# José António Portela Areia

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

## Professional Summary

Cybersecurity engineer with 4+ years' experience in AI security, specialising in computer vision and AI-driven intrusion detection systems. Over 2 years in higher education teaching, project supervision, and academic management. A strong team collaborator, detail-oriented, and highly adept at driving complex, multidisciplinary projects to successful outcomes.

## 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 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 — 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 Scrumban methodology to enhance internal work organisation and efficiency.

## 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 SECRYPT 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*