Md **Raihan** Ahmed

Software Engineer · Security Researcher

Salt Lake City, Utah, USA

(+1) 385 622 2386 | u1374605@utah.edu | mdrahmed.github.io | mdrahmed | mdrahmed

"Let me help you make the change that you want to see in this world."

Education

University of Utah — *Utah, USA*

Ph.D. in Computer Science, **GPA: 3.86** — *Aug. 2021 - Aug. 2026 (Expected)*

University of Utah — *Utah, USA*

MS. in Computer Science, **GPA: 3.86** — *Aug. 2021 - May 2024*

Experience

Meta — *Menlo Park, California, USA*

Software Engineer Intern — *May 2025 - Aug. 2025*

- Identified limitations in manual asset classification processes for securing user data, highlighting significant false positives/negatives due to lack of automation.
- Identify a scalable solution **to improve speed and accuracy.**
- Developed and implemented **machine learning models to automate asset classification**. Then, compared candidate models, selected the best, and deployed it into production.
- **Significantly reduced the aggregation process timeline** from months to a fraction of the time.

University of Utah — *Utah, USA*

Research Assistant — *Aug. 2021 - Current*

- Advanced persistent threats (e.g., Stuxnet, Ukrainian power grid attack) exposed vulnerabilities in Industrial Control Systems (ICS).
- Built ICSTracker using C++ & LLVM **to instrument controllers, enabling full activity tracing.**
- **Simulated multiple cyberattacks following MITRE ATT&CK framework on testbeds** (Fischertechnik factory, SWaT water system) to validate robustness.
- **Traced attack origins in real-time with the tool successfully** , demonstrating ability to enhance ICS security and contributing to peerreviewed publication.

University of Utah — *Utah, USA*

Teaching Assistant

- Teaching Assistant for CS 4400-001 - Computer System in Fall-2022 & Fall-2024
- Teaching Assistant for CS 6956-001 - Software and System Security in Spring-2023

Projects

ICSTracker: To Trace back to the source of Intrusion in Industrial IoT Systems. — *C++, LLVM, Python*

PhD 1st Proj — *GitHub* — *Aug. 2021 - May 2024*

- Created an instrumentation tool with LLVM to trace back to the source of attack.
- Physical process-aware, cross-iteration and cross-domain approach to backtracking intrusions in ICS
- Crafted detailed instrumentation passes to capture critical runtime data from ICS controllers; improved data collection accuracy by 56%, to enable more effective troubleshooting for complex system failures.

Interactive Visualization tool — *Javascript*

Data Visualization Course — *GitHub* — *Aug. 2022 - Dec. 2022*

- Formulated project is to build an interactive tool for video games.
- Built website with javascript to explore video game sales by year and platform.

Fuzzing XPDF-4.05 — *LLVM, C++*

Applied S/W Security Test. Course — *Git1* *Git2* — *Aug. 2022 - Dec. 2022*

- Extended fuzzing campaign with static analysis (control flow + IR inspection) to guide fuzzing input generation.
- Applied program verification tools (Z3, CBMC) to validate discovered crash paths.
- Improved open-source robustness by contributing bug reports and patches.

Rollback attack in Cars

Arduino, C++

Cyber-phys Sys & IoT Security Course — *Github* *Aug. 2022 - Dec. 2022*

- Formulated project was to build a device to perform cyberattack on modern cars.
- Built a rollback device with Arduino to access cars without using keys.

Remote control robot built with Arduino

Arduino, C++

A personal cool project — *Demo* *May 2021*

- Used arduino uno to build this robot and controlling it with Bluetooth

Publications

IEEE/IFIP International Conference on Dependable Systems and Networks

Naples, Italy

ICSTRACKER: Backtracking Intrusions in Modern Industrial Control Systems **(1st Author)** — *paper* *Apr. 2025*

- Recovered program semantics, reconstructed data dependencies, and linked controller operations to OS- level events to show the cyber-physical attacks in ICS/CPS setting.

Re-design Industrial Control Systems with Security (RICSS)

Utah, USA

Context-Aware Intrusion Detection in Industrial Control Systems **(1st Author)** — *paper* *Oct. 2024*

- Developed a provenance-based method with Linear Temporal Logic (LTL) to enhance ICS attack detection in information security.

Biointerface Research in Applied Chemistry

Bangladesh

Ovarian Cancer Substantial Risk Factor Analysis by Machine Learning: a Low Incoming Country **(1st)** — *paper* *Jul. 2020*

- Analyzed ovarian cancer data using various machine learning algorithms to identify significant risk factors

BMC bioinformatics

Bangladesh

Machine learning to reveal an astute risk predictive framework for Gynecologic Cancer and its impact on women psychology: Bangladeshi perspective **(B.Sc Proj, 2nd Author)** — *GitHub* *paper* *Apr. 2021*

- Developed a predictive algorithm using machine learning to assess the risk of cervical and ovarian cancer associated with stress

Electrical, Computer and Communication Engineering (ECCE)

Bangladesh

A Comparative Analysis of Traditional and Modern Data Compression Schemes for Large MultiDimensional Extendible Array **(5th Author)** — *paper* *Feb. 2019*

- Compared traditional and modern data compression schemes for multi-dimensional data and concluding that the Extendible Array Based Compression Scheme (EaCRS) is most efficient

Elsevier

Bangladesh

A bioinformatics approach for identification of the core ontologies and signature genes of pulmonary disease and associated diseases **(2nd Author)** — *paper* *Jul. 2020*

- Spotted out significant common genes and proteins among COPD, DM, CR, IHD, IS, TB, and OB diseases, to suggest drug signatures.

Journal of Proteins and Proteomics

Bangladesh

Protein interaction network and drug design of stomach cancer and associated disease: a bioinformatics approach **(1st Author)** — *paper* *Dec. 2020*

- Identified common genes among seven diseases (OB, SC, CC, PC, PRC, LK, MD) to analyze their biological and genetic network.

Skills

Dev. & Deployment Tools	LLVM Compiler Tools, GitHub, Docker
Programming Lang.	Python, C/C++, Javascript, C#, JAVA, PHP
Frameworks	MITRE ATT&CK, Cyber Kill Chain, React.js, Node.js, Express.js, Android Studio, Dot(.) Net
Data Science & ML	Tensorflow, NumPy, scikit-learn, Pandas, Matplotlib
Database	Oracle SQL, MySQL
Security Tools	AFL++, Z3, CBMC, Snort, Suricata, OSS-Fuzz, Provenance Tracking
Data Analysis Software	Matlab, Google Colab, Jupyter, Anaconda
Cloud & Container Security	Docker, Kubernetes
Cyber Defense & Security Engineering	Threat Hunting, Threat Intelligence, Incident Response, Vulnerability Management, Threat Modeling
Interests	Security, Privacy, Machine learning, Artificial Intelligence