

Maila Zahra

+92 (332) 546 7650 | s.mailazahra@gmail.com | [linkedin.com/in/mailazahra](https://www.linkedin.com/in/mailazahra)

Islamabad, Pakistan

EDUCATION

Bachelor of Science in Cyber Security

Sep 2021 – 2025

Air University, Islamabad, Pakistan – Ranked 9th in Pakistan in Cyber Security Programs

Thesis: Phishing and Brand Protection: Safeguarding Your Organization in Cyberspace Using AI/ML

Major coursework: Network Security, Information Security & Risk Management, Cryptography, Operating Systems, Penetration Testing, Digital Forensics, Software Engineering, Object-Oriented Programming, Data Structures

RESEARCH INTERESTS

AI & Security Research: Autonomous AI agents, agentic workflows, LLM security, offensive AI, prompt engineering, agent trace analysis (LangSmith), AI evaluation frameworks, benchmark design, AI red teaming

Security Operations & Data Analysis: AI-based SOC log analysis, alert triage, false-positive reduction, network security tools (IDS/IPS, honeypots)

PUBLICATIONS

- B. Saleem, M. Ahmed, M. Zahra, F. Hassan, M. A. Iqbal, and Z. Muhammad, “A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap,” *International Cybersecurity Law Review*, Springer, vol. 5, pp. 533–561, Sept. 2024.
- N. Ullah, M. Zahra, B. Saleem, M. Haseeb, M. Mughal, and Z. Muhammad, “DelSec: An anti-forensics data deletion framework for smartphones, IoT, and edge devices,” *International Conference on Engineering & Computing Technologies (ICECT)*, IEEE, Islamabad, Pakistan, May 23, 2024.
- B. Saleem, M. M. Zia, M. Zahra, F. Ahmad, and Z. Muhammad, “Smart Cities: A novel framework for energy production and harvesting using renewable energy,” *IEEE International Conference on IT and Industrial Technologies (ICIT)*, 2023.

OP-ED PUBLICATIONS

- M. Zahra and Z. Muhammad, “Post-Quantum Cryptography: Safeguarding the Digital Future and Bolstering Security in Critical Sectors,” *Cyber Defense Magazine*, Oct. 2023.
- Z. Muhammad and M. Zahra, “The Unintended Consequences of Electrifying Police Fleets,” *Scholars Strategy Network*, Oct. 29, 2024.

PROFESSIONAL EXPERIENCE

Air University CSOC | Air University Islamabad

Sep 2025 – Present, Islamabad, Pakistan

- Built a multi-agent AI framework that triages alerts, detects false positives, and drafts incident response playbooks, connected to Splunk and ELK to monitor security events.
- Improving the framework with prebuilt benchmarks, prompt engineering, and cost-cutting strategies.
- Set up automated AI-based analysis of SOC logs.
- Monitored and analyzed security events using Splunk and ELK Stack, performing alert triage, log correlation, escalation, and false-positive tuning.
- Conducted vulnerability assessments using Nessus, Nmap, and OWASP ZAP with risk-based prioritization and remediation tracking, feeding results into risk registers and treatment plans.
- Aligned GRC requirements (ISO/IEC 27001:2022 and PISF) with CSOC monitoring, detection, and incident response processes, ensuring policy obligations are supported by operational controls.
- Mapped ISO/IEC 27001 Annex A controls – logging (8.15), monitoring activities (8.16), incident management (5.24–5.28), and technical vulnerability management (8.8) – to SIEM use cases, alert rules, and SOC SOPs.
- Performed policy and control gap analyses against ISO/IEC 27001 and PISF; compiled audit evidence from SOC logs, incident records, and scan reports.
- Drafted and maintained security policies, SOPs, and incident response playbooks aligned with the ISMS, and produced compliance and threat reports for management.
- Tracked SOC and compliance metrics (incident volume, response times, open vulnerabilities, control coverage) to support risk reviews and continual improvement.

Cyber Security Lab Engineer | Air University Islamabad

Sep 2025 – Present, Islamabad, Pakistan

- Delivered ICT support across hardware, software, and network troubleshooting.
- Configured and maintained computer networks to ensure reliable connectivity and secure data flow.
- Applied parallel and distributed computing concepts to optimize system performance.
- Conducted digital forensic investigations, analyzing evidence and preparing formal reports.

Network Engineer Intern | Cytomate Qatar (Doha)

Jun 2024 – Mar 2025, Remote – Pakistan

- Contributed to the development of an AI-based brand protection tool targeting phishing and impersonation.
- Supported real-time network monitoring and automated incident detection mechanisms.
- Provided input on incident response workflows and threat detection automation.

Security Researcher Intern | Siber Kuza – National Aerospace Science and Technology Park (NASTP)

Jun 2023 – Sep 2023

- Performed network vulnerability assessments and penetration testing.
- Analyzed security incidents and supported the development of threat intelligence reports.
- Assisted in preparing compliance documentation aligned with cybersecurity standards.

RESEARCH & PROJECTS

Security AI Agents and AI Harness for Network Security Tools

- Researching and building security AI agent tools using LangGraph, LangSmith, and prompt engineering.
- Created an AI harness for network security tools, including IDS/IPS and honeypot systems.

AI-Based Brand Monitoring Tool for Threat Detection and Reputation Management

Supervisor: Dr. Zunaira Jalil – Associate Professor, Air University Islamabad

- Built a Python-based tool to monitor brand mentions across social platforms and forums.
- Applied NLP and sentiment analysis to detect impersonation and brand misuse.
- Enabled real-time alerts for phishing and fake-profile detection.
- Focused on proactive brand protection and digital reputation management.

Honeypot System for Threat Detection and Network Forensics

Supervisor: Engr. Maryam Mehmood Malik – Lab Engineer, Air University Islamabad

- Deployed a low-interaction honeypot simulating vulnerable services to attract attackers.
- Captured malicious traffic for analysis to understand intrusion techniques.
- Enhanced incident detection capability through real-time logging and alerting.
- Supported training use cases in cyber threat intelligence and SOC operations.

Study of Post-Quantum Cryptography and Its Impact on Digital Security

- Analyzed NIST's post-quantum cryptography standardization efforts and their relevance to security policies, cryptographic standards, risk mitigation strategies, and organizational compliance frameworks, particularly for preparing critical sectors for quantum-era threats.
- Assessed the need for **cryptographic risk assessments, migration planning, security controls, and governance policies** to support organizational readiness for emerging quantum-related threats.

SKILLS

AI & Agent Tooling: LangGraph, LangSmith, prompt engineering, multi-agent AI frameworks, NLP

Programming: Python, Object-Oriented Programming, Data Structures

Standards & Frameworks: ISO/IEC 27001 (ISMS), ISO/IEC 42001 (AI Management System), NIST Risk Management Framework (RMF), NIST AI RMF, CIS Controls, GDPR, PISF 2026, CTDISR, MITRE ATT&CK, OWASP Top 10 for LLM Applications

Cybersecurity Techniques: Vulnerability Assessment (scanning, prioritization, remediation tracking), Threat Intelligence, Log Analysis, SIEM Analysis (SOC Environment), Firewall Configuration, OSINT Investigation, Network Traffic Monitoring

Security Tools & Technologies: SIEM: Splunk, ELK Stack | IDS/IPS & Firewall: Snort, pfSense | Honeypots | Nmap, Wireshark, OWASP ZAP, Nessus, Kali Linux, Ubuntu Server, VirtualBox, Autopsy, FTK Imager, Cisco Packet Tracer

Technical Writing & Documentation: Security Policies, Standards & SOPs; Risk Assessments & Risk Registers; Compliance and Audit Reports; Control Documentation; Threat Reports; Incident Response Procedures; Business Continuity & Disaster Recovery Documentation; Governance Frameworks; Security Awareness Material; Research Publications

CERTIFICATIONS & COURSES

ISC2 Certified in Governance, Risk and Compliance (CGRC) – Red Teamers

Cybersecurity Essentials – Cisco Networking Academy – Jul 2024

INTERNATIONAL CONFERENCES ATTENDED

- International Conference on Engineering & Computing Technologies (ICECT), IEEE – NUML University, Islamabad, Pakistan – [May 23, 2024](#)
- International Conference on IT and Industrial Technologies (ICIT), IEEE – FAST University, Islamabad, Pakistan – [2023](#)

ACHIEVEMENTS

International – Global CTF Rank: Top 4 in BSides Fargo CTF (USA), outcompeting 200+ teams in exploit development.

International – Black Hat MEA 2024 (Saudi Arabia): Ranked Top 5 in Pakistan (55th overall) in advanced penetration testing challenges.

2nd Place – Ignite Hackathon 2024 (Red Teaming): Demonstrated offensive cybersecurity skills and vulnerability exploitation.

1st Place – CTS '24 CUI Tech Summit Hackathon: Showcased excellence in cybersecurity innovation and teamwork.

1st Place – PUCON CTF 2023 (Punjab University, Lahore): Specialized in OSINT, outperforming multiple teams.

Wall of Fame: Recognized for outstanding cybersecurity contributions (Aug 2024 – Present).

EXTRA-CURRICULAR

Vice President, Air University Cyber Security Society (AUCSS) – [Sep 2024 – Apr 2025](#)

Management Lead, Air University Cyber Security Society (AUCSS) – [Aug 2023 – Mar 2024](#)

Security Lead, 3rd Annual IEEE Cyber Warfare Conference, Air University Islamabad – [December 7–8](#)

Social Media Coordinator, Air University Air Tech Event '24 – [Apr 4, 2024](#)

REFERENCES

Dr. Muhammad Imran, Assistant Professor
Department of Cyber Security, Air University, Islamabad,
Pakistan
Email: m.imran@au.edu.pk

Dr. Zia Muhammad, Professor
Department of Computing, Design, and Communication,
University of Jamestown, USA
Email: zia.muhammad@uj.edu