Aryan Mondal

aryanmondal@umass.edu | LinkedIn | GitHub | Scholar

Education

University of Massachusetts Amherst — Amherst, Massachusetts
MS in Computer Science — *Sep 2026 – Present*

- **Relevant Coursework**: COMPSCI 660 Advanced Information Assurance, COMPSCI 590AF Reverse Engineering & Understanding Exploit Development, COMPSCI 589 Machine Learning

SRM Institute of Science and Technology — Chennai, Tamil Nadu
B.Tech in Computer Science And Engineering, CGPA: 8.39/10 — *Sep 2022 – May 2026*

- **Relevant Coursework**: Cryptography and Network Security, Forensics and Incident Response, Security Management, Computer Networks, Cyberwarfare, Mobile and Wireless Security, Hacker Techniques, Tools, and Incident Handling

Experience

Security Intern — Feb 2025 – Mar 2025
Thirumoolar IT Solutions — *Chennai, Tamil Nadu*

- Implemented 20+ vulnerability scans and penetration tests using OWASP ZAP, Burp Suite, and Nmap to establish a missing security baseline, identifying 40+ issues and achieving a 25% improvement in overall security posture.
- Investigated codebases of 3 internal web applications where unreviewed code posed active exploit risk, applying manual analysis to surface SQL Injection and XSS vulnerabilities and enabling developers to resolve a significant share of security flaws.
- Researched and summarized emerging threats in response to a rapidly evolving landscape, synthesizing intelligence reports to strengthen the internal knowledge base and increase team response readiness.

Projects

Network Intrusion Detection System — Apr 2025 – Apr 2026

- Engineered a hybrid NIDS to address prohibitive compute costs on edge devices, combining a 4-layer DNN (∼68K params) with a pseudo-GNN branch (∼8K params) via adaptive late fusion to achieve 99.64% accuracy on 60,000 CIC-IDS-2017 flows at 1,250× fewer parameters than Transformer-based models.
- Designed a learnable sigmoid-normalized fusion weight α to eliminate manual ensemble tuning, which autonomously converged from 68.9% DNN to 61.1% GNN over 25 epochs, empirically establishing that relational features outperform statistical ones for intrusion detection.
- Optimized an end-to-end raw-socket-to-classification pipeline on PyTorch to meet real-time edge deployment demands, achieving 16,000+ flows per second at under 5 ms latency with a false positive rate of 0.08%.

Publications

Satellite-Based Quantum Pseudonym Relay: Performance and Security Analysis — Under Review
ACM Transactions on Quantum Computing (TQC)

- Built a Micius-calibrated free-space BB84 decoy-state QKD channel model in NetSquid to quantify satellite quantum pseudonym system feasibility, achieving 157.5 kbits (615 tokens) per clear-zenith pass at 500 km with QBER 0.025, matching the published ∼0.03 Micius benchmark.
- Modeled buffer resilience under a 4-state Markov weather chain with Kaplan–Meier yearly survival estimation, showing the token buffer survives 5 consecutive cloudy passes at 50 tokens/hr with >95% survival for degraded streaks up to 12 hours across 156 simulated weeks.
- Designed an orbital G-Set CRDT revocation scheme and identified a burst-mode timing side channel to bound satellite-specific security risks, quantifying a 47-minute false-accept window (reducible to ∼50 ms via hybrid fiber backup) and a cross-pass linkability advantage of 0.567 mitigated to 0.549 via cover traffic.

An Adaptive Feedback Architecture for Stabilizing SNSPDs in TF-QKD Networks using SDQN — Under Review
IEEE Transactions on Quantum Engineering (TQE)

- Engineered an SDQN with hot-swappable PID and Bayesian controllers to counter SNSPD performance collapse under real-world thermal stress, achieving a 41% improvement in Secret Key Rate and a 4× reduction in SKR variance (σ_{SKR}: 0.180 → 0.038).
- Modeled photon detection efficiency via Ginzburg–Landau critical current equations to address PID overshoot caused by the nonlinear bias–temperature relationship, deploying a Matérn 5/2 Gaussian Process with Expected Improvement to reach 95% of the optimum in 80 cycles versus 120 for PID alone.
- Implemented Mahalanobis Distance anomaly detection across correlated SKR, QBER, temperature, and bias metrics to catch physical-layer attacks that passive countermeasures miss, triggering an automated Security Mode clamp upon a 3σ breach to defeat blinding and thermal manipulation.

A Robust and Lightweight Authentication Protocol for UAV Swarm Communications using HKDF-based Key Derivation and AEAD Jul 2026

IEEE CONECCT 2026

- Designed R-HAAP to replace a cryptographically weak Duffing chaotic-map keystream with a verified ECDH → HKDF → ChaCha20-Poly1305 pipeline, achieving 150–250 μs per-packet latency on ARM Cortex-M4 — 20–33× faster than the original protocol and immune to cache-timing side-channel attacks.
- Implemented per-packet key derivation to eliminate replay and forgery risk from reused session keys, constructing a unique HKDF.expand info string from UAV ID and monotonic offset counter to cryptographically bind metadata to the Poly1305 MAC under dual replay countermeasures.
- Validated swarm scalability to address unproven crypto overhead at scale, simulating star and FANET mesh topologies across 10–100 UAVs in UavNetSim-v1 and achieving packet delivery rate above 99.8% and end-to-end latency under 15 ms.

Lightweight Hybrid DNN-GNN Architecture for Network Intrusion Detection with Adaptive Late Fusion Apr 2026

ICNWC 2026

- Designed a hybrid NIDS to retain relational traffic learning without expensive graph construction, integrating a 4-layer DNN (∼68K params) with a pseudo-GNN MLP (∼8K params) via adaptive late fusion to achieve 99.64% accuracy on 9,000 held-out test samples with 80K total parameters.
- Analyzed a learnable scalar α to quantify statistical versus relational discriminative power, finding it shifted from 68.9% DNN to 61.1% GNN over 25 epochs, with ablation confirming the 8K pseudo-GNN matched the full hybrid while outperforming the 68K DNN-only baseline by 0.12 percentage points.
- Benchmarked the model against ConvNeXt-Tiny (28M params) and a Transformer NIDS (100M params) to establish a new efficiency frontier, achieving competitive or superior accuracy at 350× and 1,250× fewer parameters with a false positive rate of 0.08%.

Quantum Key Distribution for SCADA in Power Grids: Security Architectures and Practical Applications Nov 2025

ICETCE 2025

- Developed SVM and Random Forest anomaly detection classifiers for QKD-enhanced SCADA where conventional cryptography is insufficient against quantum threats, training on 10,000 simulated data points with linear-kernel SVM achieving 94.90% accuracy and perfect anomaly recall (1.00).
- Evaluated four classifiers — SVM, Random Forest, KNN, and Neural Network — under class imbalance to identify the optimal model for critical-infrastructure deployment, comparing precision (0.68–0.70), recall (0.94–1.00), and F1-score (0.80–0.81) and demonstrating KNN's complete failure on the anomaly class.
- Established a replicable QKD-SCADA security framework to address the lack of standardized quantum-resilient grid architectures, researching 30+ field deployments and mapping BB84, decoy-state, and SDN-monitored QKD protocols to SCADA threat vectors including FDIA, MitM, and ransomware.

Technical Skills

Programming Languages: Python, C, C++, Bash, SQL
Cyber Security & Networking: Cryptography, Digital Forensics, Anomaly Detection, Malware Analysis, Penetration Testing, Web Exploits (SQLi, XSS), Operating Systems, SIEM/SOC Operations, SCADA Security, UAV Security, Quantum Key Distribution (QKD)
Tools & Frameworks: Claude Code, OWASP ZAP, Burp Suite, Nmap, Wireshark, Scapy, PyShark, Apache Kafka, FastAPI, Grafana, TensorFlow, Keras
Other Skills: Risk Management, Compliance & Regulation, Security Awareness, Threat Intelligence, Strategic Planning, Project Management