

AMIRMAHDI NOZARI

Bushehr, Iran | +98 991 720 7001 | private.amirmahdi@gmail.com
github.com/am1rx | medium.com/@amirmahdinozari

RESEARCH PROFILE

Computer Engineering graduate focused on SCADA/ICS security, intrusion detection, and cyber deception. First author of a Scientific Reports (Nature Portfolio) paper on hybrid neural-network attack detection in petrochemical SCADA networks, and developer of six open-source security tools — including an industrial deception grid that deploys decoy PLCs and a multi-protocol honeypot with MITRE ATT&CK mapping. Backed by hands-on enterprise network engineering (Cisco, Fortinet, MikroTik). Seeking a funded, research-based Master's position in ICS security, intrusion detection, or AI-driven network defense.

RESEARCH INTERESTS

SCADA & ICS Security • Intrusion Detection Systems • Cyber Deception & Honeypots • AI for Cybersecurity • Network Security & Defense

EDUCATION

B.Sc. in Computer Engineering Sep 2023 – Sep 2025

Islamic Azad University, Bushehr Branch, Iran — GPA: 16.89 / 20 ($\approx 3.4 / 4.0$)

Associate Degree in Computer Engineering Sep 2021 – Sep 2023

Technical and Vocational University, Iran — GPA: 17.39 / 20 ($\approx 3.5 / 4.0$)

PUBLICATIONS

[1] A. M. Nozari, M. Dashtdar, A. Chamkoori, “Design of an intelligent security system for cyber-attack detection in petrochemical SCADA networks based on a hybrid artificial neural network and Krill-Herd algorithm,” **Scientific Reports (Nature Portfolio)**, 2026. DOI: [10.1038/s41598-026-62131-z](https://doi.org/10.1038/s41598-026-62131-z)

OPEN-SOURCE SECURITY PROJECTS ([GITHUB.COM/AM1RX](https://github.com/am1rx))

- **MirageOT — Industrial Deception Grid (Python)** — multi-protocol OT/ICS deception platform that deploys decoy PLCs and industrial services to lure, detect, and study attackers; an open, hackable alternative to commercial platforms such as FortiDeceptor, TrapX, and Attivo. Directly complements my SCADA attack-detection research.
- **Advanced_Honeypot (Python)** — multi-protocol deception honeypot with MITRE ATT&CK technique tagging, SIEM integration via CEF events, and real-time attacker session tracking.
- **Reverse-Proxy-WAF (Python)** — scoring-based reverse-proxy Web Application Firewall with TLS termination, rate limiting, and a pluggable detection engine.
- **PHPWAF (PHP)** — lightweight, self-contained, behavior-driven WAF protecting PHP applications against SQL injection, XSS, and related web threats.
- **netscout (Python)** — network discovery and asset-inventory tool with ARP scanning, Nmap integration, and HTML/JSON reporting — applicable to asset visibility in enterprise and OT networks.
- **Fast-SQLi (Python)** — multithreaded scanner for detecting SQL-injection vulnerabilities in URL parameters.

PRACTICAL NETWORK ENGINEERING

- Designed and hardened segmented enterprise networks with Cisco and FortiGate: VLANs, L2/L3 routing and switching, NGFW/ISFW/DCFW architectures, least-privilege policies, FortiWeb application protection, and high-availability failover.
- Simulated and validated all designs in PNETLab, covering secure north–south and east–west traffic management.

PROFESSIONAL TRAINING

Completed instructor-led professional courses: Cisco CCNA (Routing & Switching) & CCNA Security · Fortinet NSE 4 (FortiGate), NSE 6 (FortiWeb), NSE 7 (Enterprise Firewall) · MikroTik MTCNA

TECHNICAL SKILLS

- **Security:** honeypot & deception-system development, WAF design, IDS/IPS concepts, firewall policy design, network hardening, web application security
- **Programming:** Python (security tooling, ML experimentation), PHP
- **Networking:** Cisco routing & switching, enterprise network design, MikroTik administration, PNETLab emulation
- **AI/ML:** neural networks and metaheuristic optimization applied to intrusion detection

LANGUAGES

Persian (native) • English (advanced; IELTS/TOEFL planned for late 2026)