Alex **Della Bruna**

Research Fellow @ University of Milan · MSc Cybersecurity Student @ University of Milan

dellabruna@di.unimi.it | alexdellabruna.github.io | alexdellabruna | alex-della-bruna | Alex Della Bruna

Education

University of Milan — *Milan, Italy*

MSc in Cybersecurity — *Sept. 2024 - Jul. 2026 (upcoming)*

- **GPA 28.15/30 (candidate for 110/110 cum laude)**
- Master's thesis focused on **LLM certification**: behavior (Github (preliminary), Hugging Face (preliminary)), internals (Github (preliminary)), LLM-based applications (Github), MLCertOps (Github, Github)

University of Milan — *Milan, Italy*

BSc in Security of Computer Systems and Networks — *Sept. 2021 - Jul. 2024*

- Graduation Mark 100/110
- Bachelor's thesis focused on a novel **distributed infrastructure** for **security assurance** (**Moon Cloud**)

ITT Vittorio Veneto — *Vittorio Veneto, Italy*

High School Diploma (Matura) in Computer Science and Telecommunications — *Sept. 2016 - Jun. 2021*

- Graduation Mark **100/100**
- Final project focused on **Modern Web Technologies (PWA)**
- Development of a modern web application for statistical data collection of players in the **italian A1 volleyball series** (**top-tier league**)

Academic Experience

University of Milan — *Milan, Italy*

Research Fellow @ SESARLab — *Aug. 2022 - ongoing*

- Research on **security assurance** and **certification** of **machine learning** and **cloud-edge continuum** systems
- **IT Coordinator**: management of the lab's **infrastructure**(hypervisors, kubernetes cluster, networking, etc.)
- Project **PNRR MUSA WP1** "A holistic, innovative digital architecture for the storage and safe exchange of life sciences big data":
  - **Monitoring** solutions for the MUSA WP1 **execution environment** and **machine learning** models developed by the pilots of MUSA WP1
  - Collaboration with **TIM** S.p.A, **Almaviva** S.p.A., and **Engineering** S.p.A.

Consorzio Interuniversitario Nazionale per l'Informatica (CINI) — *Rome, Italy*

Research Fellow — *Oct. 2023 - Sept. 2025*

- **Security assurance** evaluation of **distributed environments**
- Focus on **security assurance of machine learning** models

Industry Experience

Moon Cloud — *Milan, Italy*

Lead R&D Infrastructure and Platform Developer — *Aug. 2022 - ongoing*

- **Spin-off of the University of Milan**
- Design and implementation of a **fully decentralized backend architecture** based on cloud-native technologies
- Design and implementation of **continuous monitoring** techniques
- Design and implementation of **security assurance controls** for **cloud-based distributed systems** and **machine learning systems**.
- Collaboration with **Revetec** s.r.l. and **Aruba** S.p.A. (upcoming)

Publications

MSc Thesis: A Certification Framework for Large Language Models

University of Milan — *July 2026 (upcoming)*

- A. **Della Bruna**, M. Anisetti, C. A. Ardagna, N. Bena, "A Certification Framework for Large Language Models", Master's Thesis, University of Milan, Milan, Italy, July 2026
- Code available at: behavior (Github (preliminary), Hugging Face (preliminary)), internals (Github (preliminary)), LLM-based applications (Github), MLCertOps (Github, Github)

A Certification Scheme for Large Language Models-Based Applications PDF

ACM Transactions on Intelligent Systems and Technology (TIST) — *May 2026*

- N. Bena, M. Anisetti, E. Damiani, A. **Della Bruna**, C. Y. Yeun, C. A. Ardagna, "A Certification Scheme for Large Language Models-Based Applications"
- Code available at: UNIMI Dataverse

Proceedings of the 4th Italian Conference on Big Data and Data Science (ITADATA 2025) — *Turin, Italy*

PDF

CEUR-WS — *Jan. 2026*

- 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

ML Assurance in 6G-Enabled Edge-Cloud Continuum Workflows PDF *Milan, Italy*

IEEE Wireless Communications and Networking Conference (WCNC) *Mar. 2025*

- M. Anisetti, C. Ardagna, F. Berto, A. **Della Bruna** "ML assurance in 6G-enabled edge-cloud continuum workflows", in Proc. of IEEE WCNC 2025, Milan, Italy, March 2025
- Code available at: Github

BSc Thesis: Design e Sviluppo di un Sistema Distribuito Avanzato per Verifiche di Security Assurance PDF *Milan, Italy*

University of Milan *Jul. 2024*

A. **Della Bruna**, M. Anisetti, N. Bena F. Berto, "Design e sviluppo di un sistema distribuito avanzato per verifiche di security assurance", Bachelor's Thesis, University of Milan, Milan, Italy, July 2024

Professional Activities

Nov. 2026	**Publication Chair and TPC Member REF,** ITADATA 2026	*Bari, Italy*
Feb. 2026	**TPC Member REF,** IEEE/INNS IJCNN 2026	*Maastricht, Netherlands*
Oct. 2025	**Co-organizer REF,** Workshop on "Cybersecurity perspectives in the Post-Globalization Era" - IRIXYS 2025	*Milan, Italy*
Sept. 2025	**Publication Chair REF,** ITADATA 2025	*Turin, Italy*
Sept. 2025	**TPC Member REF,** Workshop on "Risks and Unintended Harms of Generative AI Systems" - ITADATA 2025	*Turin, Italy*

Theses Coordination

Bachelor's and Master's Theses *Milan, Italy*

Coordinator *Nov. 2023 - ongoing*

- **28 Bachelor's theses** coordinated
- 2 Master's theses coordinated
- Main topics: **security assurance, cloud-edge continuum, and machine learning**
- Several theses involved **practical collaboration with Moon Cloud**

Presentations

On Assessing the Order Bias of Large Language Models REF *Turin, Italy*

Workshop on "Risks and Unintended Harms of Generative AI Systems" - ITADATA 2025 *Sept. 2025*

- Preliminary results presentation
- Presented also at **Workshop on "Cybersecurity perspectives in the Post-Globalization Era" - IRIXYS 2025**, Milan, Italy, Oct. 2025 REF

Assurance in DevSecOps Pipelines REF *Pisa, Italy*

The 3rd Italian Conference on Big Data and Data Science (ITADATA 2024) *Sept. 2024*

- Proposal of a novel **DevCertOps** pipeline approach
- Integration with the Moon Cloud platform

Skills

AI/ML	Numpy, Scikit-learn, Pytorch, fine tuning (Axolotl, LLamaFactory, Unsloth), evaluation (Ragas, DeepEval), G-Ollama, vLLM
DevOps	AWS, Docker, Kubernetes, Rancher, Vagrant, Packer, Terraform, Jenkins, CircleCI
Programming and Markup Languages	C/C++, Java, Golang, Python, HTML, CSS, JS, PHP, Bash scripting, Latex
Framework	C++ API OpenGL, Maven, Bootstrap/Tailwind CSS, Angular, NodeJS, development of advanced logins with Auth0, PWA with Workbox/Angular's API, Gin, Django, Gorm, REST API development, i18n with Angular's API, cloud-native messagging with NATS
Security	Continuos monitoring through IDS/IPS and SIEM, security evaluation (assurance) based on testing and monitoring, authentication and autorization through OAuth2.0 with OpenID Connect support
Database	Relational (MySQL, PostgreSQL), non-relational (MongoDB, Redis)
CI/CD	Github Actions, Gitlab CI, AWS ECS services
AWS	EC2 instances, Route53, ECS/EKS with ECR, SQS, VPC
CloudFlare	DNS, Load Balancer, Argo Tunnel
Cloud computing and SOA	VMware, Hyper-V, Proxmox, oVirt, Docker, Docker Swarm, Kubernetes hypervisors
Kubernetes	microk8s, K3s, ArgoCD, Veeam Kasten, Helm, HashiCorp Vault, Lens, K9s
Network Design	Full stack ISO/OSI design (VLAN, subnet, routing (BGP, OSPF), firewall, IDS/IPS, WAF)
Linux/Windows Server Administration	Web server management (Apache, Nginx), domain management (Active Directory), file sharing (SMB and FTP)
Data Center Administration	iSCSI, iDRAC, Dell PowerVault, Dell Poweredge, NAS, SAN, BIND DNS

Languages

Italian - Native

English - **Proficient**, Certified B2+ (Pearson VEPT)

German - Basic

Personal Projects

OAuth2.0 SSO server *May 2023 - Jul. 2023*

- Design and implementation of an **OAuth2.0 server**
- Several **authentication flows** and **Single Sign On** support
- Code available at: Github

WAF engine extension and UI *Mar. 2022 - Jul. 2022*

- Design and implementation of a **Web Application Firewall**
- Management UI and **Modsecurity** engine extension to protect applications along the entire ISO/OSI stack
- Code available at: Github

Network asset discovery system *Oct. 2021 - Jan. 2022*

- Design and implementation of a software for **continuous asset mapping**
- Support for local and remote networks
- Code available at: Github

Mistervolley *Oct. 2020 - May 2021*

- Design and implementation of a web application for **collecting, surveying, and analyzing** on-site data during volleyball matches and training sessions
- Fully decentralized architecture based on **MEAN stack**
- Collaboration with professional coaches of women's **A1 italian volleyball series** (**top-tier league**)