

Rojan Upreti

iam@rojanupreti.com | [linkedin.com/rojan-upreti](https://www.linkedin.com/rojan-upreti) | github.com/Rojan-upreti | www.rojanupreti.com

Education

William Paterson University

Bachelor of Science, Computer Science

Wayne NJ, USA

Patent

- **Cryptographic Enclave AI Pipeline:**Provisional Patent Filing No: 64/085,842 · Filed Jun 9, 2026

Research

- CEAP: A Cryptographic Enclave AI Pipeline for PHI-Safe Large Language Model Inference in HIPAA-Regulated Environments.- *HealthCom IEEE*
- Adaptive Compositional Semantic Caching for Token Optimization in Commercial LLM APIs and RAG Pipelines. - *IEEE Gen AI Hackathon*
- Design and Implementation of an AI-Integrated Job Application Automation System with RealTime Cloud Synchronization.- <https://r1.rojanupreti.com/>.
- Innovative Network Security Research: AI-Powered Honeypot for Cyber Anomaly and Threat Detection using RaspBerry PI.- <https://r2.rojanupreti.com/>.

Experience

Medlock

Nov 2025 - Present

AI Operations & Solutions Engineer

- Architected and deployed a HIPAA monitoring SaaS platform on AWS EC2 Ubuntu instances, hosting MedGamma LLMs through llama.cpp, orchestrating AI workflows with LangChain, utilizing AWS Nitro Enclaves, and implementing PostgreSQL-backed cryptographic audit logging
- Built real-time risk identification and mitigation into the compliance pipeline by gating deployments through CI/CD-integrated verification and validation, ensuring 100% of code pushes pass compliance-detection accuracy checks before reaching production.
- Automated HIPAA 45 CFR §164 compliance monitoring through an in-house AI inference pipeline, continuously analyzing system activity to identify PHI leakage risks, compliance violations, audit evidence, and remediation opportunities
- Collaborate to maintain and troubleshoot application integrations across cloud infrastructure, PostgreSQL databases, and AI services, resolving API connectivity issues, synchronization failures, and system performance incidents

TaxCurb System

Dec 2025 - Apr 2026

Founder & Software Engineer

- Built real-time risk identification and mitigation into the compliance pipeline by gating deployments through CI/CD-integrated verification and validation, ensuring 100% of code pushes pass compliance-detection accuracy checks before reaching production.
- Designed backend system architecture using Node.js, Express, and Firebase Admin SDK with secure server-side credential isolation, token-based authentication, rate limiting, and structured input validation to ensure reliability and system robustness.
- Applied data-driven system analysis using funnel metrics (drop-off rates, validation errors, processing latency) to iteratively optimize workflow efficiency and reduce system uncertainty in user completion behavior.
- Conducted structured market and competitive analysis to model demand behavior and inform pricing strategy, onboarding design, and retention optimization.
- Built data pipelines to transform sparse, user-generated inputs into normalized, document-ready outputs, strengthening understanding of system representation learning under partially observed data environments.

Jodhpuri USA (Prev. Jodhpuri Inc.)

Aug 2023 - May 2026

Operations Manager | IT, Automation & Analytics

Chester, NJ

- Maintained SAGE MAS 200 ERP hosted on Windows Workstation, IIS web servers, and Microsoft SQL Server, troubleshooting application and user issues across order management, fulfillment, inventory control, and warehouse operations to ensure data accuracy and system reliability
- Configured and troubleshot SonicWall VPN, NetExtender, and Remote Desktop environments to support remote operations, coordinating 50+ vendors, carriers, and logistics partners across transportation, warehousing, and inventory management
- Analyzed operational data via ERP Crystal Reports, Excel, and Power BI to identify routing and fulfillment inefficiencies, improving delivery performance by 18% and reducing annual operating costs by \$40K+
- Managed end-to-end supply chain operations, coordinating overseas imports, customs documentation, Bills of Lading (BOL), container shipments, warehouses, carriers, and 3PL partners across order management, inventory control, fulfillment, transportation, and distribution workflows

Atlantic Health Systems

Jun 2025 - Aug 2025

ISS Summer Intern

- Configured, deployed, and troubleshot CrowdStrike-secured clinical endpoints, Epic Hyperspace workstations, IGEL OS devices, ensuring reliable access to mission-critical enterprise applications and healthcare systems.

- Managed asset provisioning, user access, and configuration records through Active Directory, CMDB, and ITSM platforms; executed SQL queries, generated operational reports, and supported enterprise application administration across clinical and business systems.
- Supported enterprise infrastructure and end-user operations through Citrix, NetMotion VPN, Microsoft Intune, Apple Business Manager, and Imprivata OneSign, troubleshooting remote access, authentication, device enrollment, and application connectivity issues

Nepal Economics Olympiad

Jan 2022 - Mar 2022

Intern

- Recovered and restored the organization's website following a security breach, performed full backups, and migrated the platform to a new hosting server with minimal downtime.
- Redesigned and customized the website, enhancing the user interface (UI), user experience (UX), and overall site functionality.
- Provided technical support for the International Economics Olympiad, assisting the organizing team with website administration, digital platforms, and event-related technical operations.

Fantech Gaming

Oct 2021 - Aug 2022

E-Commerce Developer

- Developed a full-stack eCommerce site on Adobe Magento for an Indonesian-Nepalese brand, hosted on Cent OS VPS, implemented CRM integration and Agile workflows, enabling the client to launch online sales and expand customer reach
- Integrated Google Analytics and Google Search Console into the site and collaborated with Indonesian developers and Agile sprints for QA, resulting in accurate traffic tracking and reduced post-launch bugs
- Migrated product and customer information from CSV files into the Magento database using MS Office 365 and MySQLserver, ensuring data integrity and enabling seamless order processing

Projects

Dell × NVIDIA AI Hackathon

Aug 2026

New York City

- Built a one-click installation platform for private AI inference and healthcare AI agents on NVIDIA GB10 hardware, running all models locally to meet on-prem/no-cloud requirements, using sandboxed OpenClaw/NemoClaw agents bounded by OpenShell to safely automate hospital operational workflows
- Secured hospital AI-agent operations through MCP-based tool boundaries, human approval gates, and MongoDB-backed audit events, preventing direct exposure of EHR and ServiceNow credentials while enabling controlled, traceable clinical and operational workflow execution
- Earned recognition from MongoDB and was featured by NVIDIA Healthcare AI on social media for innovation in private, secure hospital AI infrastructure and agent-based workflow automation

AI Native HIPAA Compliance Tool

Apr 2026

William Paterson University

Wayne, NJ

- 1. Built a full-stack compliance dashboard with AI-powered PHI detection across codebases and infrastructure, de-identification tooling using Safe Harbor and Expert Determination methods, and automated findings mapped to specific HIPAA citations and SOC 2 criteria
- Designed and implemented an RBAC system with 7 clinical roles, migrating a legacy Postgres enum to a text-based permission model with 32 row-level security (RLS) policies across all tables, row-level audit logging, and an email-based invite flow with automatic membership activation
- Engineered a PHI inventory system with automated scanner sync, risk scoring, retention policy enforcement, and one-click audit package PDF generation designed to satisfy OCR audit evidence requirements for enterprise health systems

Passaic360 www.passaic360.app

Feb 2026

Passaic County of NJ

Wayne, NJ

- Built a web and mobile platform for Passaic County serving 78,000+ SNAP recipients using Next.js, Node.js, TypeScript, and Express to automate work-hour compliance tracking across residents, organizations, and county administrators.
- Architected a distributed, multi-tier role-based system with strict backend authorization, ownership-validated API routes, JWT middleware, row-level database security, and audit logging to enforce least-privilege access across all platform workflows.
- Built a federal SNAP compliance system with automated document intelligence, multi-stage approval workflows, and AI-assisted anomaly detection across timesheet submissions, projected to reduce fraudulent claims and save Passaic County up to \$2M annually.

ComposeCache <https://www.npmjs.com/package/composecache>

Jan 2025

IEEE

- Designed and implemented a middleware caching framework for RAG pipelines that decomposes compositional queries into sub-queries, enabling partial cache hits and reducing redundant LLM API calls by 58.1%
- Built a dual-representation indexing system using SHA-256 hashes for exact-match and pgvector HNSW for approximate nearest-neighbor semantic lookup, reducing median end-to-end latency by 47.4%
- Implemented an uncertainty-gating mechanism using token-level entropy to block hallucinated responses from polluting the cache, achieving **94.1% hit precision** with answer F1 within 1.2 points of the no-cache baseline
- Released as a deployable npm package and Python SDK, integrating seamlessly into existing Node.js and Python RAG pipelines using the developer's own PostgreSQL + pgvector instance

Scanara AI [HackPrinceton](#)

Nov 2025

Princeton University

- Led the design and development of a multi-platform HIPAA audit tool (web app, CLI, and VS Code extension), enabling real-time compliance analysis for developers and security analyst.
- Built a HIPAA audit platform using Azure OpenAI (BAA), Firestore, and GitHub OAuth with rule-based scoring for deterministic results. Added severity tagging, file-level evidence extraction, and compact JSON reports for scalable multi-platform usage.
- Designed and executed security audit workflows to validate access controls, configuration integrity, and change impact, producing audit-ready documentation and repeatable findings aligned with HIPAA technical safeguards

Medkey

Nov 2025

- Designing and developing a HIPAA-compliant unified patient portal integrating Athena and Epic EHR systems via HL7 v2, FHIR, and SMART on FHIR APIs to aggregate and normalize 10+ categories of health data in real time
- Implementing secure authentication with OAuth 2.0, JWT, role-based access control, and AES-256/TLS encryption to ensure HIPAA-compliant protection of patient information
- Delivering a web and mobile platform that lets patients manage their identity and access their longitudinal health records while enabling providers to view consolidated clinical data in a single interface

Exo-Explorer NASA

2024

- Developed an AI-powered interactive web platform that visualizes real exoplanet data and integrates a conversational AI assistant to enhance astronomy education.
- Built full-stack architecture using React (frontend) and Node.js (backend), integrating NASA and Caltech exoplanet datasets to dynamically render 3D planetary exploration and system simulations.
- Implemented AI-driven story generation and question-answering features using OpenAI APIs to transform complex scientific data into accessible, structured educational narratives.
- Designed a scalable data pipeline to retrieve, normalize, and present astronomical datasets while maintaining real-time user interaction.
- Earned global nomination recognition at the NASA Space Apps Challenge for innovation in AI-assisted science education.

POS UML Design SWE Project

Jan 2025 - May 2025

- Designed a grocery-store POS system with role-based access (Cashier/Manager) and centralized database synchronization across 5 terminals.
- Implemented modular OOP architecture in C++ (Transaction, Inventory, Item, Customer, Cashier, Manager) with real-time inventory updates, coupon/loyalty logic, and multi-method payment processing.
- Modeled complete system architecture using UML (Use Case Diagrams, Class Diagrams, Communication Diagrams, Sequence Diagrams), formalizing transaction workflows, inventory management, loyalty logic, and administrative overrides.
- Applied software engineering lifecycle principles from requirements analysis through implementation and validation, simulating real-world enterprise system development.

ATS Automation

Aug 2025 - Dec 2025

William Paterson University

- Designed and implemented an integrated job application automation system combining a Chrome extension (“JobFiller”) with a cloud-backed web platform for real-time profile synchronization and ATS optimization.
- Developed an AI-powered keyword extraction engine using OpenAI APIs to analyze job descriptions and generate ATS-relevant skill recommendations for resume optimization.
- Architected real-time data synchronization using Firebase Authentication, Firestore listeners, secure token management, and smart caching to ensure low-latency, cross-device consistency.
- Implemented secure document management (resume/cover letter) with Firebase Storage and REST-based API integration compatible with Chrome Manifest V3 constraints.
- Evaluated system performance across multi-step application workflows, demonstrating reliable cross-platform consistency and efficient browser resource utilization.

Skills

- **Tech Stack:** HTML, CSS, C++, Python, SQL, Bootstrap, RestApi, Spring Boot, WordPress, Woo-commerce, Oracle, FireBase, Node JS, TypeScript, Next.js, llama.cpp
- **Technical Skills:** Web Development, Graphic Design, UI/UX Design, SEO, Google Admin/Gsuite, MS Office /365, Networking Technology, Google Analytics, Docker, Ngrok, 21 CFR 820.30, MS Excel, Supply Chain, Imaging, Artificial Intelligence, RAG, OOPS, LLMs, Software Engineering , HIPAA, AI Workflow Design, API Integration, Langchain, Project Management, Electronics Repair, ERP, FHIR, Design Control, Excel, FDA Regulatory, Technical Documentation, Risk Management, Verification & Validation, ISO 13485:2016, CI/CD, Evidence Collection, Systems Integration, Agile, Product Ownership, ITSM, Electronics Troubleshooting, Product Design, CRM, HL7
- **Tools:** Imprivata, XAMPP, Intunes, Jira, Cloudflare, MS Office, CherWell, Wagtail , PuTTY, Harness, Supabase, SAP, JAMA, Jenkins, n8n, Azure, SCCM, VMware, Zscaler, Slack, Claude, QuickBooks, SAGE MAS 200, Figma, Zapier, Confluence, Crystal Reports, Salesforce, ServiceNow, Openclaw, Nemoclaw, Openshell