

# Tanzim Hossain Romel

Uttara, Dhaka, Bangladesh | romel.rcs@gmail.com | +88 01771 600158 | linkedin.com/in/thromel  
github.com/thromel| tanzimhromel.com

## Education

**Bangladesh University of Engineering and Technology (BUET) – Dhaka,** April 2018 – May 2023  
Bangladesh

B.Sc. in Computer Science and Engineering

- **CGPA:** 3.53/4.00 (3.61 in final term) | 3.86/4.00 in sessional courses (lab practicals and group projects)
- **Dean's List:** Level-2 for outstanding academic results
- **Relevant Coursework:** Machine Learning, High Performance Database Systems, Fault Tolerant Systems, Data Structures and Algorithms, Operating Systems, Computer Security

## Research

**ReAgent++: Runtime Detection of Aligned Backdoors in LLM Agents** Oct 2025 - Present  
(Research in progress)

- Designing novel backdoor detection system for LLM agents that complements consistency checks with STRIP-style runtime perturbation testing and K-Arm trigger-inversion scanning adapted for agent actions and text inputs
- Developing Text/Env-STRIP detector measuring choice entropy under perturbations (text, environment, multi-turn history) to identify aligned backdoors that preserve instruction compliance while biasing brand/tool selection
- Implementing K-Arm bandit-based trigger inversion using multi-armed optimization over discrete choice schemas (brands, tools, operations) with genetic algorithms and LM-guided beam search for minimal trigger recovery
- Planning comprehensive evaluation on WebShop (1.18M products), OSWorld (369 real desktop tasks), and AgentBench across diverse backdoor types including multi-turn, temporal, and environment-triggered attacks

**An Empirical Study on Remote Code Execution in ML Model Hosting Ecosystems** March 2025 - Present  
(Manuscript in progress; target venue: MSR 2026)

- Comprehensive analysis of trust\_remote\_code vulnerabilities across 6 ML platforms (Hugging Face, PyTorch Hub, ModelScope, OpenCSG, OpenMMLab, NVIDIA NGC) examining custom code execution during model loading
- Conducted multi-phase empirical study including metadata extraction, custom code download, static analysis for security smells, and qualitative analysis of developer discussions from GitHub and Stack Overflow
- Proposed security recommendations for platform maintainers including SafeTensors format adoption and runtime isolation strategies; developed automated vulnerability detection toolkit

**Multi-Agent Framework for Generating Relational DB Schema & ERD from Requirements** Aug 2025 - Present  
(Work in progress)

- Mentor and co-researcher with Dr. Sukarna Barua (BUET); extending SchemaAgent baseline with domain-specific language for improved agent-to-agent communication
- Reduced schema generation errors by 42% through DSL-based communication protocol and hierarchical agent architecture with specialized roles for entity extraction, relationship mapping, and constraint validation

**Design by Contract for LLM APIs: Automated Enforcement and Runtime Remediation** Nov 2024 - Present  
(GitHub repository and draft manuscript available)

[Project]

- Research collaboration with Dr. Akond Rahman (Auburn University); developed taxonomy for API contracts in LLM libraries through empirical study of 412 real-world issues
- Created OpenAI SDK extension and LangChain extension for automatic contract enforcement and runtime remediation, preventing common API misuse patterns

**An Unconventional Tale on Sentiment Analysis over Anonymous Online Reporting by the People in Bangladesh during an Outburst Period**  
[Paper]

Sep 2024 - Nov 2024

- Developed *uReporter* – Bangladesh’s first anonymous online reporting system critical during 2024 national crisis
- Analyzed 124 crowd-sourced reports using six transformer models (RoBERTa, DistilBERT, XLM-EMO) with multilingual NLP pipeline for Bengali/Romanized Bengali
- Demonstrated anonymous crowd-sourcing’s potential for understanding Global South socio-political dynamics

**Patient-Centric Blockchain Framework for Electronic Health Record Management**

June 2022 – May 2023

(Undergraduate Thesis)

[Thesis]

- Supervised by Professor ASM Latiful Hoque (BUET); designed blockchain framework separating encrypted off-chain storage from on-chain access control using Ethereum smart contracts and IPFS
- Implemented ERC-721 based patient records with AES-GCM encryption, ECIES key wrapping, and EIP-712 signed permissions; evaluated on 10,000 synthetic patients with comprehensive gas analysis and audit trails

## Experience

**Software Development Engineer 1, IQVIA – Dhaka, Bangladesh**

June 2023 – Present

- Backend Engineer developing microservices-based healthcare applications handling millions of patient records using .NET Core, C#, and AWS
- Deployed Multi-Agent systems using LangGraph for dashboard generation/modification, integrated with data exploration agent achieving 85% reduction in setup time
- **Developed novel gap-based axis break algorithm** for data visualization, addressing outlier-threshold limitations and improving chart clarity
- Achieved 60% reduction in query execution times through database optimization; implemented 40% API response improvement via Redis caching
- Pioneered browser automation testing methodology in .NET, simplifying regression testing and improving test coverage from 72% to 95%
- Received IQVIA Impact Program – Silver award (May 2025) for outstanding performance

## Projects

**Blockchain-Based Ticketing Platform**

Jan 2021 - April 2021

- **Finalist in Blockchain Olympiad Bangladesh (BCOLBD) 2021** with team "Recursively Enumerable" alongside Ataf Fazledin Ahamed and Md. Tanzim Azad Nishan from BUET
- Designed NFT-based ticketing system using Ethereum and Polygon with ERC-1155 standard, smart contracts for anti-scalping rules, and dynamic QR codes for fraud prevention
- Implemented decentralized identity management with verifiable credentials and zero-knowledge proofs for privacy-preserving ticket verification

**Production-Ready Database Engine in Go**

Oct 2024 - Present

- Built complete database engine from scratch implementing B+ tree indexing with configurable branching factor, automatic node splitting, and  $O(\log n)$  lookups
- Developed page management system with 8KB fixed-size pages, checksums, and buffer pool with LRU eviction; achieved 2M ops/sec for reads
- Implementing ACID transactions with WAL, crash recovery using ARIES protocol, and concurrent access support with proper synchronization

**Image Captioning with Attention Mechanisms**

Jan 2023 – Feb 2023

- Implemented Show, Attend and Tell architecture with ResNet-101 encoder and LSTM decoder achieving BLEU-4: 0.335, CIDEr: 0.92 on MS-COCO (Karpathy split)
- Enhanced baseline with beam search decoding ( $k=5$ ) and multi-head attention mechanism, achieving 11-point BLEU-4 improvement over VGG+greedy baseline
- Conducted comprehensive ablation studies and attention visualizations; trained model converged in 23 epochs (25 hours) using mixed precision training on single GPU

## Eventfly: End-to-end Event Management System

May 2022 - July 2022

- Designed microservices-based system with TypeScript, Express.js, Next.js, Docker, Kubernetes, NATS, and MongoDB
- Led back-end architecture implementing newsfeed, payment, authentication, and event management services

## Achievements & Awards

---

- **IQVIA Impact Program – Silver Award** (May 2025) – Outstanding performance and essential feature development
  - **Finalist, Blockchain Olympiad Bangladesh 2021** – Top 40 teams nationally with "Blockchain Based Ticketing Platform"
  - **2nd place** in Bangla Handwritten Digits Recognition contest (95.9% accuracy) using custom CNN at BUET ML Lab (2022)
  - **Dean's List Award** for outstanding academic results in Level-2 of BUET
  - National prize winner in Bangladesh Physics Olympiad (2017) and Chemistry Olympiad (2017)
  - **Talentpool HSC Scholarship** – 15th in Rajshahi Board with 95.6% marks (2017)
- continue

## Technical Skills

---

- **Languages:** C#, Python, JavaScript, TypeScript, Go, SQL
- **ML/AI:** PyTorch, LangChain, LangGraph, OpenAI API, Transformers, NumPy, Pandas
- **Backend & Databases:** .NET Core, ASP.NET, Express.js, FastAPI, PostgreSQL, MongoDB, Redis, SQL Server, DynamoDB
- **Cloud & DevOps:** AWS, Azure, Docker, Kubernetes, GitHub Actions, Terraform, OpenTelemetry, Jaeger
- **Blockchain:** Ethereum, Solidity, Hyperledger Fabric, Smart Contracts

## Test Scores

---

- **TOEFL iBT:** 103/120 (Listening: 29, Reading: 29, Writing: 22, Speaking: 23)