

José António Portela Areia

jose.apareia@gmail.com | github.com/joseareia | linkedin.com/in/joseareia

Professional Summary

Cybersecurity engineer with over four years of experience in artificial intelligence security, specialising in computer vision and AI-driven intrusion detection systems. More than two years' experience in higher education teaching, project supervision, and academic management. Skilled in coordinating team-based and individual work to achieve optimal results. Detail-oriented, focused, quick to learn, and a collaborative team player with a strong work ethic, consistently driving projects forward to deliver the best outcomes for the organisation.

Technical Skills

Languages: Python, Java, JavaScript, Bash, PHP, MySQL, Lua

Security Tools: Wireshark, Metasploit, Burp Suite, Nessus, Nmap, Wazuh

Security Practices: Risk Analysis, Vulnerability Assessment, Incident Response, Penetration Testing

Technologies and Frameworks: Linux, Docker, Git, PyTorch, TensorFlow, Scikit-Learn

Work Experience

Cybersecurity & AI Researcher, Computer Science and Communication Research Centre Feb 2022 – Present

- Created an innovative multi-objective generative model framework that can generate adversarial images, achieving an evasion success rate of up to 93% against as many as five distinct models.
- Developed AI-driven models for intrusion detection systems in the medical domain, achieving up to 97% accuracy in detecting malicious traffic across ten commonly used attack types.
- Researched vulnerabilities in ML models, focusing on privacy, security, and robustness against adversarial attacks.
- Developed IoT simulations for smart city and medical applications, including attack scenarios and traffic analysis.
- Published peer-reviewed research articles presenting key findings, methodologies, and openly available datasets.

Invited Assistant Professor, Polytechnic University of Leiria Sept 2023 – Aug 2025

- Teach in the short-cycle Cybersecurity and Computer Networks course.
- Supervise bachelor theses and manage multiple university projects within the short-cycle programme.
- Coordinate both team-based and individual work across various academic activities.

Full Stack Developer, Estudar Portugal Feb 2019 – Feb 2021

- Developed a Laravel web application for HR, document, and finance management.
- Designed the application's data model and user interfaces, while maintaining web and email servers.
- Implemented a Scrum methodology to enhance internal work organisation and efficiency.

Projects & Scientific Publications

Balancing Image Quality and Attack in Multi-Objective Adversarial Image Generation

- Created an innovative multi-objective adversarial GAN framework, internationally awarded and published by [KDD](#).

Fooling Rate and Perceptual Similarity: A Study on DCGAN-based Adversarial Attacks

- Conducted a study on DCGAN behaviour in adversarial sample generation. Presented at the [ARES](#) conference.

IoMT-TrafficData: Dataset and Tools for Benchmarking Intrusion Detection in IoMT

- Produced a dataset for an ML-based IDS system in IoMT. Paper published in [IEEE](#) and dataset on [Zenodo](#).

Dvorak: A Browser Credential Dumping Malware

- Developed a malware that retrieves web-stored passwords from five distinct browsers. Work published in [SECRYPT](#).

Education

Polytechnic University of Leiria, MSc Cybersecurity and Digital Forensics Sept 2023 – Present

- Grade: 18/20

Polytechnic University of Leiria, BSc Computer Engineering Sept 2020 – Jul 2023

- Grade: 16/20

Polytechnic University of Leiria, Short Cycle (TeSP) Web Development and Multimedia Sept 2018 – Jul 2020

- Grade: 20/20 — *Awarded Merit Student*