

# José António Portela Areia

[jose.apareia@gmail.com](mailto:jose.apareia@gmail.com) | [github.com/joseareia](https://github.com/joseareia) | [linkedin.com/in/joseareia](https://linkedin.com/in/joseareia)

## Professional Summary

Cybersecurity engineer with 4+ years securing AI-driven systems, networks, applications and IoT solutions, and 2+ years in higher education teaching and project management. Skilled in risk assessment and vulnerability management. Detail-oriented team player with a proven track record of actively contributing to complex, multidisciplinary projects.

## 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, Git Actions (CI/CD), 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 5 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 Aug 2023 – Sept 2025

- Taught Cybersecurity and Computer Networks, simplifying complex security concepts for diverse student groups.
- Supervised bachelor theses, guiding students through research and applied security projects.
- Led academic projects, showcasing leadership, organisation, and the successful delivery of multidisciplinary projects.

**Full Stack Developer**, Estudar Portugal Feb 2019 – Feb 2021

- Built and secured a Laravel-based HR and finance platform with authentication and data protection controls.
- Designed application data models and interfaces with a security-by-design mindset.
- Introduced and led adoption of the Scrumban methodology, improving efficiency and cross-functional teamwork.

## Projects & Scientific Publications

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

- Developed a Python-based multi-objective adversarial GAN framework achieving a 93% fooling rate across 5 models.
- Work internationally awarded and published in the [ACM KDD 2025](#) conference.

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

- Conducted a study using AI-based tools and frameworks on DCGAN behaviour in adversarial sample generation.
- Paper published and presented at the [ARES 2025](#) cybersecurity conference.

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

- Built a real-world IoMT environment and ML-based IDS dataset, achieving 97% accuracy in detecting malicious traffic.
- Paper published in [IEEE Access](#) and dataset on [Zenodo](#) (400+ downloads and 3000+ views).

**Dvorak: A Browser Credential Dumping Malware**

- Developed a Python-based malware that extracts and decrypts web-stored passwords from 5 major browsers.
- Work published and presented at the [SECURITY 2024](#) cybersecurity conference.

## Education

**Polytechnic University of Leiria**, MSc Cybersecurity and Digital Forensics Sept 2023 – Sept 2025

- 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*