Zuhair Khan

☎ +1 (437) 423-1620 | ✉ zuhair.khan@mail.utoronto.ca | zuhair-mzk | LinkedIn | zuhairkhan.ca

Education

University of Toronto Scarborough Sep 2022 – Dec 2026 (Expected)
Honours B.Sc. in Computer Science (Software Engineering Specialist) *Toronto, ON*

- **University of Toronto Scholar Award** — $7,500 merit scholarship (**top 3%**).
- **Key coursework:** Cybersecurity, Networks, Algorithms, Operating Systems, Quantum Computing, Databases.

Cybersecurity Training

- **Google Cybersecurity Professional Certificate (v2)** — Google/Coursera
- Hands-on labs with **SIEM** (Splunk, Chronicle), **tcpdump/Wireshark**, **Linux hardening**, SQL log analysis, and Python-based security automation.
- Performed **incident response** workflows, threat modeling, risk assessment, and **SOC-tier security analysis**.

Security, Networking & Systems Engineering Projects | View All

Production-Grade Software Router | **GitHub** | C, Mininet, Wireshark, RFC 791/792/826

- Implemented an **RFC-compliant IPv4 router** (2,000+ LOC C) with **Longest Prefix Match**, **ARP cache**, and full **ICMP** stack; achieved **100%** pass rate across ping, **traceroute**, HTTP, and stress tests.
- Performed **deep-packet inspection** and debugging using **Wireshark**, **Mininet**, and real traffic traces.
- Expanded coverage with **packet crafting** and trace analysis for edge-case debugging.

Cybersecurity CTF Portfolio (15+ Challenges) | **GitHub** | Crypto, Reverse Eng., PCAP Analysis

- Solved challenges across cryptography **(AES/ChaCha20)**, binary exploitation, Docker misconfig attacks, TLS inspection, **ARP spoofing, and SQLi**.
- Built tooling with **Python**, **Bash**, and **Scapy** for packet injection, payload automation, and **PCAP forensics**.

Intrusion Detection System (IDS) | **GitHub** | Python, PCAP, Anomaly Detection

- Developing a network-based IDS with **signature-based** and **anomaly-based detection** over parsed **Ethernet**/**IP**/**TCP**/**UDP** frames.
- Implementing **live packet capture**, malicious pattern detection, and configurable thresholds to reduce false positives.

Offline Social Network — Security Engineering Contributions | **App Store** | Node.js, JWT, API Security

- Performed backend **security review**: patched input sanitization gaps, added **rate limiting**, and mitigated **SQL injection** vectors.
- Redesigned authentication using **short-lived JWTs**, secure refresh tokens, **device-bound sessions**, and hardened password storage (**bcrypt**/**argon2**).
- Implemented **privacy-preserving** location handling and **audit logging** for sensitive API actions.

Concurrent System Monitoring Tool | **GitHub** | C, Linux, IPC, Signals

- Built a multi-process **Linux system monitor** using **fork()**, **shared memory**, and **POSIX signals** to track CPU/memory of **100+ processes**.
- Packaged with **Makefile**/**Dockerfile** and hardened error paths; emphasizes **systems-level reliability**.

Technical Skills

Security & Networking: Wireshark/tcpdump, Scapy, Nmap, Splunk/Chronicle, Linux hardening, JWT auth, SQLi/XSS/CSRF mitigation, IDS/NIDS, IPv4/ICMP/ARP, RFC 791/792/826, Mininet, SDN/OpenFlow, POX controller
Languages/Tools: Python, C/C++, Java, TypeScript/JavaScript, SQL, Bash, MIPS, Docker, Git/GitHub, PostgreSQL, MongoDB, SQLite, Vercel
Certifications: Google Cybersecurity (v2), Qiskit Summer School (QE), **CompTIA Sec+ (in progress)**
Quantum-Safe (Research): PQC (Kyber/Dilithium), lattice cryptography, QKD (BB84/E91), noise models, error mitigation

Quantum-Safe Research

Quantum-Safe Security: PQC, QKD & Cryptographic Hardening | **View Project** Aug. 2025 – Present
Undergraduate Researcher — Supervisor: Prof. Marcelo Ponce *University of Toronto*

- Analyzing **QKD protocols** (**BB84**, **E91**) vs. standardized **lattice-based PQC** (**Kyber**, **Dilithium**) to design **quantum-safe network security** for **TLS-like infrastructures**.
- Developing **Python**/**Qiskit**/**PennyLane** pipelines to run 10^3–10^4**-shot** simulations for **noise tolerance**, **QBER** thresholds, and adversarial attacks (**intercept–resend**, **PNS**).
- Producing **hybrid PQC/QKD migration strategies** for **identity**, **authentication**, and **encrypted session layers**; **Winner**, 2025 **CMS Undergraduate Research Symposium**.