Mohammad Shahedur Rahman

Ph.D. Candidate in Computer Science and Engineering
University of Texas at Arlington, Arlington, Texas
Email: shahed.uta@gmail.com || Contact No: +1 (682) 320-1210
Personal Website || Google Scholar || GitHub || LinkedIn || Alphaxiv

RESEARCH PROFILE

Security and Trustworthiness of AI Systems. My research focuses on AI supply-chain security and model provenance, using graph-based methods, static analysis, and large-scale empirical evaluations to investigate vulnerability propagation across base models and their derivatives. I also examine security threats in autonomous and multi-agent AI systems, including prompt injection, cross-agent spillover, and trust-boundary violations. Complementary work explores trustworthy and resource-efficient edge AI. My long-term goal is to develop scalable, auditable, and secure AI systems throughout their development, adaptation, and deployment.

RESEARCH AREAS

- **AI Supply-Chain Security and Provenance:** Model lineage and dependency analysis, provenance inference and verification, graph-based security analysis, and vulnerability propagation across base models and their derivatives.
- **Agentic and Multi-Agent AI Security:** Prompt injection, adversarial testing, cross-agent vulnerability propagation, trust-boundary violations, and security of autonomous LLM-based agents.
- **Trustworthy and Resource-Efficient Edge AI:** Semantic-guided data augmentation, robust low-resolution visual recognition, adaptive machine learning, and resource-constrained AI deployment.

EDUCATION

Ph.D. in Computer Science Fall 2023 – Present
University of Texas at Arlington (UTA), Arlington, TX, USA
Advisor: Dr. Mohammad Atiqul Islam
Comprehensive milestone completed.

M.Sc. in Information Systems Security Feb 2018
Bangladesh University of Professionals (BUP), Bangladesh
CGPA: 4.00/4.00 — Chancellor's Gold Medal

M.B.A. in Management Information Systems Dec 2016
University of Dhaka (DU), Bangladesh

B.Sc. in Computer Science and Engineering Feb 2011
Bangladesh University of Engineering and Technology (BUET), Bangladesh

ACADEMIC APPOINTMENTS

Graduate Research Assistant Fall 2023 – Present
University of Texas at Arlington (UTA), Arlington, TX, USA
Department of Computer Science and Engineering

Graduate Teaching Assistant 2023 – Present
University of Texas at Arlington (UTA), Arlington, TX, USA
Department of Computer Science and Engineering

PEER-REVIEWED PUBLICATIONS

Refereed Conference Papers

[1] **Mohammad Shahedur Rahman**, Mohammad Tahmid Bari, Md. Nasim Adnan, Arshad Parvez, and Sujit Maharjan. "AgentFuzz: Trace-Level Fuzzing for Prompt Spillover in LLM Multi-Agent Systems." *IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2026.

[2] **Mohammad Shahedur Rahman**, Sujit Maharjan, Roya Choupani, Mohammad Tahmid Bari, Erdogan Dogdu, and Md Delwar Hossain. "DiscoAct: Securing Autonomous Multimodal LLM Agents Against Cross-Modal Trust Flattening." *IEEE International Conference on Tools with Artificial Intelligence (ICTAI)*, 2026. **(Accepted, to appear)**

[3] **Mohammad Shahedur Rahman**, Mohammad Tahmid Bari, Md. Nasim Adnan, and Arshad Parvez. "LiteAugNet: A Lightweight Semantic-Guided Augmentation Network for Efficient Edge-Level Image Classification." *International Conference on Pattern Recognition (ICPR)*, Springer LNCS, vol. 16816, pp. 159–174, 2026. [DOI]

[4] **Mohammad Shahedur Rahman**, M Tahmid Bari, Md. Delwar Hossain, Roya Choupani, and Erdogan Dogdu. "SEGA-Net: LLM-Guided Semantic-Enhanced GAN Augmentation Network for Low-Resolution Image Classification." *IEEE International Conference on AI x Data and Knowledge Engineering (AIxDKE)*, pp. 135–142, 2026. [DOI]

[5] Emmanuel Oseghale, **Mohammad Shahedur Rahman**, Ashwani Manoj Kumar Rai, Xing Gao, and Yuede Ji. "Beyond CVSS: Context-Aware Exploitability Assessment of Vulnerabilities in HPC Containers." *IEEE Cloud Summit*, pp. 204–209, 2026. [DOI]

[6] **Mohammad Shahedur Rahman**, Peng Gao, and Yuede Ji. "HuggingGraph: Understanding the Supply Chain of LLM Ecosystem." *Proceedings of the 34th ACM International Conference on Information and Knowledge Management (CIKM)*, pp. 5997–6005, 2025. [DOI]

MANUSCRIPTS AND ONGOING RESEARCH

Manuscripts Under Review

- **ProvCode: Static Auditing of Provenance Carryover for Hugging Face Models.** Submitted to the IEEE/ACM International Conference on Software Engineering (ICSE 2027). *(Under Review)*
- **ChainInfer: Graph-Based Model Provenance Inference.** Inference of missing model lineage relationships using graph topology, repository metadata, and learned representations. Submitted to The Web Conference (WWW). *(Under Review)*
- **SEGA-COM: Semantic-Reliability-Aware Generative Communication and Energy Allocation.** Submitted to the IEEE International Conference on Communications (ICC 2027). *(Under Review)*

Research in Progress

- **VulChain: AI Supply-Chain Vulnerability Propagation.** Empirical investigation of package hallucination and insecure URL generation across base models and their fine-tuned, adapter-based, and quantized derivatives. *(Manuscript Revision in Progress)*
- **ChronoResolve: Retrospective Artifact Resolution for Model Lineage.** Identification of historical upstream model artifacts using file, configuration, weight, and temporal evidence to support reproducible provenance and security auditing. *(Research in Progress)*
- **LiteAdapt: Adaptive Semantic Augmentation for Resource-Constrained Edge Environments.** Resource-adaptive semantic augmentation with reliability-aware sample selection and dynamic budget allocation for edge-based visual recognition. *(Journal Manuscript in Preparation)*

SELECTED RESEARCH PROGRAM AND CONTRIBUTIONS

I. AI Supply-Chain Security, Provenance, and Vulnerability Propagation

- **HuggingGraph – Large-Scale AI Supply-Chain Characterization.** Developed a heterogeneous graph of the Hugging Face LLM ecosystem comprising 402,654 entities and 462,524 relationships, capturing model derivation, fine-tuning, adapters, quantization, merging, and dataset dependencies. Analyzed ecosystem structure, connectivity, and provenance gaps to support graph-based AI supply-chain analysis. *(ACM CIKM 2025)*
- **Large-Scale Model Lineage Analysis.** Extended AI supply-chain data collection and dependency extraction to approximately three million Hugging Face model records, investigating missing, incomplete, and nonstandard lineage declarations across the broader ecosystem. *(Ongoing Research)*
- **ProvCode – Static Provenance Auditing.** Developed static analysis methods to examine whether model repositories and associated source code preserve upstream provenance claims. Investigated inconsistencies between declared and code-derived lineage across a corpus of approximately 75,000 Hugging Face models. *(Under Review, ICSE 2027)*
- **ChainInfer – Graph-Based Model Provenance Inference.** Investigated missing model-to-model lineage relationships using graph topology, repository metadata, and learned representations to recover potential upstream dependencies. *(Under Review, WWW)*

- **VulChain – Vulnerability Propagation Across LLM Derivatives.** Designed controlled empirical evaluations to investigate whether unsafe behaviors, including package hallucination and insecure URL generation, persist through fine-tuning, adapter-based adaptation, and quantization. Evaluated vulnerability persistence using matched prompts and validated detectors. *(Research in Progress)*
- **ChronoResolve – Artifact-Level Provenance Resolution.** Investigating retrospective identification of historical upstream model artifacts using file hashes, configurations, weight signatures, and temporal evidence to reduce lineage ambiguity and support reproducible security auditing. *(Research in Progress)*

II. Agentic and Multi-Agent AI Security

- **AgentFuzz – Security of LLM Multi-Agent Systems.** Developed a trace-level fuzzing framework to investigate adversarial prompt spillover across interacting LLM agents. Evaluated attack propagation across communication topologies, injection channels, and verification configurations to characterize security failures in multi-agent workflows. *(IEEE ICMLA 2026)*
- **DiscoAct – Security of Autonomous Multimodal LLM Agents.** Developed a model-agnostic runtime verification framework combining symbolic policy validation, cross-modal consistency checking, and knowledge–environment alignment. Evaluated the framework across 240 adversarial scenarios and three LLM backbones, achieving a 94.2% unsafe-action prevention rate. *(IEEE ICTAI 2026, Accepted)*

III. Trustworthy and Resource-Efficient Edge AI

- **LiteAugNet – Lightweight Semantic-Guided Image Augmentation.** Developed a lightweight semantic-guided augmentation approach to improve low-resolution image classification while addressing computational constraints in edge environments. *(ICPR 2026)*
- **SEGA-NET – LLM-Guided Semantic Image Augmentation.** Investigated LLM-guided semantic augmentation and generative image synthesis for improving low-resolution visual recognition. *(IEEE AIxDKE 2026)*
- **LiteAdapt – Resource-Adaptive Semantic Augmentation.** Extending semantic-guided augmentation through reliability-aware sample weighting, adaptive verification, and dynamic resource allocation for constrained edge environments. *(Journal Manuscript in Preparation)*

TEACHING EXPERIENCE AND READINESS

Graduate Teaching Assistant 2023 – Present
Department of Computer Science and Engineering, University of Texas at Arlington

Courses Supported

Supported laboratory instruction, technical coursework, student consultations, and course assessments across undergraduate and graduate Computer Science courses.

- **CSE 6392 – Special Topics in AI Supply Chain (Graduate):** AI supply-chain security, model dependencies, and provenance analysis.
- **CSE 4380 / CSE 5380 – Information Security (Undergraduate and Graduate):** Teaching assistant across three separate semesters; laboratory instruction and course assessments.
- **CSE 5307 – Programming Language Concepts (Graduate):** Programming language concepts, technical coursework, and student support.
- **CSE 2312 – Computer Organization and Assembly Language Programming (Undergraduate):** Computer architecture and low-level programming.
- **CSE 1310 – Introduction to Computer & Programming in C (Undergraduate):** C programming, debugging, and problem-solving exercises.
- **CSE 1106 – Introduction to Computer Science & Engineering (Undergraduate):** Computational thinking and foundational computer science concepts.

Courses Prepared to Teach

- **Cybersecurity and Information Assurance:** Information Security, Computer and Network Security, Software Security, Cybersecurity Risk Management, and AI Supply-Chain Security.
- **Artificial Intelligence and Machine Learning:** Introduction to Artificial Intelligence, Machine Learning, AI Security, Neural Networks, Large Language Models, and Agentic AI Security.
- **Programming Languages and Computer Systems:** Programming Language Concepts, and Computer Networks.

- **Foundational Computer Science:** Introduction to Computer Science, Programming Fundamentals (C, Python), and Data Structures and Algorithms.

STUDENT MENTORING AND EDUCATIONAL ENGAGEMENT

- **Academic Mentoring and Student Support:** Provided laboratory-based mentoring and individualized academic support for undergraduate computer science students at the University of Texas at Arlington, including technical guidance, problem-solving assistance, programming support, and assessment preparation.
- **Cybersecurity Training and Professional Mentorship:** Delivered cybersecurity training, technical mentoring, and knowledge-sharing activities across financial services and national cybersecurity initiatives, translating industry security practices into practical technical guidance for multidisciplinary teams.

SCHOLARLY SERVICE AND RESEARCH COMMUNITY

- **Journal Peer Reviewer:** IEEE Open Journal of the Communications Society (OJ-COMS), 2026.
- **Conference Peer Reviewer:**
  - IEEE International Conference on Machine Learning and Applications (ICMLA), 2026.
  - IEEE International Conference on Tools with Artificial Intelligence (ICTAI), 2026.
  - International Conference on Pattern Recognition (ICPR), 2026.
  - IEEE International Conference on AI x Data and Knowledge Engineering (AIxDKE), 2026.
- **Open Research Contributions:** Contributed publicly available research artifacts, graph datasets, and companion documentation supporting the reproducibility of *HuggingGraph* (ACM CIKM 2025).

PRESENTATIONS AND SCHOLARLY DISSEMINATION

- **AgentFuzz: Trace-Level Fuzzing for Prompt Spillover in LLM Multi-Agent Systems.** IEEE International Conference on Machine Learning and Applications (ICMLA), 2026. *Conference Presentation.*
- **DiscoAct: Securing Autonomous Multimodal LLM Agents Against Cross-Modal Trust Flattening.** IEEE International Conference on Tools with Artificial Intelligence (ICTAI), 2026. *Conference Presentation.*
- **LiteAugNet: A Lightweight Semantic-Guided Augmentation Network for Efficient Edge-Level Image Classification.** International Conference on Pattern Recognition (ICPR), 2026. *Conference Presentation.*
- **SEGA-Net: LLM-Guided Semantic-Enhanced GAN Augmentation Network for Low-Resolution Image Classification.** International Conference on AI x Data and Knowledge Engineering (AIxDKE), 2026. *Conference Presentation.*
- **HuggingGraph: Understanding the Supply Chain of LLM Ecosystem.** ACM International Conference on Information and Knowledge Management (CIKM), 2025. *Conference Presentation.*

RESEARCH ARTIFACTS AND REPRODUCIBILITY

- **HuggingGraph – Open Research Artifacts:** Publicly available model and dataset dependency graph artifacts, documentation, and companion research repository supporting the ACM CIKM 2025 publication. [GitHub Repository]
- **AI Security Research Infrastructure:** Developed experimental pipelines for LLM derivative vulnerability evaluation, static model provenance analysis, prompt-level vulnerability detection, multi-agent trace analysis, and large-scale graph processing. Code-release status varies across projects.

HONORS, AWARDS, AND ACADEMIC SUPPORT

- **Teaching Assistant of the Month** Feb 2025
  University of Texas at Arlington. Recognized for teaching excellence among 175 teaching assistants in Computer Science and Engineering.
- **Chancellor's Gold Medal** 2020
  Bangladesh University of Professionals. Awarded for outstanding master's-level academic performance; conferred by the President of Bangladesh.
- **Academic Gold Medals** 2007
  Janata Bank, Bangladesh. Awarded for exceptional academic performance in higher secondary education.
- **STEM Scholarship and Graduate Assistantship** 2023 – Present
  University of Texas at Arlington. Full tuition support and graduate assistantship funding for doctoral studies.

INDUSTRY LEADERSHIP AND APPLIED CYBERSECURITY EXPERIENCE

Summer Security Audit Intern May 2025 – Jul 2025
Federal Home Loan Bank of Dallas, TX, USA

- Supported IT and compliance audits covering SOX, business continuity, disaster recovery, record retention, and FHFA requirements; prepared audit workpapers.

Chief Information Security Officer (CISO) Nov 2022 – Aug 2023
BRAC Bank PLC, Bangladesh

- Led a 30-member cybersecurity team supporting 187 branches and 1,041 agent-banking outlets; presented enterprise cyber risks to senior leadership and the board.
- Directed security strategy, incident response, third-party risk, and security operations, including SIEM/SOAR, EDR/XDR, and DLP technologies.

National IT Security Consultant Jan 2019 – Sep 2022
e-GOV CIRT (World Bank-Funded), Bangladesh

- Contributed to national cybersecurity strategy, IT audit and cloud-computing frameworks; coordinated security assessments of critical government infrastructure.
- Collaborated with government, financial, and technical stakeholders on cybersecurity risk assessments and incident preparedness.

Assistant Vice President, IT Security Nov 2016 – Dec 2018
Eastern Bank PLC, Bangladesh

- Led enterprise threat detection, incident response, security automation, and regulatory compliance initiatives.

Assistant Manager, Cybersecurity Feb 2015 – Nov 2016
KPMG, Bangladesh

- Led financial sector's security audits and risk assessments; advised on ISO, COBIT, and ITIL-aligned security controls.

Senior Programmer, ERP Security Jan 2014 – Jan 2015
IBCS-PRIMAX Software (Bangladesh) Ltd.

- Supported secure ERP implementations, access controls, data protection, system patching, and security auditing.

IT Specialist, Security Oct 2012 – Dec 2013
IBM, Bangladesh

- Performed security monitoring, VAPT, access management, and infrastructure security operations.

SELECTED PROFESSIONAL CERTIFICATIONS

- **Cybersecurity and Governance:** Certified Information Systems Auditor (CISA); Certified in Risk and Information Systems Control (CRISC); Certified Ethical Hacker (CEH); ISC2 Certified in Cybersecurity (CC); ISO/IEC 27001 Lead Auditor and Lead Implementer; ISO/IEC 27701 Lead Implementer; PCI-DSS Implementation; ISO 27032.
- **Leadership and Management:** Project Management Professional (PMP); PRINCE2 Practitioner; Six Sigma Black Belt; ITIL Foundation.

TECHNICAL AND RESEARCH EXPERTISE

- **Research Methods:** AI-model provenance and metadata analysis, large-scale graph analytics, static analysis, LLM security evaluation, and agent trace analysis.
- **Programming and AI Tools:** Python, Bash, SQL, C; PyTorch, TensorFlow, Hugging Face, scikit-learn, NumPy, Pandas, NetworkX, Jupyter.
- **Systems and Cybersecurity:** Linux, Docker, Kubernetes, AWS, GCP, Azure; container/HPC security, vulnerability assessment, SIEM/SOAR, and enterprise security auditing.

PROFESSIONAL MEMBERSHIPS

Information Systems Audit and Control Association (ISACA); Project Management Institute (PMI); Institution of Engineers, Bangladesh (IEB); Bangladesh Computer Society.