

Md Nafiu Rahman

📍 Dhaka, Bangladesh ✉ nafiur.rahman@gmail.com ☎ +88 01933-002218 🌐 nafiurahman00.github.io
in mdnafiurahman 🔄 nafiurahman00

About Me

I am a curious and driven computer science student and researcher with a keen interest in software engineering and LLMs. I enjoy the art of teaching.

Education

Bangladesh University of Engineering & Technology (BUET), Dhaka B.Sc. in Computer Science & Engineering CGPA: 3.81 / 4.00 (Final year: 3.94 / 4.00)	<i>Feb 2020 – Mar 2025</i>
◦ Relevant coursework: Data Structures & Algorithms, Object Oriented Programming, Software Engineering, Database Systems, Numerical Methods, Machine Learning.	
Notre Dame College, Dhaka Higher Secondary Certificate	<i>Jan 2017 – Jan 2019</i> GPA: 5.00 / 5.00
Bir Shrestha Noor Mohammad Public College, Dhaka Secondary School Certificate	<i>Jan 2009 – Dec 2016</i> GPA: 5.00 / 5.00

Professional Experience

Lecturer, Department of CSE, BRAC University, Dhaka	July 2025 – Present
◦ Teaching undergraduate courses including Numerical Methods and Software Engineering. I design course materials, assignments, and practical labs with an emphasis on clear, reproducible programming and sound engineering practices.	
Research Assistant, Department of CSE, BUET, Dhaka	Mar 2025 – June 2025
◦ Worked on a pipeline to generate Playwright testing scripts automatically from high-level website descriptions and web UI traces. Explored benchmarks and WebUI gyms, prototyped selector generation methods, and evaluated the reliability of generated tests focusing on practical integration with developer workflows.	

Research Experience

Secret Breach Detection in Source Code with Large Language Models.

Authors: Md Nafiu Rahman, Sadif Ahmed, Zahin Wahab, Rifat Shahriyar, S. M. Sohan.
(ESEM 2025 Technical Track) [🔗](#)

We propose a hybrid LLM-based framework for secret detection in source code, combining regex-based extraction with LLM classification to reduce false positives. Fine-tuned open-source models, including LLaMA-3.1 8B and Mistral-7B, achieve up to 0.985 F1 and 0.982 accuracy on a large GitHub benchmark, demonstrating the effectiveness and practicality of LLM fine-tuning for secure, local deployment.

Secret Leak Detection in Software Issue Reports using LLMs: A Comprehensive Evaluation.

Authors: Sadif Ahmed, Md Nafiu Rahman, Zahin Wahab, Rifat Shahriyar, Gias Uddin.
(arXiv) [🔗](#)

Submitted at MSR 2026 Technical Track

We introduce a hybrid LLM-based pipeline for detecting secret leaks in GitHub issue reports, combining regex extraction with contextual classification. Trained on 54,000 instances with 5,800+ verified secrets, fine-tuned open-source models like Qwen and LLaMA achieve up to 94.49% F1 and generalize well to real-world repositories (81.6% F1), highlighting their effectiveness for practical secret detection.

A Survey on Agentic Security: Applications, Threats and Defenses.

Authors: Asif Shahriar, Md Nafiu Rahman, Sadif Ahmed, Farig Sadeque, Md Rizwan Parvez.
(arXiv) [🔗](#)

Submitted at EACL 2026

We present the first comprehensive survey of the rapidly evolving field of agentic security, systematically reviewing

more than 150 papers published primarily between 2024 and 2025. Our study organizes the domain into three interconnected pillars: Applications, Threats, and Defenses, providing a unified framework to understand the capabilities and vulnerabilities of Large Language Model (LLM) agents in cybersecurity.

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

Submitted at BLP Workshop at AACL-IJCNLP

Authors: Mahir Labib Dihan, Sadif Ahmed, Md Nafiu Rahman.

We introduce BanglaForge, a new framework designed to generate executable code from Bangla language descriptions, addressing the challenges of a low-resource setting. Our approach employs a retrieval-augmented dual-model collaboration paradigm with iterative self-refinement guided by execution feedback. By integrating LLM-based translation and in-context learning, the system achieves a strong Pass@1 accuracy of 84.00% on the BLP-2025 Bangla Code Generation benchmark, demonstrating the effectiveness of our method for low-resource code generation.

EVCC: Enhanced Vision Transformer-ConvNeXt-CoAtNet Fusion with Adaptive Routing for Classification.

Authors: Kazi Reyazul Hasan, Md Nafiu Rahman, Sadif Ahmed, Wasif Jalal, Shahriar Raj, Mubasshira Musarrat, Muhammad Abdullah Adnan.

([OpenReview submission](#))

Submitted at WACV 2026

We introduce EVCC, a multi-branch hybrid architecture that combines Transformers and convolutional backbones via adaptive token pruning, gated cross-attention, auxiliary heads, and a dynamic routing mechanism. Experiments demonstrate improved accuracy-efficiency trade-offs across multiple datasets, with meaningful FLOP reductions while maintaining or improving classification accuracy.

Explainable Transformer-CNN Hybrid for Modeling Brain Aging from MRI Images.

Authors: Wasif Jalal, Md Nafiu Rahman, Md Sohel Rahman (ongoing).

An ongoing research into hybrid Transformer-CNN models for brain-age prediction from MRI slices, emphasizing explainability and interpretable feature fusion between slice-wise and volumetric representations.

Technical Skills

Data Science & ML: Python, NumPy, Pandas, scikit-learn, PyTorch, TensorFlow, torchvision, Microsoft Excel.

Databases: PostgreSQL, PL/pgSQL, MongoDB, Firebase Firestore.

Full-Stack: Node.js (backend), HTML/CSS, React, Svelte, Flutter (mobile).

Languages: C/C++, Python, Java, JavaScript / TypeScript, PHP, Bash, Dart.

Languages (spoken/written): English (proficient), Bengali (native).




Achievements

- Top 20 finalists Robi Datathon 2024 (national deep learning competition).
- Deans list award and university merit scholarship at BUET.
- 5th at BLP 2025 Code Generation Challenge





Academic Projects

- **Machine Learning Algorithms and Neural Network from Scratch** – github.com/nafiurahman00/CSE-472 – Implementations of core ML algorithms (logistic regression with ensembles, PCA/SVD for reconstruction, EM clustering) and a feed-forward neural network with Adam optimizer built from numpy.
- **Cryptography and Security Attacks** – github.com/nafiurahman00/CSE-406 – Implemented AES encryption and Diffie-Hellman key exchange, socket communication demos, and reviewed a mobile pentesting framework as part of course project.
- **Network Simulation** – github.com/nafiurahman00/CSE-322 – Implemented Congestion Control Algorithm, threaded server-client sockets, error correction algorithms and simulated wired/wireless mobility scenarios.
- **Operating System Internals with xv6** – github.com/nafiurahman00/CSE-314 – Implemented threading and synchronization primitives, system calls, and explored scheduler internals in xv6.
- **BusBuddy (Android)** – github.com/nafiurahman00/BusBuddy-Client-End – Flutter app with Node.js

backend, PostgreSQL and Firebase integration. Provided ticketing, schedules, tracking and real-time updates for university bus users.

- **Nishorgo (E-commerce)** – [Term-Project-2-2-Nishorgo](#)  – Full stack e-commerce site for plant sales with filtering, cart, admin analytics and order management.
- **Compiler (subset of C)** – github.com/nafiurrahman00/Compiler  – Subset-of-C compiler using Lex/Yacc and 8086-style assembly generation: lexer, parser, and intermediate code generation.
- **Catch the Egg (Game)** – github.com/nafiurrahman00/Catch-The-Egg  – OpenGL / Igraphics game for catching falling eggs; implemented game mechanics, scoring and difficulty scaling.

References

- **Dr. Rifat Shahriyar**, Professor, Department of CSE, Bangladesh University of Engineering and Technology (BUET) – rifat.shahriyar@gmail.com  – rifat@cse.buet.ac.bd 
- **Dr. Md Rizwan Parvez**, Scientist, Qatar Computing Research Institute (QCRI) – rizwan@ucla.edu  – rizwan.incipient@gmail.com 
- **Dr. Farig Sadeque**, Associate Professor, Department of CSE, BRAC University – farig.sadeque@bracu.ac.bd 