Muhammad Tehmasib Ali Tashfeen

PhD Candidate
Research: AI for Software & Mobile Security
Citizenship: Pakistan | F-1 visa (STEM field; eligible for OPT and STEM-OPT extension)
mxalitashfeen@shockers.wichita.edu LinkedIn GitHub Google Scholar
ORCID: 0009-0007-3209-5760 muhammadtehamsibalitashfeen.github.io

Education

Wichita State University Aug 2023 – May 2027 (expected)
PhD in Electrical Engineering & Computer Science (GPA: 3.70 / 4.00) *Wichita, Kansas*

- **Dissertation (in progress):** "LLM-Assisted Static Analysis for Android Application Leak Detection."
- **Advisor:** Dr. Zhiyong Shan, Software Analysis and Intelligence Laboratory (NSF-supported).
- **Research focus:** AI for software/mobile security, static program analysis, LLM-assisted vulnerability detection, side-channel attacks in SDNs.

National University of Computer and Emerging Sciences (FAST-NUCES) Aug 2015 – Jul 2019
Bachelor of Science in Electrical Engineering (CGPA: 3.41 / 4.00) *Islamabad, Pakistan*

- **Senior Design Project:** "IoT-Based Smart Metering System" – designed and implemented an Internet-of-Things platform for remote utility consumption monitoring and reporting.
- **Dean's List** – 3 semesters (Fall 2016, Fall 2017, Fall 2018) for academic excellence.

Research Interests

- **Software & Mobile Security:** static program analysis, vulnerability detection, Android security, memory-leak analysis
- **AI for Software Engineering:** large language models for bug detection, data-driven program analysis, dataset engineering for security
- **Network Security:** Software-Defined Networks (SDNs), side-channel attacks, secure system design
- **Trustworthy ML:** robustness, evaluation, and explainability of ML models for security-critical applications

Research Experience

Wichita State University – Software Analysis & Intelligence Laboratory (NSF-supported) Aug 2023 – Present
Graduate Research Assistant (Doctoral Researcher) – Advisor: Dr. Zhiyong Shan *Wichita, KS*

- Conduct doctoral research at the intersection of **Artificial Intelligence** and **Mobile/Software Security**, developing static-analysis and data-driven methods for Android application security as part of an NSF-supported research group.
- Designed and led the construction of a **large-scale, manually validated dataset of memory leaks** in Android Java applications, sourcing and compiling 650+ open-source GitHub projects to enable reproducible, data-driven security research.
- Developed automated compilation pipelines and conducted rigorous **manual ground-truth verification**, producing a high-fidelity benchmark suitable for training and evaluating AI-based bug detection models.
- Built deep static-analysis tooling on the **Soot framework** to detect bug patterns and security violations in Android Java applications, with measurable improvements over prior baselines.
- Pioneered the use of **Large Language Models (LLMs)** for software bug detection and categorization, integrating LLM-based reasoning with classical program analysis.
- Leveraged the **NSF Expanse high-performance computing cluster** for large-scale model training and evaluation.
- Mentor junior graduate and undergraduate researchers; collaborate on paper writing, experimental design, and reproducibility practices.

Industry Experience

Ernst and Young Ford Rhodes Mar 2023 – Jun 2023
Senior Consultant, Technology Risk *Islamabad, Pakistan*

- Led a cybersecurity audit for Pakistan Telecommunication Company Ltd (PTCL) and Ufone, assessing data centers, network security, and Security Operations Centers (SOC) to identify vulnerabilities and compliance gaps.
- Evaluated security controls, incident-response mechanisms, and risk-management practices against industry standards and best practices.

The Bank of Punjab Nov 2020 – Mar 2023
Information Systems Auditor *Lahore, Pakistan*

- Conducted security audits across critical banking systems, evaluating 100+ applications to identify vulnerabilities and ensure regulatory compliance.
- Authored quarterly Information Security Assurance reports for the Board of Governors; translated penetration-test and vulnerability findings into executive risk heat maps with remediation timelines.

Iron Bridge Systems Jan 2020 – Nov 2020
Executive Engineer *Lahore, Pakistan*

- Implemented network and infrastructure security solutions (Firewalls, SIEM, WAF, endpoint protection), reducing security incidents by 90% at client premises.

Publications

Google Scholar metrics (April 2026): 28 citations, h-index: 3, i10-index: 1.

Profile: scholar.google.com/citations?user=hlxSvmsAAAAJ

Peer-Reviewed Journal Articles

1. M. Y. Ayub, U. Haider, A. Haider, **M. T. A. Tashfeen**, H. Shoukat, A. Basit. "An Intelligent Machine Learning Based Intrusion Detection System (IDS) for Smart Cities Networks." *EAI Endorsed Transactions on Smart Cities*, vol. 7, no. 1, e4, 2023. *[13 citations]*

Peer-Reviewed Book Chapters and Conference Papers

1. **M. T. A. Tashfeen**. "Intrusion Detection System using AI and Machine Learning Algorithm." In *Cyber Security for Next-Generation Computing Technologies*, pp. 120–140, 2024. *[6 citations]*
2. U. Haider, H. Shoukat, M. Y. Ayub, **M. T. A. Tashfeen**, T. K. Bhatia, I. U. Khan. "Cyber Attack Detection Analysis using Machine Learning for IoT-based UAV Network." In *Cyber Security for Next-Generation Computing Technologies*, pp. 253–264, 2024. *[7 citations]*
3. **M. T. A. Tashfeen**. "Building Blocks of Incident Response: Security Operation Centers." *International Conference on Advances in Communication Technology, Computing and Engineering (ICACTCE)*, 2023. *[2 citations]*
4. **M. T. A. Tashfeen**, M. Y. Ayub, U. Haider, T. K. Bhatia, S. G. Tawaseem. "Intrusion Detection System for IoT Infrastructure." *Proceedings of the 1st International Conference on Trends and Innovations in Smart Technologies (ICTIST'22)*, London, UK, October 7–8, 2022.

Under Review

1. **M. T. A. Tashfeen**, Z. Shan. "Side-Channel Attacks in Software-Defined Networks: A Comprehensive Survey." *ACM Computing Surveys* (under review).

Conference Presentations and Talks

1. **"Software-Based Side-Channel Attacks in SDNs"** (Oct 2024) – Oral presentation, Technical Session #1, 17th Central Area Networking and Security Workshop (CANSec 2024), University of Oklahoma, Norman, OK. *Authors:* **M. T. A. Tashfeen**, Z. Shan (advisor). 15-minute talk with 5-minute Q&A on software-based side-channel attack vectors against software-defined networking control and data planes.
2. **"Software-Based Side-Channel Attacks"** (Nov 2023) – Poster presentation, College of Engineering Research Day, Wichita State University, John Bardo Center, Wichita, KS. *Authors:* **M. T. A. Tashfeen**, Z. Shan (advisor).
3. **"Three Minute Thesis (3MT) Competition"** (Spring 2026) – Graduate School, Wichita State University.

Teaching Experience

Wichita State University, School of Computing Jan 2026 – May 2026
Graduate Teaching Assistant – Advanced Algorithm Analysis (Graduate) *Wichita, KS*

- Support graduate-level instruction in advanced algorithm design and analysis: asymptotic analysis, divide-and-conquer, dynamic programming, graph algorithms, NP-completeness, and approximation/randomized algorithms.
- Hold office hours, lead recitations and problem-solving sessions, and provide individualized feedback on proofs, algorithm correctness, and complexity analysis.
- Develop and grade homework, programming assignments, and exams; mentor students on research-style algorithmic problems.

Wichita State University, School of Computing Jan 2026 – May 2026
Graduate Teaching Assistant – Introduction to Programming *Wichita, KS*

- Mentor undergraduate students in foundational programming concepts including control flow, data structures, recursion, object-oriented design, and debugging.
- Conduct weekly lab sessions, deliver targeted code reviews, and provide structured feedback to support students from diverse academic backgrounds.
- Collaborate with course instructor on assessment design, rubric calibration, and accessibility of course materials.

Honors and Awards

Young Researcher Award – 3rd International Conference on Emerging Trends & Innovation (ICETI 2025) Oct 2025

- Awarded in recognition of exceptional dedication and promise in research; presented for outstanding early-career achievements and potential as a future leader in academia. Proceedings published by *Springer* in the *Information Systems Engineering and Management* series (vol. 86).

Research Excellence Award – 3rd International Conference on Emerging Trends & Innovation (ICETI 2025) Oct 2025

- Recognized for high quality, originality, and impactful contribution to the field of Computing, Artificial Intelligence, and Emerging Technologies. Proceedings published by *Springer* in the *Information Systems Engineering and Management* series (vol. 86).

Professional Service

Journal Reviewing Activities

- **Reviewer**, *Iraqi Journal of Information and Communication Technology (IJICT)*, 2026. Manuscript reviewed (double-anonymous): "mTON-IoT: A Modified Dataset Engineering for Multifactor Authentication with Comparative Study Based RL and ML."

Conference Service

- Participant and contributor, 3rd International Conference on Emerging Trends & Innovation (ICETI 2025).

Memberships in Professional Societies

- Member, Institute of Electrical and Electronics Engineers (IEEE)

Technical Skills

- **Program Analysis:** Soot framework (static analysis, IR transformation, call-graph construction), bytecode-level instrumentation, memory-leak and bug-pattern detection
- **Mobile / Android Security:** Android internals (Dalvik bytecode, manifest & permission model), APK analysis, large-scale OSS Android dataset construction and validation
- **Network & Systems Security:** Software-Defined Networks (SDNs), side-channel attacks and mitigations, security control assessment, firewalls / SIEM / WAF (operational exposure from prior industry roles)
- **Machine Learning:** supervised classification (logistic regression, random forest, XGBoost), evaluation and cross-validation, class-imbalance handling
- **Large Language Models:** LLM-assisted code/bug analysis, prompt engineering, Hugging Face Transformers and OpenAI API for research prototypes
- **Programming:** Python (research, scripting, ML), Java (Android, Soot), Bash; reading-level: C/C++, SQL
- **Research Computing:** NSF ACCESS / Expanse HPC cluster (Slurm, GPU jobs), Linux, Git/GitHub, LaTeX, reproducible experiment workflows

Certifications

EC Council: Certified Ethical Hacker (CEHv11) | *ECC9765324108*
(ISC)² Certified in Cybersecurity | *914385*