Md Athikul Islam

Graduate Research Assistant — Boise, ID, USA

Phone: (+1) 986-837-6172

Email: mdathikulislam@u.boisestate.edu

in LinkedIn: linkedin.com/in/mdathikulislam   ⭘ GitHub: github.com/atikbappy

G Google Scholar: scholar.google.com   🌐 Website: atikbappy.github.io/mdathikulislam

Summary

Ph.D. candidate with expertise in **Generative AI, LLMs, RAG**, and **Agentic AI**, focusing on enhancing the robustness and security of **NLP** systems. Developed adversarial attack/defense strategies, researched **LLMs**, and designed a **Linux kernel-swapping policy**. Improved language model robustness by **+41.6%** in accuracy under attack and led the technical development of a Dutch startup grow revenue from **$0 to $1M**. Proficient in **C, C++, Python, TensorFlow, PyTorch, and GCP**, with 7+ years of software engineering experience.

Education

Boise State University, Boise, ID, USA

Ph.D. in Computer Science, CGPA: 3.96   2021 – Present

Relevant Coursework: **ML, NLP, Data Science,** OS, Algorithms, SWE

Pabna University of Science and Technology, Pabna, Bangladesh

B.Sc. in Computer Science and Engineering, CGPA: 3.71   2008 – 2013

Professional Experience

Graduate Research Assistant

AI-Based Security Lab, Boise State University, Boise, ID, USA   Aug 2021 – Present

- Researching **adversarial attacks in NLP** and developing the GenFighter defense strategy, improving model robustness by +41.6% in accuracy under attack and reducing attack success rates by +37.0%.
- Developing **LLMs** and **Reinforcement Learning-based attack strategies** to generate realistic user comments that outperform state-of-the-art fake news detection evasion methods.
- Implemented **Linux kernel-swapping policy**, boosting system performance by 30% over traditional policies.
- Assisting in teaching Operating Systems and Algorithms, and mentoring undergraduate students.
  Technologies: C, C++, Python, PyTorch, TensorFlow, Pandas, LLMs, RAG, RL, GNNs, GMM, Clustering, Docker.

Senior Software Engineer

Impel IT Solutions, Dhaka, Bangladesh   Sep 2016 – Jul 2021

- Led the design and development of Eyevestor, a **GCP-based** share funding platform, helping grow revenue from **$0 to $1M** as a startup. Improved user engagement by 70% through responsive UI and scalable backend systems. Developed **atomic, async services** handling thousands of transactions per second with Firebase integration.
  Technologies: Python, Flask, TypeScript, Angular, GCP, NoSQL, REST APIs, CI/CD.

Software Engineer

Hard-Won International Technologies Bangladesh LTD., Dhaka, Bangladesh   Mar 2015 – Aug 2016

- Developed an **IoT-based** Android bus ticketing system that enhanced public transportation accessibility through **real-time transaction-based data**, providing a highly scalable solution for fare payment.
  Technologies: Python, Django, DRF, PostgreSQL, Android, REST APIs, SQLite.

Freelance Full Stack Developer

Upwork Global Inc. (Remote)   Apr 2013 – Feb 2015

- Worked on **AI-based chat systems, medical systems**, and numerous full-stack and backend development projects, achieving top-rated freelancer status with a 100% job success rate.
  Technologies: Python, Tensorflow, Celery, JavaScript, Django, Flask, MySQL, SQLite, Docker, HTML, CSS, Git.

Technical Skills

- **Core Competencies:** ML, NLP, Problem-Solving, Algorithms, CI/CD, OOP, REST APIs
- **Programming Languages:** Python, C++, C, JavaScript, Java, TypeScript, PHP
- **Frameworks/Libraries:** PyTorch, TensorFlow, PySpark, Django, Flask, Angular, Docker, Git
- **Databases:** PostgreSQL, MySQL, Google Datastore (NoSQL), SQLite
- **Machine Learning Techniques:** Adversarial Attacks, LLMs, RAG, Deep Learning, RL, Decision Trees, Reflection, Generative AI, Agentic AI, GNNs
- **Operating Systems:** Unix, Linux, Windows
- **Cloud Platforms:** AWS, GCP, Firebase, Heroku

Research Publications

- **GenFighter: A Generative and Evolutive Textual Attack Removal**
  MA Islam, E Serra, S Jajodia. Accepted for publication in ACM Transactions on Intelligent Systems and Technology
  https://doi.org/10.1145/3729240
- **Inconsistent Reasoning Attacks to Identify Weaknesses in Automatic Scientific Claim Verification Tools**
  MA Islam, N Ellison, B Lakha, E Serra. (Under Review)
- **Generating Realistic Adversarial User Comment Attacks to Evaluate the Robustness of Fake News Detectors**
  C Underwood, MA Islam, E Serra, F Spezzano. (Under Review)
- **Graph-LLM: Natural Language Explainer for Anomalous Cyber Events**
  B Lakha, MA Islam, E Serra. (In preparation)
- **Documentation Practices in Agile Software Development: A Systematic Literature Review**
  MA Islam, R Hasan, NU Eisty. Accepted at SERA 2023
  https://doi.org/10.1109/SERA57763.2023.10197828
- **Automatic Pull Request Description Generation Using LLMs: A T5 Model Approach**
  MN Sakib, MA Islam, MM Arifin. Accepted at AIBThings 2024
  https://doi.org/10.1109/AIBThings63359.2024.10863720

Selected Projects

- **GenFighter (Novel NLP Defense):** Developed a robust defense strategy for adversarial attacks, improving model accuracy by +41.6% and reducing attack success by +37.0%.
  GitHub: https://github.com/atikbappy/GenFighter
- **Linux Kernel Swapping Policy:** Designed an optimized kernel management strategy, improving system performance by 30%.
  GitHub: https://github.com/atikbappy/swapping-policy
- **Eyevestor:** Led the design and development of a share funding platform, improving user engagement by 70% with scalable backend services and Firebase integration.
- **PrismERP:** Built a comprehensive ERP system to streamline business processes and integrate key modules for efficient management.
- **FLEXANSWER Chatbot:** Created an NLP-based virtual assistant to improve customer support with efficient automated responses.

Additional Activities

- 1st Place – MBSTU Inter-University Programming Contest, 2013
- 5th Place – Jagannath University CSE Carnival Programming Contest, 2013
- Financial Officer, Bangladesh Student Association: Oversaw budgets and funding for student initiatives and events.