

Summary. Ph.D. student building LLM-based systems for access control policy synthesis and studying online scams and privacy risks at scale, with experience in LLM pipelines, data analysis, and user studies.

EDUCATION

University of Massachusetts Amherst, MS/Ph.D., Computer Science (Advisor: Dr. Pubali Datta)Sep 2025 – Sep 2031 (Exp.)

BUET, BSc, Computer Science & Engineering (Thesis advisor: Dr. Anindya Iqbal)2019 – 2024

PUBLICATIONS

1. *Quantifying Risk Perception and Scam Response Among International and Domestic U.S. University Students.* A. X. Li, E. Bouma-Sims, L. Klucinec, R. Liu, **Ayesha Binte Mostofa**, A. Arunasalam, L. F. Cranor, P. Datta, L. Simko, K. Sowon. **SOUPS 2026**.
2. *Reparo: Synthesizing and Validating Access Control Policies.* **Ayesha Binte Mostofa**, G. Zhang, S. Stern, J. Zhai, P. Datta. Under review at a top-tier conference.
3. *Characterizing Scam Experiences, Harms, and Responses Among U.S. College Students.* **Ayesha Binte Mostofa**, K. Fatima, A. A. Kamath, A. Arunasalam, P. Datta. Under review at a top-tier conference.
4. *Understanding Synthetic Politics on Reddit: Spread and Community Reactions to Political Deepfakes.* **Ayesha Binte Mostofa** and P. Datta. **USENIX Security '26** (Poster).
5. *Advancing Code Review and Code Refinement Automation Using LLMs.* **Ayesha Binte Mostofa***, S. S. B. Mosaddek*, A. Haider*, T. Ahmed, A. Iqbal. [Preprint](#), 2024. (*Equal contribution)

RESEARCH EXPERIENCE

Research Assistant, Security Research Group, UMass AmherstFall 2025 – Present

• **Access control (first author):** Built a multi-LLM framework that generates, validates, and repairs access control policies (Cedar, OpenFGA, Rego) from repository artifacts; evaluated on 228 real-world repositories.

• **Scams and online harms (first author):** Analyzed 26K+ posts across 83 college subreddits with LLM-based methods to characterize student scam experiences and responses; studied political deepfake spread on Reddit; designing a survey and interview study on scams targeting international workers in the U.S.

• **App privacy and agentic AI (first author):** Measuring privacy practices of 50+ student-used apps; exploring Cedar-based authorization for agentic AI systems.

Undergraduate Researcher, BUET2023 – 2025

• Improved code review comment and code refinement generation by combining static program metadata (call graphs) and natural-language summaries in prompts with QLoRA fine-tuning. (Advisors: Dr. A. Iqbal, Dr. T. Ahmed)

• Detected benign and malicious behaviors in DARPA OPTC and TC E3 logs using PostgreSQL and provenance graphs. (Advisors: Dr. S. Hossain, Dr. S. Iqbal)

TEACHING AND INDUSTRY EXPERIENCE

Teaching Assistant, UMass Amherst (COMPSCI 250, COMPSCI 220)Fall 2025 – Spring 2026

Lecturer, CSE, Presidency Univ. and Canadian Univ. of BangladeshJul 2024 – Jul 2025

Machine Learning Intern (part-time, remote), Red.Digital LimitedMay – Jun 2023

SELECTED PROJECTS

LLMComp: prompt compression as a defense against LLM jailbreaks (LLMs, few-shot)2025

IaC-Eval: replication and extension study of LLM-generated infrastructure-as-code (LLMs, CoT)2025

MISP Tool: cryptography and malware analysis tool (Python, Docker, Azure) [Code](#) | [Demo](#)2023

HONORS AND AWARDS

Stemple Scholarship in Computing, UMass Amherst (\$2,300); USENIX Security Travel Grant (\$825)2026

GREPSEC VII, 1 of 48 participants selected internationally (\$1,175 travel grant)2026

RISE-BUET Research Grant (thesis); Dean's List, BUET2023 – 2024

TALKS AND SERVICE

Talks and posters: Boston Security Usable Research Day (talk); GREPSEC VII; New England Security Day2026

External reviewer: IEEE Transactions on Dependable and Secure Computing2026

TECHNICAL SKILLS

Languages: Python, C/C++, Java, JavaScript, Bash, MySQL, LaTeXML: QLoRA, Keras, scikit-learn, Pandas

Tools and systems: Docker, PostgreSQL, Git, Linux, Node.js, React, Wireshark, Cedar, OpenFGA, Rego