Inés Ortega-Fernández

Vigo (Spain) | iortega@gradiant.org | Website | LinkedIn | GitHub

I hold a PhD in Information and Telecommunications Technologies from the University of Vigo. Since 2022 I have been a Technical Manager of Data Analytics and AI at the Security and Privacy department of the Galician Research and Development Centre for Advanced Telecommunications (Gradiant), where I manage and develop R&D projects on the use of AI techniques to address cybersecurity and data privacy issues.

Experience

Associate Lecturer at the Statistics and O.R. Department, University of Vigo Jan 2024 – July 2024

- Teaching the Statistics course for the Bachelor's Degree in Business Administration and Management.
- Course Content: descriptive statistics, calculation of probabilities, random variables, parametric inference.

Technical Manager of Data Analytics and AI, Gradiant – Vigo, Spain Apr 2022 – Present

- Oversee the development, implementation and research activities of a team of 25+ researchers in different R&D projects related to the use of AI for cybersecurity.
- Project coordinator of the PRESERVE Horizon Europe project (GA 101168309) to develop a privacy-preserving Big Data platform to support criminal investigations.
- Task and work package leader of different R&D projects (TRUMPET, INFINITECH)

Senior Researcher – Engineer, Gradiant – Vigo, Spain Mar 2020 – Mar 2022

- Development of novel solutions to improve security in industrial environments including the use of unsupervised anomaly detection and clustering techniques to detect advanced cyberattacks in real environments.
- Research and development of privacy and anonymization methods for the protection of personal data.
- Development of a novel data anonymization algorithm for GPS data which improves the current state-of-the-art in terms of the quality of the anonymised data points while providing a similar level of privacy.

Software Engineer, Microsoft – Vancouver, Canada Oct 2018 – Feb 2020

- Development of big data infrastructure to support processing of Windows telemetry.
- Improvement of data pre-processing and data aggregation jobs to provide increased value to the collected telemetry allowing to compute and report the cost of different processing jobs.

Education

PhD in Information and Telecommunications Technologies – University of Vigo, Oct 2020 – July 2024

- Thesis: *Machine Learning Approaches and Explainability for Real-Time Cyberattack Detection*
- Qualification: *Cum Laude*. International and Industrial mention.
- Supervisors: Marta Sestelo and Juan C. Burguillo

M.Sc in Cybersecurity – Carlos III University of Madrid Sept 2016 – July 2017

- Final Thesis: *Implementation of the General Data Protection Regulation in R&D in biometrics.*
- R&D grant at the University Group for Identification Technologies supporting development tasks on biometric recognition, working with Prof. Raul Sanchez-Reillo

B.Sc in Computer Science – Carlos III University of Madrid Sept 2012 – July 2015

- Final Thesis: *Biometric data capturing platform supporting data protection regulations.*
- R&D grant at the University Group for Identification Technologies supporting development tasks on biometric recognition, working with Prof. Raul Sanchez-Reillo
- Academic year 2015 – 2016 at the Aalto University (Helsinki, Finland)

Publications

These are my most relevant and recent publications. For a complete list, please visit my Google Scholar profile.

Journal papers

- Ortega-Fernandez, I., Sestelo, M., & Villanueva, N. M. (2023). Explainable generalized additive neural networks with independent neural network training. *Statistics and Computing*, *34*(1), 6. https://doi.org/10.1007/s11222-023-10320-5
- Ortega-Fernandez, I., Sestelo, M., Burguillo, J. C., & Piñón-Blanco, C. (2023). Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. *Wireless Networks*. https://doi.org/10.1007/s11276-022-03214-3
- Ortega-Fernandez, I., & Liberati, F. (2023). A review of denial of service attack and mitigation in the smart grid using reinforcement learning. *Energies*, *16*(2). https://doi.org/10.3390/en16020635

Conference papers

- Loureiro-Acuña, J., Martínez-Luaña, X., Padín-Torrente, H., Jiménez-Balsa, G., García-Pagán, C., & Ortega-Fernandez, I. (2024). Enhancing privacy in federated learning: A practical assessment of combined pets in a cross-silo setting. *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security*, 265–270. https://doi.org/10.1145/3658664.3659661
- Rodriguez-Viñas, J., Ortega-Fernandez, I., & Martínez, E. S. (2023). Hexanonymity: A scalable geo-positioned data clustering algorithm for anonymisation purposes. *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 396–404. https://doi.org/10.1109/EuroSPW59978.2023.00050
- Piñón-Blanco, C., Otero-Vázquez, F., Ortega-Fernandez, I., & Sestelo, M. (2023). Detecting anomalies in industrial control systems with lstm neural networks and ueba. *2023 JNIC Cybersecurity Conference (JNIC)*, 1–8. https://doi.org/10.23919/JNIC58574.2023.10205609

Software

- Ortega-Fernandez, I., & Sestelo, M. (2023, September). *Neuralgam: Interpretable neural network based on generalized additive models* [R package version 1.1.0]. https://CRAN.R-project.org/package=neuralGAM

R&D Projects

For a complete list of projects, please visit my website.

PRESERVE – Ethics and Privacy-preserving Big Data platform for Supporting criminal investigations

- Project coordinator and WP leader.

TRUMPET – TRUstworthy Multi-site Privacy Enhancing Technologies

- Research and development of privacy-enhancing technologies based on differential privacy for the protection of federated learning models.
- Research and development of privacy metrics based on the execution of membership inference attacks.

INFINITECH – Tailored IoT & BigData Sandboxes and Testbeds for Smart, Autonomous and Personalized Services in the European Finance and Insurance Services Ecosystem

- Development and evaluation of an advanced data anonymization tool.
- Research of novel methods for the anonymization of GPS data.

SafeNet UEBA – Centro de Operaciones de Seguridad basado en UEBA explicable

- Project Coordinator

CICERO – Contramedidas inteligentes de ciberseguridad para la red del futuro

- Research and validation of privacy-enhancing technologies for the protection of Large Language Models.