Aryan Mondal

aryanmondal@umass.edu | LinkedIn | Scholar

Education

SRM Institute of Science and Technology Chennai, Tamil Nadu

B.Tech Computer Science And Engineering, CGPA: 8.23 *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 – Apr 2025

Thirumoolar IT Solutions *Chennai, Tamil Nadu*

- Performed 20+ vulnerability scans and penetration tests using OWASP ZAP, Burp Suite, and Nmap, identifying 40+ security issues and contributing to a 25% improvement in system security posture.
- Reviewed codebases of 3 internal web applications, detecting SQL Injection and XSS vulnerabilities; collaborated with developers to achieve substantial reduction in exploitable security flaws.

Publications

A Robust Face Expression Recognition System with Music Recommendations Mar 2025

CoaCoNS 2025

- Designed real-time facial expression recognition using modified VGG-16 with transfer learning and data augmentation, achieving 88% accuracy on JAFFE (∼213 images, 7 classes); integrated Haar Cascade detection and a music recommendation engine mapping expression classes to playlists, validated on RTX 3080 over 50 training epochs.

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

ICETCE-2025

- Achieved 94.9% classification accuracy for anomaly detection in QKD-enhanced SCADA systems using SVM and Random Forest; SVM attained 100% recall with consistent F1-scores (0.80–0.81) validated on a 10,000-sample dataset.

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

ICNWC-2026

- Designed a hybrid DNN (256→128→64→32, ∼68K params) and Pseudo-GNN (64→64→32, ∼8K params) with adaptive late fusion, achieving 99.64% accuracy on CIC-IDS-2017 (60K samples) — 350× fewer params than ConvNeXt-Tiny and 1,250× fewer than Transformer-based NIDS, enabling edge deployment on Raspberry Pi.
- Learnable fusion weight α autonomously converged from 0.689→0.389 over 25 epochs, establishing GNN relational features as more discriminative; achieved 0.08% false positive rate and 16,000+ flows/sec at under 5 ms latency on RTX 3070.

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

IEEE CONECCT 2026

- Designed R-HAAP replacing chaotic-map keystream with ECDH → HKDF → ChaCha20-Poly1305; achieved 150–250 μs per-packet latency on ARM Cortex-M4 — 12–20× faster than AES-GCM and 20–33× faster than the original Duffing-map protocol.
- Validated via UavNetSim-v1 demonstrating 99.8%+ packet delivery and under 15 ms end-to-end latency across 10–100 UAV swarms; per-packet HKDF key derivation with monotonic counters provides provable resistance to replay and forgery attacks with forward secrecy via ephemeral ECDH session keys.

An Adaptive Feedback Architecture for Stabilizing SNSPDs in TF-QKD Networks using SDQN Under Review

IEEE Transactions on Quantum Engineering (TQE)

- Deployed SDQN-based adaptive stabilization of SNSPDs in Twin-Field QKD, achieving 41% Secret Key Rate improvement and 4× stability gain through hot-swappable PID and Bayesian optimization controllers validated via physics-realistic simulation with real-time security and environmental resilience.

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: 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