Sadif Ahmed

☎ (880)1521564856 ✉ ahmedsadif67@gmail.com ✉ sadif.ahmed@bracu.ac.bd in in/sadif-ahmed-092b60307

Sadif-Ahmed sadif-ahmed.github.io Dhaka, Bangladesh

About Me

I'm a passionate and versatile researcher with a keen interest in software engineering and LLMs. I enjoy the art of teaching.

Research Interests

Software Engineering and Security, Web UI Automation, AI for Software Engineering.

Education

Bangladesh University of Engineering & Technology Dhaka,Bangladesh
B.Sc. Computer Science, *CGPA: 3.83 out of 4 [Final Year: 3.96/4.00]* Feb 2020 - March 2025
Related Coursework: Structured Programming Language (C), Data Structures and Algorithms (C++), Object Oriented Programming (C++, Java), Software Engineering (Java), Information Systems Design, Database (SQL), Numerical Methods (Python), Computer Architecture, Machine Learning (Python)

Notre Dame College Dhaka,Bangladesh
Higher Secondary School Certificate, *GPA: 5 out of 5* Jan 2017 - Jan 2019

St. Joseph High School Dhaka,Bangladesh
Secondary School Certificate, *GPA: 5 out of 5* Jan 2009 - Dec 2016

Professional Experience

- Lecturer, CSE Department, BRAC University, Dhaka, Bangladesh July 2025 - Present
  Courses Taught:
  - Computer Architecture
  - Software Engineering
- Research Assistant, CSE Department, BUET, Dhaka, Bangladesh March 2025 - June 2025
  - Explored WebUI Gyms such as **WebArena** and worked on a UI Testing Automation Pipeline.
  - Worked on creating a end to end pipeline to generate **playwright** testing scripts from user stories of a website.

Research Experience

- **Secret Breach Detection in Source Code with Large Language Models**
  Undergraduate Thesis, **ESEM 2025 Technical Track Publication** October 2024 - July 2025
  - **Key Contribution**: We introduce a novel approach for Secret Breach Detection in source code using a Small Language Model (SLM) fine-tuned with QLoRA. Our model demonstrably outperforms several established state-of-the-art regex-based tools (like Trufflehog) and large, general-purpose LLMs (like GPT-4o) on the SecretBench dataset. We establish the efficacy of leveraging compact, specialized models over large, zero-shot models for this specific, critical software security task.
  - **Technology & Tools**: **QLoRA**, **DeepSeek-7B**, **Gemma-7B**, **LLaMA-3.1-8B**, **Mistral-7B**, **DeepSeek-V3**, **GPT-4o**
  - **Supervisor**: Dr. Rifat Shahriyar, Professor, CSE, BUET
- **Secret Leak Detection in Software Issue Reports using LLMs: A Comprehensive Evaluation**
  Undergraduate Thesis, Under Review in **MSR 2026**, ArXiv July 2024 - October 2025
  - **Key Contribution**: We present the first large-scale study and a robust hybrid detection pipeline for secret leaks in GitHub issue reports. Our pipeline integrates regex-based extraction with LLM contextual classification to effectively reduce false positives. We curated and released the first public benchmark dataset of over 54,000 labeled instances and demonstrated that fine-tuned LLMs achieve state-of-the-art performance (up to 0.945 F1), significantly outperforming traditional methods.
  - **Technology & Tools**: **Small Language Models such as RoBERTa-base, BERT-base-cased and BERT-base-uncased, CodeBERT-base etc**, **GPT-4o**, **Gemini-2.0-Flash**, **QLoRA**, **PEFT**, **DeepSeek-7B**, **Gemma-7B**, **LLaMA-3.1-8B**, **Mistral-7B**, **Qwen-7B**
  - **Supervisor**: Dr. Rifat Shahriyar, Professor, CSE, BUET; Dr. Gias Uddin, Associate Professor, York University

- **A Survey on Agentic Security: Applications, Threats and Defenses**

  Independent Research Group, Under Review in **ACL Rolling Review**, ArXiv August 2025 - October 2025

  - **Key Contribution**: We present the first holistic survey of the rapidly evolving agentic security landscape, systematically analyzing over 150 papers published primarily between 2024-2025. We structure the field around three interdependent pillars: Applications, Threats, and Defenses, providing a unified framework to understand the capabilities and vulnerabilities of Large Language Model (LLM) agents in cybersecurity.
  - **Supervisor**: Dr. Farig Sadeque, Associate Professor, BRAC University; Dr. Md Rizwan Parvez, Scientist, QCRI

- **BanglaForge: LLM Collaboration with Self-Refinement for Bangla Code Generation**

  Independent Research Group, Workshop co-located with IJCNLP-AACL 2025, Under Review in **AACL 2025**
  August 2025 - September 2025

  - **Key Contribution** : We introduce BanglaForge, a novel framework for generating executable code from Bangla descriptions, a low-resource language. We utilize a retrieval-augmented dual-model collaboration paradigm with iterative self-refinement based on execution feedback. This system, combining LLM-based translation and in-context learning, achieves a competitive Pass@1 accuracy of 84.00% on the BLP-2025 Bangla Code Generation benchmark, validating our approach for low-resource code generation.
  - **Technology & Tools**: **Dual-LLM architecture**, **Retrieval-Augmented few-shot prompting**, **TF-IDF**, **Iterative self-refinement**, **Execution feedback**, **Lg Exaone Deep 32B**, **Gemini-2.5-Pro**
  - **Collaborators** : Mahir Labib Dihan, Lecturer BRAC University; Md Nafiu Rahman, Lecturer BRAC University

Technical Skills

Languages:	C, C++, Java, JavaScript, TypeScript, Python, Latex
Frameworks:	NodeJS, ExpressJS, SvelteJS
Databases:	PostgreSQL, Oracle
Machine Learning & Data Analysis:	TensorFlow, PyTorch, Matplotlib, NumPy, Pandas
Development Tools:	Git, Github, Github Projects, Linux OS
Cloud Platforms:	Vercel, Supabase, Azure
Security Tools:	Velociraptor

Achievements

Top 20 finalists *of Robi Datathon 2024, A countrywide Deep Learning Competition*

Dean's list award and university merit scholarship *recipient in four terms of undergraduate study in BUET*

TalentPool Scholarship *for outstanding academic result in the Higher Secondary Certificate Exam in Dhaka, Bangladesh*

Academic Projects

- **Network Flow Classification and Anomaly Detection**
  Technology & Tools: *Python, Pytorch, Tensorflow* Mohaimin41/ml_project

  - Developed a **novel pipeline** using **BERT and GPT** for **binary and multi-label classification** of anomalous network traffic from pcap data.

- **Machine Learning Algorithms and Neural Network from Scratch**
  Technology & Tools: *Python, Numpy, Scikit-learn* Sadif-Ahmed/CSE-472

  - Implemented core ML algorithms: **logistic regression** (with bagging/stacking), **SVD** (for image reconstruction), **PCA**, and **GMM/EM** clustering.
  - Built a **feed-forward neural network** and the **Adam** optimizer from scratch using only `numpy`.

- **AuthentiDocs - Team Collaboration Authenticated By Digital Signature**
  Technology & Tools: *JS, TS, Svelte, PostgreSQL, Supabase* AuthentiDocs/authentidocs

  - Created a full-stack document management application integrating file flow, sharing, **digital signature** and verification. Focused on back-end development.

- **Cryptography, Malware Analysis, and Security Attacks**
  Technology & Tools: *Python, Docker, Wireshark, Azure* Sadif-Ahmed/CSE-406

  - Implemented **AES, Diffie-Hellman, and RSA** with socket communication. Demonstrated a **buffer-overflow attack** and pedagogical **malware functionalities** in `Docker`.

- **VLAN Configuration and Wireless Network Simulation**
  Technology & Tools: *Java, Cisco Packet Tracer, NS3* Sadif-Ahmed/CSE-322
  - Implemented **threaded server-client sockets**. Configured **NAT** and **ACLs** on **VLANs**. Simulated various wired and wireless mobile networks.

- **Operating System Internals with xv6**
  Technology & Tools: *Bash, C, Assembly* Sadif-Ahmed/CSE-314
  - Explored **bash scripting** and **synchronization** (pthreads). Implemented **system calls** and the **round robin scheduler** in the `xv6` operating system.

- **Anidex - Simple Online Anime Database**
  Technology & Tools: *JS, Svelte, ExpressJS, PostgreSQL* KyojinsAnidex/Anidex
  - Developed a full-stack anime database with features for listing, discovery, and **forum discussions**. Focused on front-end and full-stack integration.

- **Online Utility and Handyman Services**
  Technology & Tools: *JS, Svelte, ExpressJS, PostgreSQL* Siam11651/cse326-project
  - Full-stack development of a service application using **Svelte** and **PostgreSQL** following a modular design and web development best practices.

References

- Dr. Rifat Shahriyar — Professor, CSE, BUET
  ✉ rifat.shahriyar@gmail.com, rifat@cse.buet.ac.bd
- Dr. Md Rizwan Parvez — Scientist, QCRI
  ✉ rizwan@ucla.edu, rizwan.incipient@gmail.com
- Dr. Farig Sadeque — Associate Professor, BRAC University
  ✉ farig.sadeque@bracu.ac.bd