Muhammad Ahsan

Richmond, Virginia, 23220, USA

ahsanm5@vcu.edu mahsan321.github.io/Portfolio/ +1(804) 591 6460

Ph.D. Candidate in Computer Science with 8+ years of research experience in cybersecurity, IoT security, and cyber-physical systems. Dedicated to integrating teaching with innovative research to advance digital forensics, malware analysis, and side-channel defenses.

Education

Virginia Commonwealth University (VCU) — **Richmond, Virginia USA**
PhD in Computer Science (CGPA: 4.00) — *Aug 2021 - (Continued)*

University of Engineering and Technology (UET) — **Lahore, Pakistan**
Master of Electrical Engineering (CGPA: 3.75) — *Jan 2015 - July 2018*

University of Engineering and Technology (UET) — **Lahore, Pakistan**
B.Sc. Electrical Engineering (CGPA: 3.70) — *Aug 2010 - June 2014*

Research Interests

Artificial Intelligence, Cybersecurity, Digital Forensics and Malware Analysis, Side-Channel Analysis, IoT Security, Secure Additive Manufacturing, Cyber-Physical Systems Security.

Awards and Achievements

- US Cyber Command Cyber Recon 2025, Best category Defender Award.
- US Cyber Command Cyber Recon 2024, Best category Guardian award.
- US Cyber Command Cyber Recon 2024, Commander's award for outstanding research.
- 4-star challenge coin, Got recognized by General Timothy D. Haugh, commander of the United States Cyber Command and director of the National Security Agency.
- People's Choice Award 2024, MegaHack@VCU
- Dean's Honor Certificate (5 semesters), UET Lahore.
- B.Sc. Electrical Engineering with honors.

Industry/Research Projects

Academic Research

Security and Forensics Engineering (SAFE) LAB — **Position: Graduate Assistant**
VCU, Richmond — *Aug 2021 - Current*

Project Title: Side Channels for Securing Cyber-Physical Systems (CPS).
Description: My research is centered around securing the additive manufacturing process chain using side-channel data. My work explored both the offensive and defensive sides of polymer-based 3D printing and 3D bioprinting.

- Investigated the attack side of the printing process, where an adversary could add malicious changes to the printed construct, consequently altering their mechanical/biochemical properties.
- Proposed monitoring frameworks for detecting malicious variations in the 3D printing process using side-channel data.

Applied/Industry Research

Al-Khawarizmi Institute of Computer Science (KICS) — **Position: Sr. Research Officer**
UET, Lahore — *Oct 2014 - July 2021*

Project Title: Lightweight security framework for IoT.
Description: Worked on the Interoperability and Security challenges associated with IoT devices following OneM2M specification. The project includes the following modules

- Implementation of horizontal layer OneM2M standard framework for M2M and IoTs.
- Sensor nodes on MbedOS running over Nucleo STM32 L476rg boards. MQTT client/broker model implementation on Raspbian OS running on Raspberry Pi 3.
- Gateway application that supports DTLS for MQTT-SN multithreaded gateway application.

GitHub Link: https://github.com/AikM2M

Other Industrial Projects

Smart Home: Worked on a customized smart home solution. Designed and developed a gateway device for connecting to smart plugs and switchboards.
Smart Irrigation: Using LoRaWAN to develop a gateway application that collects and updates moisture sensing data to the user's mobile application.
IoT Firewall: Worked on analyzing, writing, and testing firewall rules for SCADA/IoT Protocols. Evaluate the firewall by reproducing reported Common Vulnerabilities and Exposures (CVEs) and generating different attacks on the network to test the rules.
Automation Projects: Automated the Paddy dryer for the rice mill industry and university water storage tanks.
Solar thermal Collectors: Worked on the design and implementation of solar tracking systems for industrial-grade heliostats and parabolic troughs.
Motor test Bench: Designed and developed an industrial standard motor test bench for IEC 60034-2-1 compliance testing.

Major Subjects

Memory and Malware Forensics	High Performance Distributed Systems
Network Security	Design and Analysis of Algorithms
Advance Operating System	Machine Learning

Teaching/Mentoring Experience

- Instructor - PLC short courses, UET Lahore
- Graduate Assistant - CMSC 355, VCU
- Invited Speaker - Seminar series, VCU
- Mentored multiple undergrad students on research projects.
- Development of energy efficiency advisory course in collaboration with sequa gGmbH – GiZ

Academic Services

- Conference Manager (2016-2019): IEEE International Conference on Open Source Systems and Technologies (ICOSST).
- Conference Manager (2017, 2018): IEEE International Conference on Energy Conservation and Efficiency (ICECE).
- Reviewer Services: IEEE IoT Journal, FSI Digital Investigation, Computers & Security

Publication List

1. Muhammad Haris Rais, **Muhammad Ahsan**, Irfan Ahmed, "PrintSafe - A near real-time anomaly detection framework for fused filament fabrication printing using printing environment estimation", Journal of Manufacturing Processes, **Submitted (under review).**
   (Q1 Journal with an impact factor of 6.03 in 2023)
2. **Muhammad Ahsan**, Eunice Pak, Kate Jackson, Muhammad Haris Rais, Barry Najarro-Blancas, Nastassja Lewinski, Irfan Ahmed, "BioSaFe: Bioprinting Security Framework for Detecting Sabotage Attacks on Printability and Cell Viability", In the 40^{th} IEEE Annual Computer Security Applications Conference **(ACSAC)**, Dec 2024, Hawaii.
   (Acceptance rate (21.5%): 83 out of 381 submissions)
   *(Included in the VA Commonwealth Cyber Initiative's **2025 CCI Research Showcase**, a curated collection of significant, influential peer-reviewed research papers published in the last two years.)*
3. **Muhammad Ahsan**, Irfan Ahmed, "WattShield: A Power Side-Channel Framework for Detecting Malicious Firmware in Fused Filament Fabrication", In the 18^{th} IEEE International Symposium on Hardware Oriented Security and Trust **(HOST)**, May 2025, San Jose, CA.
   (Acceptance rate (31.57%): 42 out of 133 submissions)
4. **Muhammad Ahsan**, Barry Najarro-Blancas, Johanna Tsala Ebode, Nastassja Lewinski, Irfan Ahmed, "3D Bioprinter Firmware Attacks: Categorization, Implementation, and Impacts", In the 18^{th} IEEE International Symposium on Hardware Oriented Security and Trust **(HOST)**, May 2025, San Jose, CA.
   (Acceptance rate (31.57%): 42 out of 133 submissions)
   (Semi-Finalists for the Best Paper Award - among the top 6 papers)
5. Muhammad Haris Rais, **Muhammad Ahsan**, Irfan Ahmed, "SOK: 3D Printer Firmware Attacks on Fused Filament Fabrication." In the 18^{th} USENIX WOOT Conference on Offensive Technologies **(WOOT)**, August 2024, Philadelphia, PA.
   (Acceptance rate (35%): 18 out of 51 submissions)
6. **Muhammad Ahsan**, Muhammad Haris Rais, and Irfan Ahmed, "SOK: Side Channel Monitoring for Additive Manufacturing-Bridging Cybersecurity and Quality Assurance Communities." In the 8^{th} IEEE European Symposium on Security and Privacy **(EuroS&P)**, July 2023, Netherlands.
   (Acceptance rate (35%): 63 out of 180 submissions)
   *(Included in the VA Commonwealth Cyber Initiative's **2024 CCI Research Showcase**, a curated collection of significant, influential peer-reviewed research papers published in the last two years.)*
7. Muhammad Haris Rais, **Muhammad Ahsan**, Irfan Ahmed, "Sabotaging Material Extrusion-Based 3D Printed Parts through Low-Magnitude Kinetic Manipulation Attacks." In ACM Transactions on Cyber-Physical Systems **(TCPS)**, Vol. 9, No. 1, pp. 1-26, January 2025.
   (Q1 Journal with an impact factor of 2.3 in 2023)
8. Bilal Imran, **Muhammad Ahsan**, Ali Hammad Akbar, and Ghalib Asadullah Shah. "D4gw: Dtls for Gateway Multiplexed Application to Secure MQTT (SN)-Based Pub/Sub Architecture.", In Elsevier **Internet of Things Journal**. 2024.
   (Q1 Journal with an impact factor of 7.6 in 2024)
9. Muhammad Haris Rais, **Muhammad Ahsan**, and Irfan Ahmed. "FRoMEPP: Digital Forensic Readiness Framework for Material Extrusion based 3D Printing Process", In 10^{th} Annual Digital Forensics Research Conference Europe (DFRWS EU'23), March 2023, Bonn, Germany
   - Published by Forensic Science International (FSI): Digital Investigation Journal, Elsevier.
   (Acceptance rate (23%): 16 out of 70 submissions)
10. **Muhammad Ahsan**, and Muhammad Ali. "LsStk: Lightweight solution to preventing Stack from buffer overflow vulnerability", 2023 IEEE 17th International Conference on Open Source Systems and Technologies **(ICOSST)**, 2023.
11. Muhammad Rais, **Muhammad Ahsan**, Vaibhav Sharma, Radhika Barua, Robert Prins, and Irfan Ahmed, "Low-Magnitude Infill Structure Manipulation Attacks on Fused Filament Fabrication Printers", In the 16^{th} IFIP International Conference on Critical Infrastructure Protection **(ICCIP)**, March 2022, Arlington, Virginia.
12. **Muhammad Ahsan**, Bilal Afzal, Bilal Imran, Asim Tanwir, Ali Hammad Akbar, and Galib. A. Shah. "OneM2M Architecture Based Secure MQTT Binding in Mbed OS", IEEE **Euro S&P** Workshop on Software Security for Internet of Things. 2019.
13. Bilal Imran, Bilal Afzal, Dr. Ali Hammad Akbar, **Muhammad Ahsan**, Dr. Ghalib A. Shah. "MISA: Minimalist Implementation of oneM2M Security Architecture for Constrained IoT Devices", IEEE **Globecom** 2019.
    (Acceptance rate (40%): 69 out of 172 submissions)
14. **Muhammad Ahsan**, Naseer Ahmad, Waqas Badar. "Simulation of Solar angles for maximizing Efficiency of Solar Thermal Collectors", 3rd Inter. Conference on Energy Conservation and Efficiency **(ICECE)**, 2019.