



Aditya Sharma

Roll No.: 2023A7PS0265U
B.E. Computer Science
BITS Pilani, Dubai Campus
Dubai, UAE

971507324469

✉ aditya.137.sharma@gmail.com
✉ f20230265@dubai.bits-pilani.ac.in
🐙 GitHub Profile
🌐 LinkedIn Profile

EDUCATION

- **BITS Pilani, Dubai Campus** Graduation 2027
B.E. in Computer Science CGPA: 8.92
 - Awarded 25% Merit Scholarship for academic excellence.
 - Relevant coursework: Intro. to LLM (BITS F471), QuantumArchitecture and Programming (CS F316), Public Policy (GSS F233), Machine Learning (CS F464), Deep Learning (CS F425), Design & Analysis of Algorithms (CS F364), Computer Networks (CS F303), Foundations of Data Science (CS F320), DBMS (CS F212), Operating Systems (CS F372).
- **Delhi Public School, Bhopal, India** Graduated 2023
High School (PCM Stream) Score: 93.8%

RESEARCH & PUBLICATIONS

- **QKnot: Hybrid Signatures that Outlive their Classical Half** Mar 2026 - Aug 2026
Post-quantum signing and identity registration for the ML supply chain. Sole author. Under review
 - to be submitted at USENIX Security 2027
 - Designed non-separable hybrid signatures with direction-typed timestamps and post-quantum key registration that does not inherit trust from classical PKI.
 - Ran a cross-registry audit of roughly 60,000 artefacts across HuggingFace, PyPI and npm; found no post-quantum signatures on any of them.
 - Shipped an accompanying Python CLI implementing ML-DSA-44/65/87 with Sigstore interoperability.
- **QResP: Cryptographic Provenance of Public ML Models** Feb 2026 - Mar 2026
Pilot audit that motivated QKnot; mapped to EU AI Act provenance obligations. Independent Research
 - Audited the top 1,000 HuggingFace models: 99.8% carry no cryptographic signature at all, and none are post-quantum safe.
- **White-Box Auditing of LoRA-Poisoned LLMs via Stackelberg Security Games** Feb 2026 - Present
Game-theoretic allocation of audit effort to detect covertly poisoned language models. Under revision
 - Submitted to the ICML Mechanistic Interpretability Workshop; two positive reviews and one substantive critique, full revision in progress.
 - Game theory and Stackelberg solver lead on a four-person team.
 - Revision work: treating attacker alignment γ as a continuous strategic choice, formalising undefined Q-entries as an imperfect-observation problem, and deriving a certifiable compliance bound framed around EU AI Act conformity assessment.
- **Privacy in Person Re-Identification** 2026 - Present
Ongoing collaboration with researchers at IIT Delhi and IIT Madras. Collaboration
- **Adversarial Vulnerabilities in Vision-Language Models** Apr 2026
White-box and black-box attack study on SmolVLM-500M. CS F425 — Course Project
 - Implemented white-box PGD and GCG attacks, and evaluated black-box universal adversarial perturbation transfer using XTransferBench.

EXPERIENCE

- **Indian Institute of Technology (BHU)** June 2025 - August 2025
Research Intern — Algorithmic Fairness Audit Varanasi, India
 - Audited ride-hailing platforms for pricing dark patterns, building instrumented data collection across repeated matched trips.
 - Trained models to test whether fare quotes varied with device and handset characteristics for otherwise identical routes.
 - Findings were written up as a report submitted to the Ministry of Consumer Affairs, followed by a presentation of the results.
- **Registrar's Office, BITS Pilani — Dubai Campus** Sept 2025 - Jan 2026
Professional Assistant Dubai, UAE
 - Built Python automation for KHDA student registration and bulk Excel data-filling workflows, replacing repetitive manual entry with validated pipelines.
 - Owned validation and reconciliation of large-scale institutional datasets on the KHDA portal, ensuring accuracy, traceability and on-time regulatory reporting.
 - Identified data inconsistencies and process gaps, improving reporting readiness and operational reliability for planning and governance decisions.
- **ANSOZ Creations** March 2020 - Feb 2022
Operations & Product Support Ashok Nagar, India
 - Contributed to the launch and iteration of a COVID-response mobile application used by local administration.
 - Triaged user feedback into prioritised change requests for the development team.

SELECTED PROJECTS (CLICK TITLE FOR GITHUB)

-  **a compliance + red-teaming harness for tool-using LLM agents (in working)** Sept 2026
You score an agent run against a declared policy Independent Project
 - a compliance + red-teaming harness for tool-using LLM agents.
 - keep the run isolated, and produce an auditable record.
-  **PolicyLens — Lineage-Tracked Policy Data Platform** Aug 2026
End-to-end pipeline from raw price data to a pre-registered statistical finding, dashboard and policy brief. Independent Project
 - Showed that retail markups on essential commodities vary significantly across Indian states.
 - Built with DuckDB, DVC and OpenLineage for reproducibility and column-level lineage; Streamlit and Plotly front end; ships a two-page policy brief.
-  **Dynamic Elo — Grand Slam Match Prediction** Mar 2026
Multifactor Elo rating extending standard Elo with Fatigue Index, Clutch Factor and Biometric Edge. CS F320 — Team Lead
 - 73.5% accuracy and 0.818 AUC on a held-out 2024 test set, using XGBoost over Jeff Sackmann's historical match data.
 - Led a team project through to clean Python scripts, a documented repository and a full academic report.
-  **Statistical Modelling and Verification** Nov 2025
Hypothesis testing and inference across multiple datasets using SciPy. Academic Project — Grade: A
 - Applied ANOVA, regression and a range of parametric and non-parametric tests with explicit assumption checking.

TECHNICAL SKILLS, LANGUAGES & INTERESTS

Languages: English (Fluent), Hindi (Native), French (Amateur), Arabic (Learning)

Programming: Python, Java, C, SQL, HTML, CSS, JS

ML / Research: PyTorch, Scikit-Learn, XGBoost, Pandas, NumPy, SciPy, HuggingFace, Qiskit

Security / Crypto: ML-DSA (Dilithium), Sigstore, hybrid signatures, supply-chain provenance, adversarial ML (PGD, GCG, UAP)

Data & Tooling: DuckDB, DVC, OpenLineage, Streamlit, Plotly, Git, L^AT_EX

Focus Areas: AI Security, Mechanistic Interpretability, Post-Quantum Cryptography, Technology Governance

Sports: Tennis, Snooker, Cricket

POSITIONS OF RESPONSIBILITY

- **Maintainer**, Q-BITS — quantum computing club org at BITS Pilani Dubai) *August 2026 - Present*
- **Program Coordinator**, SPIC MACAY Club, BITS Pilani Dubai *Oct 2024 - Present*
- **Student Social Worker**, Multiple NGOs *March 2020 - Present*
- **President**, The Universal Club, DPS Bhopal *July 2021*

ACHIEVEMENTS

- **Awarded 25% Scholarship** BITS Pilani Dubai Campus (Academic Merit) *Ongoing*
- **Ideal Student Award (PCM)** For outstanding conduct and academic excellence at DPS Bhopal *2023*
- **Marker Cup & Blue Blazer** Highest score in Physics/Chemistry; eight years of consistent excellence *2023*
- **High Commendation Awards** Multiple Model United Nations, for excellence in debate *2021*