Tanzim Hossain Romel

+88 01771 600158 | romel.rcs@gmail.com | tanzimhromel.com

LinkedIn: thromel | GitHub: thromel

Uttara, Dhaka, Bangladesh

Education

- **Bangladesh University of Engineering and Technology (BUET)** *Mar 2018 - May 2023*
  B.Sc. in Computer Science and Engineering Dhaka, Bangladesh
  - CGPA: 3.53/4.00 [3.61 in final term]
  - Thesis: Patient-Centric Blockchain Framework for Electronic Health Record Management

Research Interests

AI for Software Engineering (AI4SE), Empirical Software Engineering, Software and LLM Security, Human-Centered Computing, Blockchain Systems

Work Experience

- **IQVIA** *June 2023 - Present*
  Software Development Engineer Dhaka, Bangladesh
  - 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
  - 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

Research Experience

- **An Empirical Study on Remote Code Execution in ML Model Hosting Ecosystems** *June 2025 - Oct 2025*
  Tools: Python, Bandit, CodeQL, Semgrep, YARA, CWE Analysis | In Review at MSR 2026
  - First large-scale cross-platform study analyzing ~45,000 repositories across 5 major platforms (Hugging Face, ModelScope, OpenCSG, OpenMMLab, PyTorch Hub) with co-authors Mohammad Latif Siddiq and Joanna C. Santos
  - Detected security vulnerabilities using static analyzers and YARA malware signatures: found CWE-502 (unsafe deserialization) in 74.54% and CWE-95 (eval injection) in 15.02% of affected repositories; 10.41% of Hugging Face repos contain security smells
  - Analyzed 600+ developer discussions to create taxonomy of security misconceptions; revealed only 6.6% SafeTensors adoption and widespread trust_remote_code usage
- **ReAgent++: Detecting Aligned Backdoors in LLM Agents** *August 2025 - Present*
  Tools: Python, STRIP, K-Arm, UCB Scheduler, WebShop, OSWorld, AgentBench
  - Extending ReAgent to detect aligned backdoors that maintain semantic consistency while subverting user intent through preference manipulation; collaboration with Dr. Chowdhury Md. Rakin Haider (BUET)
  - Implementing Text/Env-STRIP for perturbation-based runtime detection, and K-Arm trigger inversion for forensic analysis with multi-armed bandit optimization
  - Evaluating on 3 benchmarks (WebShop-1.18M products, OSWorld-369 tasks, AgentBench) against comprehensive attack suite including Sleeper-style, instruction backdoors, and multi-turn hidden triggers
- **Multi-Agent Framework for Generating Relational DB Schema & ERD** *July 2025 - Present*
  Tools: Python, LangGraph, StateGraph, Z3 Solver, SQLAlchemy, Text2Schema
  - Extended SchemaAgent with Dr. Sukarna Barua (BUET) using LangGraph StateGraph architecture with conditional routing and 3-tier auto-repair system
  - Designed 6-stage decomposed pipeline with specialized agents for entity extraction, relationship mining, and normalization with Z3 formal verification
  - Implemented granular component-level retry mechanism with intelligent violation analysis, reducing redundant LLM calls by 80%
- **Design by Contract for LLM APIs** *Nov 2024 - Present*
  Tools: Python, OpenAI SDK, LangChain, Runtime Monitoring, Contract Enforcement | Manuscript in preparation

- Developing taxonomy for API contracts through empirical study of 412 real-world issues with Dr. Akond Rahman (Auburn University)
- Created OpenAI SDK and LangChain extensions for automatic contract enforcement and runtime remediation
- Implemented precondition/postcondition validators with automatic retry mechanisms and fallback strategies

- **Sentiment Analysis of Anonymous Crisis Reports in Bangladesh** *Sep 2024 - Nov 2024*
  Tools: Python, BERT, XLM-RoBERTa, Transformers, Bengali NLP, Flask
  - Developed uReporter – Bangladesh's first anonymous reporting system during 2024 national crisis
  - Analyzed 124 crowd-sourced reports using six transformer models 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 Secure EHR Management** *June 2022 – May 2023*
  Tools: Solidity, Ethereum, IPFS, React, Web3.js, AES-GCM, ECIES, EIP-712
  - Proposed a patient-centric blockchain architecture that decouples encrypted off-chain FHIR record storage from on-chain access control, eliminating trusted intermediaries and enabling verifiable patient.
  - Implemented an ERC-721–based smart contract for record ownership with EIP-712 signed, time-bounded permissions and ECIES-wrapped AES-GCM keys ensuring confidentiality and non-repudiable authorization.
  - Integrated off-chain IPFS storage with on-chain audit trails, achieving tamper-evident data integrity and complete access traceability through event logs.
  - Evaluated scalability on 10,000 synthetic FHIR records; achieved 1.3–2.0 s end-to-end latency for 1 MB records and 10× gas reduction via Layer-2 (zkSync/Arbitrum) deployment.

Projects

- **Yet Another C Compiler** *Jun-Aug 2021, Oct 2024*
  Tools: C++17, CMake
  - Built complete C compiler with hand-written lexer and parser, semantic analysis, and x86-64 code generation
  - Implemented SSA-based optimization pipeline including SCCP, GVN, LICM, and dead code elimination
  - Designed a linear scan register allocator with spilling support
  - Modernized legacy Flex/Bison-based prototype into a compiler architecture with modular IR passes and extensible optimization pipeline
- **Database Engine in Go** *Oct 2024 - Present*
  Tools: Go, B+ Tree, WAL, ARIES Protocol
  - Built complete database engine from scratch with B+ tree indexing and page management system with 8KB pages
  - Implemented LRU buffer pool achieving ~2M ops/sec for reads
  - Implemented ACID transactions with WAL, crash recovery using ARIES protocol, and concurrent access support
- **Modern Image Captioning System** *Jan 2023 – Feb 2023*
  Tools: PyTorch, CLIP, ViT, GPT-2, AoA, SCST, MS-COCO
  - Built modular image captioning system combining vision (ResNet, ViT, CLIP) and language (LSTM, Transformer, GPT-2) models
  - Reached **127.6 CIDEr**, **0.392 BLEU-4**, **0.298 METEOR** on MS-COCO (Karpathy split) using CLIP + GPT-2 + AoA + SCST
  - Improved CIDEr by +26.4 over ResNet-LSTM baseline through architectural and training refinements
  - Applied Self-Critical Sequence Training and attention visualization for interpretability
- **Eventfly: End-to-end Event Management System** *May 2022 - July 2022*
  Tools: TypeScript, Express.js, Next.js, Docker, Kubernetes, NATS, MongoDB
  - Designed microservices-based event management system
  - Led back-end architecture implementing newsfeed, payment, authentication, and event management services
- **Network Simulation & TCP Protocol Analysis** *Jan 2022 - May 2022*
  Tools: NS3, C++, TCP Reno, TCP Vegas
  - Implemented and analyzed TCP congestion control variants (Reno vs Vegas) using NS3 network simulator
  - Designed TCP Vegas+ modification addressing fairness issues through dual-mode operation
  - Conducted comprehensive performance analysis measuring throughput, fairness index, and packet drop ratios

Skills

- **Programming Languages:** C#, Python, JavaScript, TypeScript, Go, SQL, Java, Solidity
- **ML/AI Frameworks:** PyTorch, LangChain, LangGraph, Transformers, ResNet, LSTM, BERT
- **Backend Frameworks:** .NET Core, ASP.NET, Express.js, FastAPI, Next.js
- **Databases:** PostgreSQL, MongoDB, Redis, SQL Server, DynamoDB
- **Cloud & DevOps:** AWS, Azure, Docker, Kubernetes, GitHub Actions, Terraform, OpenTelemetry, Jaeger, NATS
- **Blockchain & Web3:** Ethereum, Solidity, IPFS, ERC-721, ERC-1155, Web3.js
- **Tools & Technologies:** NS3, Flex, Bison, Git, Linux, WAL, ARIES Protocol

Honors and Awards

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

Test Scores

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

Additional Information

Languages: Bengali (Native), English (Professional proficiency)
Interests: AI Security Research, Blockchain Technology, Database Systems, Reading Research Papers