddisfi i requisiti posti. In [CI-9, CI-10] sono stati definiti i requisiti ed è stato implementato un *framework di assurance* che supporta lo schema di certificazione al punto i) focalizzandosi sulle peculiarità del paradigma (IoT)-edge-cloud, caratterizzato da alta volatilità dei componenti. Lo stesso problema è stato affrontato in [CI-12, CI-13], focalizzandosi sulla necessità di automazione e sulle peculiarità di sistemi ibridi, in cui la componente privata dei sistemi riveste comunque importanza e richiede di essere valutata limitandone però l'impatto sui sistemi stessi.

Assurance e certificazione di applicazioni basate su ML. La crescente diffusione di applicazioni basate su ML e il loro crescente utilizzo in contesti critici introduce il bisogno sempre più pressante di tecniche di assurance e certificazione in grado di verificarne proprietà non-funzionali. L'attività di ricerca, svolta all'interno del progetto di ricerca *MUSA* e nel contesto della collaborazione con la Khalifa University (progetto di ricerca *PALM*), si è concentrata sulla definizione e applicazione pratica di schemi di certificazione per applicazioni basate su ML.

Per prima cosa, in [RI-4], sono state analizzate le peculiarità delle applicazioni basate su ML e come esse impattano sulle tecniche di certificazione esistenti, identificando quindi le principali sfide di ricerca in tal senso. Successivamente, è stato proposto un primo adattamento dello schema di certificazione multi-dimensionale in [RI-8]. Lo schema si focalizza su tre dimensioni rilevanti per ML: dataset, processo di training, e modello ML.

Successivamente, l'attività di ricerca si è concentrata sulla verifica della proprietà di *robustezza* rispetto ad attacchi a *training time* (*poisoning*) [RI-5, IS-2, IS-3] e a *inference time* [CI-6, RI-2]. Per quanto riguarda la robustezza a training time, in [RI-5] è stata definita una tecnica per migliorare la robustezza dei modelli di ML ad attacchi di data poisoning. La tecnica consiste nel sostituire il modello di ML base con un *ensemble* di modelli, ciascuno dei quali allenato su una porzione disgiunta del dataset di allenamento. La tecnica proposta è stata validata su modelli *random forest* mostrandone l'efficacia rispetto ad attacchi di *poisoning random*.

Per quanto riguarda la robustezza a inference time, in [CI-6] è stato presentato un nuovo approccio per malware detection basato su ML. Il malware detector propone un approccio innovativo a bassa invasività, collezionando dati dal sistema da analizzare senza richiedere alcun privilegio di accesso. Il malware detector è stato successivamente certificato in [RI-2], insieme a due approcci esistenti in letteratura, per le proprietà di accuracy, privacy e robustezza. A questo scopo è stato utilizzato lo schema di certificazione definito in [RI-4]. La proprietà di robustezza è stata infine studiata in contesti specifici, come l'elaborazione di segnali di elettroencefalografie [RI-7].

Infine, in [RI-1], è stata proposta una nuova metodologia per la gestione a run time di applicazioni basate su ML. La metodologia si basa su un *dynamic Multi-Armed Bandit* (MAB), il quale valuta il comportamento dell'applicazione basata su ML rispetto a una proprietà non-funzionale di interesse. Un peggioramento in tale comportamento scatena un processo di sostituzione del modello di ML, garantendo che il comportamento dell'applicazione rimanga complessivamente stabile.

Trust management. Il trust management, ovvero il processo mediante il quale due parti (tipicamente un utente e un servizio) stabiliscono una relazione di fiducia prima di effettuare una transazione, è stato un ambito di ricerca ampiamente investigato a partire dall'inizio degli anni 2000, per poi perdere relativamente importanza. Tuttavia, l'avvento di applicazioni spesso distribuite tra più provider e, più in generale, che coinvolgono diverse parti con interessi conflittuali, sta richiedendo con sempre maggior insistenza un ripensamento delle tecniche di trust management. In [RI-3], nel contesto della collaborazione con il laboratorio interuniversitario LIRIS di Lione (progetto di ricerca *FRIENDLY*), sono state analizzate le peculiarità delle applicazioni moderne e il loro impatto sulle tecniche di trust management esistenti. Sulla base delle sfide individuate, è stata definita una *roadmap* di ricerca, identificando una serie di macro-azioni di ricerca distribuite nel breve, medio, e lungo periodo. In [CI-2], la roadmap è stata ulteriormente rifinita e istanziata in maniera preliminare nel contesto dell'allocazione *fair* di risorse in computazioni basate su federated learning. Sulla base della roadmap, in [IS-1] è stato proposto un *trust management system* utilizzabile per applicazioni distribuite basate su servizi, in cui la trust viene aggiornata in funzione del tempo e dei cambiamenti nei servizi stessi.

12.2 Pubblicazioni

Dati tratti dal profilo Google Scholar <https://scholar.google.com/citations?user=dTTH3GgAAAAJ>

- Dati aggiornati all'11 Gennaio 2025.
- *h-index*: 8
- *Numero totale citazioni*: 139

- Dati aggiornati all'11 Gennaio 2025.
- *h-index*: 6
- *Numero totale citazioni*: 82

12.2.1 Specchietto riassuntivo delle pubblicazioni

L'attività di ricerca svolta è risultata in diverse pubblicazioni elencate in Sezione 12.2.2 e classificabili come segue:

- **3 Curatele di Volume** [CV-1, ..., CV-3]
- **8 pubblicazioni referate su Riviste Internazionali** [RI-1, ..., RI-8] di cui
 - 7 con SJR *Q1*
 - 1 con SJR *Q2*
- **13 pubblicazioni referate in atti di Conferenze e Workshop Internazionali** [CI-1, ..., CI-13]
- **3 Capitoli in Libri** [CL-1, ..., CL-3]
- **1 Tesi di Dottorato** [TD-1]
- **2 Altre Pubblicazioni** [AP-1, AP-2]
- **3 Paper In Sottomissione** [IS-1, ..., IS-3]

12.2.2 Elenco delle pubblicazioni

Curatele di volume

- CV-1 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 (to appear).
- CV-2 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-3 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.

Articoli in riviste internazionali

- RI-1 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*. DOI: 10.1109/TSC.2024.3486226
- RI-2 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
- RI-3 C. A. Ardagna, N. Bena, N. Bennani, N. Grecchi, C. Ghedira-Guegan, 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
- RI-4 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
- RI-5 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

- RI-6 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
- RI-7 Z. Zhang, S. Umar, A. 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
- RI-8 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

Articoli in atti di conferenze e workshop internazionali

- CI-1 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, Novembre 2024 (to appear).
- CI-2 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, Ottobre 2024 (to appear).
- CI-3 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, Cina, Luglio 2024 (**Fattore di accettazione 19.56%**). DOI: 10.1109/ICWS62655.2024.00071
- CI-4 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, Novembre – Dicembre 2023 (**Fattore di accettazione 17%**). DOI: 10.1007/978-3-031-48421-6_1
- CI-5 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, Luglio 2023 (*invited paper*). DOI: 10.1109/SSE60056.2023.00020
- CI-6 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, Grecia, Maggio 2023. DOI: 10.1007/978-3-031-51643-6_17
- CI-7 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, Agosto 2022 (**Fattore di accettazione 20.33%**). DOI: 10.1145/3538969.3539012
- CI-8 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)*, Barcellona, Spagna, Luglio 2022. DOI: 10.1109/ICWS55610.2022.00017
- CI-9 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, Finlandia, Giugno 2022. DOI: 10.1109/VTC2022-Spring54318.2022.9860757
- CI-10 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, Cina, Dicembre 2021. DOI: 10.1109/EDGE53862.2021.00015
- CI-11 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, Settembre 2021 (**Fattore di accettazione 23.7%**). DOI: 10.1109/ICWS53863.2021.00068
- CI-12 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)*, Parigi, Francia, Luglio 2020. DOI: 10.1007/978-3-030-90428-9_4

CI-13 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)*, Parigi, Francia, Luglio 2020 (**vincitore del premio “Best Student Paper Award”**). DOI: 10.5220/0009822600980109

Capitoli in libri/enciclopedie

CL-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

CL-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

CL-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

Tesi di dottorato

TD-1 N. Bena, “Non-Functional Certification of Modern Distributed Systems,” Tesi di Dottorato in Informatica, Relatore: Prof. Claudio A. Ardagna, Correlatore: Prof. Marco Anisetti, Università degli Studi di Milano, Gennaio 2024

Altre pubblicazioni

AP-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/>

AP-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/>

Paper in sottomissione

IS-1 N. Bena, G. Vargas-Solar, N. Bennani, C. Ghedira-Guegan, N. Grecchi, C. A. Ardagna, “Trust Negotiation in Dynamic Service-Based Applications” (sottomesso a *Future Generation Computer Systems*), 2025

IS-2 , N. Bena, M. Anisetti, E. Damiani, C. Y. Yeun, C. A. Ardagna, “Protecting Machine Learning from Poisoning Attacks: a Risk-Based Approach” (sottomesso a *Computers & Security*), 2024

IS-3 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” (sottomesso a *ACM Computing Surveys*), 2023

Data: 13 GENNAIO 2025

Luogo: MILANO

APPENDICE A: LETTERA DI INVITO PER VISITING PRESSO KHALIFA UNIVERSITY FEBBRAIO-APRILE 2025



Khalifa University of Science and Technology
Cybersecurity Theme Leader
Center for Cyber-Physical Systems
Computer Science Department
P.O.Box 127788, Abu Dhabi, UAE
T: +971-(0)-2-3124180
F: +971-(0)2-4472442
E: chan.yeun@ku.ac.ae
20 December 2024

RE: Dr. Nicola Bena: Visiting Scholar at C2PS on the PALM project

Dear Dr. Nicola Bena,

On behalf of the Center for Cyber physical Security (C2PS), Khalifa University, Abu Dhabi, we would like to invite Dr. Nicola Bena as a visiting scholar for one month for our mutual PALM project.

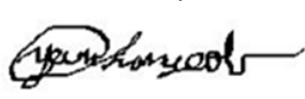
The first visiting month is due to start from the 15th of February to the 16th of March 2025.

The second month consists of a remote visiting and is due to start from the 17th of March to the 16th of April 2025.

Expenses will cover the first month and will be provided by Khalifa University as the visiting scholar.

We are Looking forward to collaborating with you soon.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Chan Yeob Yeun', enclosed in a thin black rectangular border.

Chan Yeob Yeun, Associate Professor, Ph.D., SMIEEE, MIET, MIMA, MBCS, CMath

Cybersecurity Theme Leader of Center for Physical Systems (C2PS), Khalifa University