

Rishi Saha

Kalyani, West Bengal, India

brownjeesus@icloud.com | cse25073@iiitkalyani.ac.in

github.com/saintbelow | linkedin.com/in/rishi-saha-0a3614380

EDUCATION

Indian Institute of Information Technology (IIIT) Kalyani

Bachelor of Technology in Computer Science and Engineering

Kalyani, WB

Expected 2029

TECHNICAL SKILLS

Languages: C, C++, Rust, Go, Python, JavaScript, TypeScript, Java, Assembly (x86-64, ARM64), Lua, Bash/Zsh, SQL, Verilog, LaTeX

Systems & Low-Level: POSIX/Linux APIs, GDB, LLDB, Ptrace, Makefiles, CMake, Bare-Metal Bootloaders, Hypervisor-class Analysis, Memory Mapping, Entropy Analysis, Custom ELF Loaders

Offensive & Defensive Security: Reverse Engineering (Ghidra, IDA Pro, Radare2), Binary Exploitation, ROP/JOP Chains, Fuzzing (AFL++, libFuzzer), Threat Modeling (STRIDE/PASTA), Network Forensics (Wireshark, tcpdump), Zero-Day Triage, ATT&CK Mapping, OWASP Top 10, Burp Suite, Nmap, Metasploit

AI / ML & Adversarial: PyTorch, TensorFlow, Hugging Face Transformers, LangChain, LangGraph, RAG Pipelines, Vector Databases (pgvector, Pinecone, Qdrant), LLM Fine-Tuning (LoRA/QLoRA), Small Language Models (SLMs), Adversarial ML, Prompt Injection & Jailbreak Defenses, Model Red-Teaming

Infrastructure & Cloud: Next.js, React, Supabase, PostgreSQL, Redis, Docker, Kubernetes, Nginx, Caddy, Cloudflare Tunnels, SeaweedFS, Vercel, Self-Hosted Coolify/Dokku, Serverless Architecture, WebRTC, WebSockets

Hardware & RF: FPGA Synthesis (Verilog, Vivado), Software-Defined Radio (BladeRF, HackRF), GNU Radio, ODU Firmware Reverse Engineering, JTAG/SWD Debugging, Logic Analyzers, Professional A/V Hardware Integration

Scientific Computing: Quantum Field Simulation (Axion-Photon Conversion), Orchestrated Objective Reduction (Orch-OR) theoretical modeling, Numerical Methods, NumPy/SciPy

PROFESSIONAL EXPERIENCE & OPERATIONS

Confidential Defense Sector Client

Security Operations Contractor

- Conducted targeted threat modeling and security auditing under a strict Non-Disclosure Agreement (NDA) to identify and mitigate architectural vulnerabilities across mission-critical national infrastructure.
- Executed low-level vulnerability assessments, binary-level reverse engineering, and system hardening protocols to elevate baseline operational security against advanced persistent threat (APT) vectors.
- Performed adversarial red-team simulations and post-exploitation telemetry analysis, mapping observed TTPs to the MITRE ATT&CK framework while honoring compartmentalized disclosure.
- Collaborated with defense-sector stakeholders to audit system integrity, strictly adhering to classified reporting methodologies, chain-of-custody protocols, and compliance boundaries.

IEEE Student Branch, IIIT Kalyani

Lead Digital Architect & Webmaster

- Engineered a proprietary, fully **self-hosted** serverless web application and researcher dashboard utilizing **Next.js**, **Supabase (self-hosted on bare-metal via Docker Compose)**, **PostgreSQL**, and **Redis**, decommissioning legacy on-premise servers and eliminating third-party data residency exposure.
- Provisioned the entire stack behind **self-hosted Nginx reverse proxies**, **Cloudflare Tunnels**, and **Coolify orchestration**, achieving a zero-latency, end-to-end encrypted event pipeline with full data sovereignty.
- Directed digital infrastructure and technical moderation for a high-stakes institutional broadcast on “*Real Talk: Adversaries, Defense, and the Future of Cybersecurity*” featuring **Bruce Schneier** (Harvard Kennedy School Lecturer, internationally renowned cryptographer) – youtu.be/2z6KuGzZb8U.
- Architected the broadcast pipeline and moderated a deep-tech academic discourse with **Dr. Tanmoy Chakraborty** (Head of LCS2 Lab, IIT Delhi) on Small Language Models (SLMs), automated zero-day exploit generation, and adversarial ML – youtu.be/E1eonWXxwts.
- Scaled the encrypted broadcast architecture to host hundreds of concurrent international viewers across both sessions while maintaining **100% system uptime** and zero packet drops.
- Managed an end-to-end professional media production stack – integrating high-end A/V hardware (Sony A7 IV, multi-channel audio mixers) and **self-hosted SeaweedFS distributed storage** – to capture, encode, and distribute long-form deep-tech academic discourse with full archival sovereignty.

repX Framework | *Native C/C++, Reverse Engineering, Systems Architecture*

- Architected a multi-architecture, boot-centric reverse-engineering framework written natively in C/C++ to enable bare-metal system introspection without OS-level dependencies.
- Engineered hypervisor-class analysis tools, custom ELF loaders, and memory mapping protocols, facilitating automated execution tracing, register snapshotting, and hardware-level state extraction across heterogeneous targets.
- Integrated entropy analysis pipelines to detect packed/obfuscated binaries, anti-debugging primitives, and high-randomness regions characteristic of embedded cryptographic payloads.
- Designed a highly modular architecture optimized for cross-platform compatibility, with deterministic memory management routines and zero-allocation hot paths.
- Authored custom Makefile build systems automating the cross-compilation pipeline across multiple OS architectures, entirely independent of high-level IDE dependencies.

Adversarial LLM Red-Team Sandbox | *Python, PyTorch, LangGraph, Self-Hosted Inference*

- Built a self-hosted adversarial evaluation harness for open-weight Small Language Models (SLMs), automating prompt-injection, jailbreak, and indirect-injection attack vectors against retrieval-augmented generation (RAG) pipelines.
- Engineered a fuzzing-style mutation engine that programmatically generates adversarial inputs and scores model robustness using a custom STRIDE-aligned threat taxonomy.
- Deployed the full inference stack on self-hosted GPU nodes via Docker + vLLM, with pgvector for embeddings and Qdrant for hybrid search – eliminating reliance on third-party LLM providers.
- Implemented telemetry capture and automated regression scoring to track model degradation across fine-tuning checkpoints (LoRA / QLoRA).

Hardware & Quantum Architectural Research | *SDR, FPGA, Compute Simulation*

- Simulated quantum field scanners modeling axion-photon conversion parameters to evaluate theoretical detection limits in high-energy physics regimes.
- Analyzed hardware-software co-design bottlenecks utilizing **BladeRF** for Software-Defined Radio (SDR) research and synthesizing custom FPGA architectures (Verilog) to intercept and evaluate ODU firmware mechanics.
- Investigated Orchestrated Objective Reduction (Orch-OR) theoretical models, bridging quantum computation primitives with classical neural architecture for novel inference substrates.

Institutional Broadcast Infrastructure | *Next.js, Supabase, PostgreSQL, SeaweedFS*

- Engineered and deployed a proprietary serverless web architecture handling institutional digital routing, real-time database management, and encrypted session brokering – fully self-hosted with zero managed-service dependencies.
- Implemented a zero-latency, end-to-end encrypted event pipeline that scaled to host hundreds of concurrent users across geographically distributed endpoints.
- Integrated self-hosted SeaweedFS distributed object storage for high-throughput archival of multi-hour 4K broadcast assets with sub-millisecond seek latency, replacing commercial CDN reliance.
- Hardened the perimeter using Cloudflare Tunnels, WireGuard mesh, and fail2ban-driven intrusion deterrence to neutralize automated scanning and credential-stuffing attempts.