

Jesús F. Cevallos-Moreno

Curriculum Vitae Accademico

Dipartimento di Scienze Teoriche e Applicate (DISTA), Università degli Studi dell'Insubria – Varese, Italia –
+39 333 8508324 – jf.cevallosmoreno@uninsubria.it – Sito web – [GitHub](#) – [Google Scholar](#) – [Scopus](#)

1. POSIZIONE ACCADEMICA E LAVORATIVA

Aprile 2024 **Assegnista di ricerca**
Oggi DISTA, Università degli Studi dell'Insubria
Progetto PRIN 2022 “[SERENA-IIoT](#): SEcure and REliable Networked Architecture for Industrial Internet of Things digital transformation”. Responsabile: Prof.ssa [Alessandra Rizzardi](#).

Marzo 2023 **Assegnista di ricerca**
Marzo 2024 DISTA, Università degli Studi dell'Insubria
Progetto “ESPE: Enforcing Security and Privacy at the Edge of the IoT networks”. Responsabile: Prof.ssa [Alessandra Rizzardi](#).

Sett. 2019 **AI Consultant**
Febbraio 2023 ELIS Innovation Hub, Roma
Attività di technical leading e design di soluzioni industriali mobile in ambito IA.

Sett. 2017 **AI Analyst**
Sett. 2019 ELIS Innovation Hub, Roma
Attività di sviluppo e manutenzione software centrata su mobile systems security.

Dic. 2013 **Full-stack Developer**
Sett. 2014 CFP Informatica srl, Roma
Sviluppo full-stack di web application framework proprietario.

2. FORMAZIONE

Sett. 2022 **Dottorato di ricerca in Ingegneria Informatica, XXXIV ciclo**
Università degli Studi di Roma “La Sapienza”
Tesi: *Deep Learning applications over Heterogeneous Networks: from Multimedia to Genes*.
Tutor: Prof. [Massimo Mecella](#); co-tutor: Prof. [Aminael Sánchez R.](#)

Luglio 2018 **Laurea magistrale in Ingegneria Informatica**
Università degli Studi di Roma “Tor Vergata”
Tesi: *Design of a mobile and distributed auto-adaptive system*. Relatore: Prof. [Vincenzo Grassi](#).

Marzo 2015 **Laurea triennale in Ingegneria Informatica**
Università degli Studi di Roma “Tor Vergata”
Tesi: *Progettazione e sviluppo full-stack di un web application framework proprietario per gestionali di case edili*. Relatore: Prof. [Giovanni Cantone](#)

3. PARTECIPAZIONE A PROGETTI E COLLABORAZIONI SCIENTIFICHE

- Sett. 2023 **Membro del progetto PRIN 2022 SERENA-IIoT**
Febbraio 2025 Ministero dell'Università e della Ricerca / Next Generation EU
Membro dell'Università degli Studi dell'Insubria per il progetto "SERENA-IIoT", finanziato dal MUR e dall'Unione Europea (Next Generation EU), codice progetto 2022CN4EBH.
- Sett. 2021 **Collaborazione scientifica con il gruppo del Prof. Aminaël Sánchez R.**
Ott. 2022 Universidad Técnica Particular de Loja, Departamento de Ciencias Biológicas y Agropecuarias
Ottimizzazione dei servizi di rete tramite meta-euristiche di ispirazione biologica.
- Sett. 2021 **Collaborazione scientifica con il gruppo del Prof. Peyman Zarrineh**
Ott. 2022 University of Manchester
Analisi di sequenze di DNA con strumenti di machine learning per la predizione di pattern di sviluppo del miocardio.
- Sett. 2014 **Collaborazione scientifica con il gruppo del Prof. Lorenzo Ricciardi-Celsi**
Marzo 2015 Joint Research Project tra Università degli Studi di Roma "La Sapienza", ELIS Innovation Hub ed ENEL
Tecniche di analisi del linguaggio naturale per l'estrazione di skill non dichiarate da curricula digitali.

4. ATTIVITÀ DIDATTICA

4.1 Docenze in corsi universitari

- A.A. 25/26 **Titolare dell'insegnamento ufficiale**
A.A. 24/25 Probabilità e Statistica per l'Informatica, Università degli Studi dell'Insubria
A.A. 23/24 Insegnamento per il corso di laurea triennale in Informatica, 48 ore.
- A.A. 22/23 **Didattica integrativa**
Advanced Coding Tools and Methodologies, Politecnico di Milano
Insegnamento per il corso di Laurea Magistrale in Music and Acoustic Engineering, 20 ore.
- A.A. 25/26 **Responsible lecturer**
Active Inference, Pontificia Universidad Católica del Ecuador Sede Santo Domingo
Digital Workshop for the EHIC Academic Week, School of Habitat, Infrastructure and Creativity, 24 ore.

4.2 Seminari

- Maggio 2026 **"Immunisation of Language Models"**
Pontificia Universidad Católica del Ecuador Sede Santo Domingo
Invited Keynote speaker at the EHIC Academic Week, School of Habitat, Infrastructure and Creativity, academic period 2026-01, 2 ore.
- Maggio 2026 **"Educarci per educare al tempo dell'IA"**
Università degli Studi dell'Insubria
Seminario tenuto nell'ambito dell'insegnamento in Intelligenza artificiale nel lavoro di comunità, Master per Educatori di Comunità Interculturali (EDC), 2 ore.

Maggio 2026	“Active Inference” Universidad Técnica Particular de Loja Seminario tenuto nell’ambito dell’insegnamento in Machine Learning, Corso di Laurea in Informatica, 2 ore.
Maggio 2026	“Introduction to Machine Learning” Pontificia Universidad Católica del Ecuador Sede Ibarra Seminario tenuto nell’ambito dell’insegnamento in Programmazione, Corso di Laurea in Informatica, 4 ore.
Novembre 2025	“Come programmare artificialmente un’intelligenza” Università degli Studi dell’Insubria Seminario tenuto nell’ambito dell’insegnamento in Informatica Giuridica, Corso di Laurea Magistrale a ciclo unico in Giurisprudenza, 2 ore.
Novembre 2024	“Principi di funzionamento dell’IA, vantaggi e svantaggi” Università degli Studi dell’Insubria Seminario tenuto nell’ambito dell’insegnamento in Informatica Giuridica, Corso di Laurea Magistrale a ciclo unico in Giurisprudenza, 2 ore.
Settembre 2024	“Inductive Biases for meta-learning” Università degli Studi di Napoli “Federico II” Seminario tenuto nell’ambito della collaborazione per il progetto PRIN 2022 “ SERENA-IIoT : SEcure and REliable Networked Architecture for Industrial Internet of Things digital transformation”, 1 ora.
Giugno 2024	“Machine learning for the IoT” Università degli Studi dell’Insubria Seminario tenuto nell’ambito del corso di dottorato in Informatica e Matematica Computazionale “Early design of Internet of Things networks towards real deployment” (XXXIX ciclo), 2 ore.
Novembre 2023	“IA e Cyber-security” Università degli Studi dell’Insubria Seminario tenuto nell’ambito dell’insegnamento in Informatica Giuridica, Corso di Laurea Magistrale a ciclo unico in Giurisprudenza, 2 ore.

4.3 Relatore di Tesi

A.A. 25/26	Relatore e correlatore di tesi
A.A. 24/25	Università degli Studi dell’Insubria
A.A. 23/24	Supervisione di tesi triennali e magistrali su cyber-defence / AI-safety in ambito IIoT, machine learning, active inference, mechanistic interpretability of language models, generative models, containerised environments e neuromorphic-AI.

	Numero di tesi	
	Relatore	Correlatore
Magistrale	0	2
Triennale	21	0

5. ATTIVITÀ DI RICERCA

Durante il dottorato, l'attività di ricerca si è incentrata su tecniche per migliorare l'efficacia e l'efficienza di training di pipeline di Deep Learning per il processing di grafi eterogenei. In particolare, si sono usati **inductive biases architetturali** e **tecniche di deep reinforcement learning** per la risoluzioni di problemi di ottiizzazione combinatoria in ambito telecomunicazioni, humman-resources e genomics. Tali attività di ricerca sono state svolte in collaborazione con altri istituti di ricerca quali l'UTPL, l'università di Manchester e il centro di ricerca EIH di Roma. [R5] [R6] [R7]

Attualmente, l'attività di ricerca si svolge presso il Dipartimento di Science Teoriche e Applicate (DISTA) dell'Università degli Studi dell'Insubria, nel gruppo dei prof. Coen-Porisini/Sicari/Rizzardi, dove si studiano e sviluppano **deep learning inductive biases per applicazioni in ambito cybersecurity e safety**. Più specificamente, la ricerca possiede tre stream principali:

1. **Online-learning e differenziabilità end-to-end** per pipeline di deep learning volte al **rilevamento di cyber-intrusioni in rete**. La ricerca si incentra sulla creazione di piattaforme e benchmark opensource realistici in ambito IIoT per un confronto equo e sistematico delle diverse architetture neurali e data sources. [R3] [C1] [C2] [R8] [R9] [R12] [R13] [R15]
2. Applicazioni di **Neural Algorithmic Reasoning e Active Inference** per aumentare la generalità di deep learning volte al **rilevamento e mitigazione di cyber-intrusioni in rete**. Il principale focus di questa linea di ricerca è il meta-learning, inteso come la caratterizzazione delle distribuzioni delle relazioni tra classi, in modo da generalizzare il criterio di separazione/identificazione di nuove classi in modalità zero-shot. [R1] [R2] [R11] [R14] [R16]
3. Tecniche per l'**allineamento/immunizzazione** dei modelli di linguaggio naturale open-source basati sulla **mechanistic interpretability**. Questo stream di ricerca si focalizza sull'implementazione di **tamper-proof safety policies** su modelli di linguaggio laddove il vettore di attacco non presuppone nessun constraint da parte dell'attaccante (open-weight models). [R4] [R10]

5.1 Indicatori bibliometrici

Articoli su riviste internazionali peer-reviewed	13	
Articoli in atti di conferenze internazionali peer-reviewed	2	
Articoli in fase di revisione	3	
Metrica	Google Scholar	Scopus
Citazioni	243	171
Hirsch-index	7	7

5.2 Pubblicazioni su Riviste Internazionali Peer-Reviewed

[R1]

Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **ASAP: Automatic Synthesis of Attack Prototypes, an online-learning, end-to-end approach**. *Computer Networks* (Elsevier): 110828 (2024).
[ScienceDirect](#)

[R2]

Jesus F. Cevallos-Moreno, Rizzardi, Alessandra, Sabrina Sicari, and Alberto Coen Porisini: **NE-RO: NEural algorithmic reasoning for zeRO-day attack detection in the IoT: A hybrid approach**. *Computers & Security* (Elsevier): 103898 (2024).
[ScienceDirect](#)

- [R3] Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **Deep Reinforcement Learning for Intrusion Detection in Internet of Things: Best Practices, Lessons Learnt, and Open Challenges**. *Computer Networks* (Elsevier): 236 (2023).
[ScienceDirect](#)
- [R4] Sabrina Sicari, Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Alberto Coen-Porisini: **Open-Ethical AI: Advancements in Open-Source Human-Centric Neural Language Models**. *ACM Computing Surveys*: Volume 57, Issue 4 (2024).
[ACM](#)
- [R5] L.R. Celsi, Jesus F. Cevallos-Moreno, F. Kieffer, V. Paduano (2022): **HR-specific NLP for the Homogeneous Classification of Declared and Inferred Skills**. *Applied Artificial Intelligence* (Taylor & Francis), 36 (2022).
[Taylor & Francis](#)
- [R6] Jesus F. Cevallos-Moreno, R. Sattler, R. P. Caulier C., L. R. Celsi, A. Sánchez Rodríguez, and M. Mecella (2021): **Online Service Function Chain Deployment for Live-Streaming in Virtualized Content Delivery Networks: A Deep Reinforcement Learning Approach**. *Future Internet* (MDPI) 13 (11): 278.
[MDPI](#)
- [R7] Jesus F. Cevallos-Moreno, P. Zarrineh, A. Sánchez, and M. Mecella (2022): **DeepReGraph Co-Clusters Temporal Gene Expression and Cis-Regulatory Elements through Heterogeneous Graph Representation Learning**. *F1000Research* 11: 518.
[F1000Research](#)
- [R10] Jesús F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **Ethical treatment of language models against harmful inference-time interventions**. *Engineering Applications of Artificial Intelligence* 172 (2026): 114317.
[ScienceDirect](#)
- [R11] Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **HE-RO: from Highdimensional network traffic to zERO-Day attack detection**. *Computer Networks* 265 (June 1, 2025): 111264.
[ScienceDirect](#)
- [R12] Alessandra Rizzardi, Raffaele Della Corte, Jesus F. Cevallos-Moreno, Vittorio Orbinato, Simona De Vivo, Sabrina Sicari, Domenico Cotroneo, Alberto Coen-Porisini: **SereWay: Toward Security and Reliability Benchmarking for the RailWAY IIoT**. *Journal of Network and Systems Management* 34, 52 (2026).
[Springer](#)
- [R16] Alessandra Rizzardi, Sabrina Sicari, Jesus F. Cevallos-Moreno, Alberto Coen-Porisini: **IoT-driven Blockchain to manage the Healthcare Supply Chain and protect Medical Records**. *Future Generation Computer Systems* (Elsevier): 161: 415-431 (2024)
[ScienceDirect](#)
- [R9] Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **TIGER: an opensource cyber-Threat Intelligence Game Environment for Reinforcement learning**. *IEEE Transactions on Network and Service Management* (2026).
[IEEE Xplore](#)

[R8] Jesus F. Cevallos-Moreno, Stefano Ianello, Giuseppe Grattacaso, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **SmartVille: A Framework for Realistic Deep Learning-Based Online Network Intrusion Detection**. *Journal of Network and Systems Management* 34, 4 (2026).

[Springer](#)

5.3 Proceedings di Conferenze Internazionali Peer-Reviewed

[C1] Alessandra Rizzardi, Raffaele Della Corte, Jesus F. Cevallos-Moreno, Vittorio Orbinato, Simona De Vivo, Sabrina Sicari, Domenico Cotroneo, Alberto Coen-Porisini: **RailRED: a Node-RED-based framework for modeling Train Control Management Systems**. 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2024).

[IEEE Xplore](#)

[C2] Alessandra Rizzardi, Raffaele Della Corte, Jesus F. Cevallos-Moreno, Vittorio Orbinato, Simona De Vivo, Sabrina Sicari, Domenico Cotroneo, Alberto Coen-Porisini: **Open-FARI: An Open-source testbed for Federated Anomaly detection in the Railway IIoT**. 21st International Wireless Communications & Mobile Computing Conference IWCMC 2025 IoTSN Symposium, Abu Dhabi, United Arab Emirates, 2025, pp. 764–769, doi: 10.1109/IWCMC65282.2025.11059481.

[IEEE Xplore](#)

5.4 Articoli sottomessi in fase di revisione

[R13] Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **Generalist Intrusion Detection through Neural Algorithmic Alignment: vision, applications & research challenges**.

Under Review.

[R14] Jesus F. Cevallos-Moreno, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: **ACID: beta-testing ACtive Inference for active cyber-Defence**.

Under Review. [TechRxiv preprint](#)

[R15] Alessandra Rizzardi, Raffaele Della Corte, Jesus F. Cevallos-Moreno, Vittorio Orbinato, Simona De Vivo, Sabrina Sicari, Domenico Cotroneo, Alberto Coen-Porisini: **SereBench: Adversarial Robustness Benchmarking for Security and Reliability Event Classification in Networked Railway Cyber-Physical System**.

Under Review.

6. COMPETENZE LINGUISTICHE

Lingua	Comprensione (Ascolto)	Comprensione (Lettura)	Parlato (Interazione)	Parlato (Produzione)	Scritto
Spagnolo	Madrelingua	Madrelingua	Madrelingua	Madrelingua	Madrelingua
Italiano	C2	C2	C2	C2	C2
Inglese	C1	C1	C1	C1	C1

7. ATTIVITÀ DI SERVIZIO ACCADEMICO

- TPC Member per IJCAI-25, ResGenXAI 2025 e SecSoft 25.
- Revisore per conferenze internazionali, tra cui WiMob24, IJCAI-25, IJCAI-26, ResGenXAI e SecSoft.
- Revisore per riviste internazionali, tra cui *Computer Networks*, *Pervasive and Mobile Computing*, *Transactions on Emerging Telecommunications Technologies*, *Internet Technology Letters*, *Journal of Information Assurance and Security*, *IoT, Electronics, Symmetry, Eng, Applied Sciences*, *International Journal of Computer Theory and Engineering*, *Computers & Security*, *Information, Sensors*, *IEEE Transactions on Industrial Informatics* e *IEEE Transactions on Information Forensics and Security*.

Il/La sottoscritto/a è consapevole che:

- è soggetto/a alle sanzioni previste dal codice penale e dalle leggi speciali in materia qualora rilasci dichiarazioni mendaci, formi o faccia uso di atti falsi od esibisca atti contenenti dati non più rispondenti a verità (art. 76 D.P.R. 28.12.2000, n. 445);
- decade dai benefici eventualmente conseguenti al provvedimento emanato sulla base della dichiarazione non veritiera qualora dal controllo effettuato dall'Amministrazione emerga la non veridicità del contenuto della dichiarazione (artt. 71 e 75 D.P.R. 28.12.2000, n. 445).

Autorizzo il trattamento dei dati personali ai sensi del Regolamento UE 2016/679. Aggiornato a 13 settembre 2026

Varese, 03/06/2026

Firma:
