

Tanzim Hossain Romel

tanzimho@ualberta.ca | tanhromel@gmail.com | tanzimhromel.com

LinkedIn: [thromel](#) | GitHub: [thromel](#) | Google Scholar

Uttara, Dhaka, Bangladesh

RESEARCH INTERESTS

AI for Software Engineering (AI4SE), Software Engineering for AI (SE4AI), Trustworthy AI, Software Security, LLM Security

EDUCATION

- **University of Alberta** Starting Sep 2026
Incoming M.Sc. in Computing Science Edmonton, Canada
 - Incoming member of the [U-A-Goose](#) research group in the Department of Computing Science.
- **Bangladesh University of Engineering and Technology (BUET)** Mar 2018 - May 2023
B.Sc. in Computer Science and Engineering Dhaka, Bangladesh
 - Thesis: Patient-Centric Blockchain Framework for Electronic Health Record Management

WORK EXPERIENCE

- **IQVIA** June 2023 - June 2026
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
 - Contributed to 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 (SELECTED)

- **An Empirical Study on Remote Code Execution in ML Model Hosting Ecosystems** June 2025 - Oct 2025
Tools: Python, Bandit, CodeQL, Semgrep, YARA, CWE Analysis | Submitted to TOSEM 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.
 - Analyzed 600+ developer discussions to create taxonomy of security misconceptions.
- **The Choice Can Be the Attack: Auditing Aligned Backdoors in LLM Agents** August 2025 – Present
Tools: Python, WebShop-style Evaluation, Hugging Face Jobs, vLLM, Counterfactual Auditing, Choice Modeling
 - Built **SHIFT** (*Structured Hidden Influence Test*), an endpoint-black-box audit for *aligned backdoors* in LLM agents, targeting attacks that preserve instruction validity while covertly steering which acceptable brand, seller, or product gets chosen.
 - Reframed aligned backdoor detection as *choice auditing* rather than task-failure detection by combining a matched trigger audit with a feature-controlled choice model to test whether a trigger adds extra preference for attacker-chosen options after accounting for observable quality signals.
 - Implemented the full controlled WebShop-style evaluation stack: synthetic confounding studies, live clean/suspect endpoint logging, 29-variant benign-vs-trigger-preserved stress suites, same-anchor external baseline comparisons, and a Qwen3.5-9B scale-up replication.
 - Showed a strong 9B endpoint case study with perfect weak-stage clean/suspect separation and large bounded target uplift, while also documenting the method's main limitation: stronger benign catalog shifts and omitted option features remain the key calibration boundary.
- **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

PROJECTS

- **Yet Another C Compiler**

Jun-Aug 2021, Oct 2024

Tools: C++17, CMake

- Built complete C compiler with 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

- **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

OPEN SOURCE CONTRIBUTIONS

- **Open Source Contributions (Selected)**

2025 – 2026

Selected upstream contributions across agent systems, program analysis, compilers, developer tooling, and .NET

[GitHub](#)

- **deepagents**: merged a CLI fix that stops and clears LoadingWidget animation timers on stop and unmount, preventing interval leaks in long-running terminal sessions and adding regression coverage for both cleanup paths.
- **RefactoringMiner**: merged merge-parent-aware commit diff support for merge commits, including parent selection in the CLI and webdiff, parent-aware caching, and robust handling of empty commit compares.
- **typescript-go**: merged an upstream-aligned declaration-emit alias-resolution fix that preserves imported type aliases for inferred exports across module boundaries in Microsoft's Go port of TypeScript.
- **EF Core**: merged runtime migration creation/application, ON DELETE SET DEFAULT support, and nullable complex-property reload handling.
- **LangChain**: improved diagnostics for non-JSON-serializable tool schemas during tool definition.
- **GenHTTP**: added automatic request decompression and binary-response support.

SKILLS

- **Agentic AI & LLM Systems:** LLM agents, tool calling, RAG, prompt engineering, multi-step workflows, LLM evaluation, counterfactual auditing, model serving, fine-tuning
- **ML/AI Frameworks:** PyTorch, Transformers, Hugging Face, LangChain, LangGraph, vLLM
- **Programming Languages:** Python, TypeScript, JavaScript, C#, C++, Go, SQL, Java, Solidity
- **Backend Frameworks:** .NET Core, ASP.NET, FastAPI, Express.js, 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 & Platforms:** Linux, Git, Hugging Face Jobs, WebShop, NS3, Flex, Bison

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)