Faisal AlRomaihi

Faisalalromaihii@gmail.com | 38831000 | Personal Website | Linkedin | Github

Education

University of Edinburgh , MSc in Cyber Security, Privacy, and Trust — Sept 2024 – Sept 2025

- Dissertation: Privacy for Hire – Incentivising Scalable, Secure, and Fair Anonymous Communications

University of Bahrain , BS in Software Engineering — Sept 2020 – May 2024

- GPA: Excellent (3.58/4.0)

Research

MSc Dissertation : Privacy for Hire – Incentivising Scalable, Secure, and Fair Anonymous Communications — May 2025 - Aug 2025

- *University of Edinburgh*, Supervisor: Dr Tariq Elahi. Analyzing volunteer, commercial, and cryptoeconomic models to evaluate their impact on privacy guarantees, decentralization, and network sustainability. Uses game-theoretic modeling and simulation to study relay operator behavior, Sybil resistance, and reward fairness.

Experience

Cyber Security Specialist, National Cyber Security Center (NCSC), Bahrain — Feb 2026 – Present

- Designing and managing enterprise-grade Web Application Firewall (WAF) policies to protect national-level digital infrastructure
- Developing and maintaining network security architecture standards across government entities
- Contributing to national cybersecurity policy frameworks and security architecture reviews
- Advising on security controls, threat modeling, and risk mitigation strategies

Software Engineer Intern, GBM — July 2023 - Aug 2023

- Built and deployed a company-wide meeting room booking system using PHP, MySQL, and JavaScript, adopted in production
- Implemented room availability search, calendar integration, conflict resolution, and admin controls for non-technical staff

Certifications

AWS Certified Solutions Architect – Associate, *Amazon Web Services* — March 2026

Projects

Revealing Weaknesses in Google reCAPTCHA Using Adversarial ML — May 2025

- Assessed vulnerabilities in Google reCAPTCHA (v2/v3) using adversarial ML techniques (e.g., FGSM, PGD, SimBA)
- Demonstrated risks of model extraction and membership inference attacks
- Proposed mitigations including adversarial training, federated learning hardening, and privacy-aware design

ML for Genre Clustering and Popularity Forecasting from Spotify Charts — Dec 2024

- Clustered 7,700+ songs using PCA and GMM based on genre and audio characteristics
- Engineered features and trained classifiers to predict hit songs and popular artists (F1-score: 0.89)
- Forecasted top 2024 artists using ARIMA, Prophet, XGBoost, and LightGBM

FairPlay: Secure Two-Player Smart Contract Using Commit-Reveal on Ethereum — Dec 2024

- Developed a commit-reveal smart contract game on Ethereum Sepolia ensuring fairness and state consistency
- Prevented reentrancy and cheating with pull-payment patterns and refund logic
- Optimized gas usage with efficient storage and completed full game cycle testing

Secure Programming: Vulnerability Analysis & Defense Nov 2024

- Exploited CVEs (e.g., CVE-2024-3094, CVE-2020-11899) to demonstrate memory and logic vulnerabilities
- Hardened a Flask-based VPN system against STRIDE-modeled threats (e.g., spoofing, tampering, escalation)
- Applied secure coding practices (AES encryption, PBKDF2, RBAC, session security) for backend defense limiting

Technologies

Languages: C++, C, Java, Python, SQL, JavaScript, Solidity, HTML, CSS, PHP

AI/ML Tools & Libraries: Pandas, NumPy, Scikit-learn, XGBoost, LightGBM, Prophet, TensorFlow, Matplotlib

Cybersecurity & Blockchain: Kali Linux, Wireshark, STRIDE Threat Modeling, Memory Safety (CWE/CVE Analysis), Secure Coding, Anonymity Networks (Tor, Nym), Smart Contracts, Ethereum, Hardhat, Sybil Resistance

Web & App Frameworks: React, Next.js, Django, Flask, Bootstrap

Databases & Tools: MySQL, PostgreSQL, MongoDB, Git, Docker, Jupyter Notebook, Maven, Game-Theoretic Modeling