UMARA HANIF

Final Year Ph.D. Student

PROFILE

Cybersecurity researcher with expertise in fortifying digital infrastructures against sophisticated threats. Specialising in hardware security, IoT devices, and FPGA security as a current researcher. Dedicated to advancing resilience against evolving cyber threats through innovative solutions and collaborative efforts.

CONTACT

umara.hanif@u.nus.edu

https://www.linkedin.com/in/umara-hanif-5a86021a6/

Cisco Corp, Block E1A #03-03, NUS,
Singapore

EDUCATION

NATIONAL UNIVERSITY OF SINGAPORE, PHD

Aug 2022 — Jul 2026 Singapore

Electrical and Computer Engineering

UNIVERSITY OF ENGINEERING & TECHNOLOGY, B.SC

Oct 2016 — Aug 2020 Lahore

Computer Science

PROJECTS

ALEXIS: ANOMALY-BASED INTRUSION DETECTION IN FPGA-ENABLED CYBER-PHYSICAL SYSTEMS

FPGA Security | Machine Learning | Embedded Systems

- Developed Alexis, a lightweight intrusion detection system leveraging autoencoder neural networks to detect hardware Trojans in FPGA bitstreams.
- Achieved 91% accuracy with high AUC (0.96) and minimal reconstruction error (MSE/MAE), proving its reliability in real-time hardware monitoring.
- Optimized for embedded use with <0.021s latency and 1.14 MiB memory usage, ideal for resource-constrained FPGA platforms.
- Positioned Alexis as a scalable, high-accuracy solution for cyber-physical hardware security.

ENVOT: SECURE ATTESTATION OF IOT SWARMS USING ENSEMBLE LEARNING

IoT Security | Machine Learning | Edge Computing

- Engineered ENVOT, a hybrid attestation framework combining VAEs, Random Forest, and XGBoost with a weighted voting scheme for IoT SWARM security.
- Extracted 10% RAM for feature collection to ensure low-power, low-latency attestation; achieved 90% detection accuracy.
- Demonstrated 66.25% latency reduction and 60.63% lower energy consumption over prior state-of-the-art.
- Defended against diverse attacks (e.g., firmware tampering, DoS, side-channel), showing strong relevance to trusted hardware environments.

FFAT: A SEMANTICS-AWARE FRAMEWORK FOR FPGA HARDWARE FUZZING

Hardware Validation | Fuzz Testing | Formal Analysis

- Created FFAT, the first semantics-aware fuzzing framework tailored for runtime anomaly detection in FPGAs, deployed on Xilinx ZCU102.
- Combined formally guided fuzzing, semantic-aware mutation, and real-time anomaly injection to simulate fault scenarios (e.g., rowhammer, voltage spikes).
- Achieved 97% accuracy and reduced fault detection time by 35.8%, outperforming state-of-the-art fuzzers.
- Enabled detection of stealth hardware Trojans and generalized to unseen attacks via open-set classification

SKILLS

PROGRAMMING LANGUAGES

- Python
- C/C++
- Verilog/VHDL
- Bash/Shell Scripting

PLATFORMS & TOOLS

- Vivado/Vitis
- Linux
- Real-Time OS concepts for embedded security
- Xilinx ZCU102
- Arduino
- Metasploit
- W3AF
- Wireshark
- MATLAB

FRAMEWORKS & LIBRARIES

- Scikit-learn
- TensorFlow
- Keras
- Autoencoders/Variational Autoencoders
- SMOTE
- NumPy
- Pandas
- Scapy
- Psutil
- Tracemalloc
- Attack simulation frameworks
- Custom ensemble learning pipelines

EXPERIENCE

RESEARCH INTERN, AMD SINGAPORE

Jul 2025— Dec 2025 Singapore

As a Research Intern, I worked on optimizing LLM inference on AMD GPUs, focusing on how different scheduling and batching choices affect performance. I set up offline profiling runs in vLLMs to examine prefill and decode behavior, collect analyzer-friendly traces, and identify pipeline inefficiencies. I also explored how input length, batch size, and KV-cache limits influence latency metrics, running controlled sweeps and tying the results back to the model/runtime's reported concurrency on the hardware.

CYBERSECURITY ENGINEER, VAPORVM

Dec 2021— Jul 2022 Lahore

As a cybersecurity engineer, I fortified digital infrastructures against sophisticated threats, ensuring integrity, confidentiality, and availability of critical systems. Responsibilities included implementing robust security measures, conducting vulnerability assessments, and devising proactive strategies. Collaborated with cross-functional teams to develop and enforce security policies, conduct incident response procedures, and provide ongoing training. Stayed abreast of emerging threats and technologies to refine security protocols continuously.

CYBERSECURITY RESEARCH ANALYST, VULTARA, INC.

Jun 2021 — Nov 2021 Detroit

Engaged in security research initiatives focusing on IoT automotive and medical device product security. Conducted research to identify known threats and vulnerabilities associated with popular protocols, products, and weaknesses inherent in IoT devices.

ETHICAL HACKER, PROGRAMMERS FORCE

Nov 2020 — Mar 2021 Lahore

Performed vulnerability assessments, conducted penetration tests, created detailed reports on security weaknesses, and advised on corrective measures like system upgrades and patches.

RESEARCH ASSISTANT, HUAWEI TELECOM & IT CENTRE

Jun 2019 — Jun 2020 Lahore

Conducted analysis of encrypted traffic to discern patterns and potential security risks. Engaged in research endeavors to explore vulnerabilities and attack vectors within encrypted traffic. Utilized machine learning algorithms, designed and developed a model to identify and analyze malicious activities present in encrypted traffic.