Akshat Dharmesh Patel

AI Solutions & Systems Engineer | Secure Agentic AI & Automation

240-351-7070 | patelaksht24@gmail.com | linkedin.com/in/akshat-patel64 | akshatdpatel.com

Summary

AI Solutions & Systems Engineer who takes agentic AI from stakeholder discovery to systems staff use every day, on **AWS (Amazon Bedrock, Step Functions, Lambda)** and **Azure AI Foundry** with **Terraform** underneath. Built a sales-outreach engine with capacity for **1.6M personalized emails a year**, a contract review assistant that cut review from **hours to minutes**, and the single sign-on platform they run on. Security-first by design: compliance gates in code, evaluation benches, human approval, and least privilege (**OWASP Top 10 for LLM Applications, NIST AI RMF**). First-authored Springer Nature security research; AWS Certified Security – Specialty; former adjunct professor at the University of Maryland.

Technical Skills

AI Engineering & Agents	Generative AI (GenAI) and large language model (LLM) application development, agentic AI systems, Retrieval-Augmented Generation (RAG), prompt engineering, tool/function calling, Model Context Protocol (MCP), agent evaluation, guardrails, knowledge grounding, multi-model review, structured outputs, Amazon Bedrock, Azure AI Foundry hosted agents, Microsoft Fabric data agents, Microsoft Copilot Studio, AI workflow automation
Programming & Data	Python, TypeScript, SQL, PowerShell, Bash, FastAPI, React, Next.js, Pandas, REST APIs, Azure SQL, DynamoDB, data validation
Cloud & AI Infrastructure	AWS (Lambda, Step Functions, DynamoDB, SES, EventBridge, S3, VPC endpoints, IAM, KMS, CloudWatch, Secrets Manager), Azure (Container Apps, Entra ID, managed identities, Key Vault), serverless and event-driven architecture, Docker, Terraform, CI/CD with human-approved pipelines
MLOps / Observability	OpenTelemetry, Prometheus, Grafana, GitHub Actions, LLM response monitoring, tracing, alerting, rollback testing
AI Security & Governance	NIST AI RMF, OWASP Top 10 for LLM Applications, prompt-injection risk, threat modeling, software risk assessment, data-classification review, RBAC, least privilege, SSO/MFA, secrets management, Secure SDLC
Security Operations & Testing	Rapid7 InsightVM, Splunk, Security Onion, ELK Stack, CrowdStrike, Snort, Wireshark, vulnerability management, SIEM-aligned triage, endpoint security, Burp Suite, OWASP ZAP, Nmap, Metasploit, Nikto
Certifications	AWS Certified Security – Specialty, CompTIA Security+, AWS Certified Cloud Practitioner, ISC2 CC, Microsoft Azure AI Engineer Associate (in progress)

Experience

University of Maryland – Intercollegiate Athletics **College Park, MD**

AI Solutions & Systems Engineer **June 2026 – Present**

- Architected and built an **agentic sales-outreach engine** on serverless AWS (**Step Functions, Lambda, DynamoDB, SES, Amazon Bedrock, Terraform**) that turns cold, never-worked prospects into warm conversations and booked meetings, so a 7-person sales team can focus on premium fans and donors. Capacity for **1.6M personalized emails a year** at **80%+ lower running cost** than a comparable commercial product.
- Made the engine safe by construction: opt-outs, suppression, quiet hours, a price scan and a kill switch run **in code before any model**; replies are sorted into 7 kinds and pass **3 separate model calls** (classify, draft, review). Validated with **10,000+ simulated replies and conversations** against the live model.
- Built a **contract review assistant** on **Azure AI Foundry** that checks each vendor agreement against **80+ rules from 8 reference documents** and returns a report, a marked-up Word and PDF copy, and a draft vendor letter: **2–3 hours of manual review down to a 3.5-minute median**. Every quote is verified word for word in code (zero invented quotes).
- Designed the **staff app platform** for all **38 Athletics departments** (**FastAPI, React, Azure SQL, Entra ID**): one sign-in, department-scoped access re-checked on every request, a tamper-evident audit log, and a Terraform module that makes each new app a configuration change. Adopted as the team's standard pattern for staff web apps.
- Prototyped a **natural-language revenue analytics agent** (**Azure AI Foundry, Microsoft Fabric**) over **4.9M ticketing transactions** with per-user data access, and set the evaluation rule that an answer counts only when the query log proves a query ran.
- Built the **leadership project board** and the AI skill that keeps it current across 4 AI tools, so executives see every IT project on one page in plain language and approve what is waiting on them.

- Designing a **recruiting intake pipeline** for a varsity program handling **1,000+ recruit emails a year**: structured extraction, a single coach review queue, and an NCAA-compliant contact log.
- Built an AI-driven **dynamic pricing agent** in 3 weeks, replacing 2–3 hours of manual analysis with same-day executive pricing guidance, and launched an **IT software intake and AI procurement governance program** (triage rubric, questionnaire, SLAs).
- Authored executive **AI initiative** reporting delivered to **500+ Athletics staff** and the Athletic Director, with adoption growing to **6 departments opening AI discovery within 3 months**.

Sr. IT Security & AI Automation Specialist **July 2025 – June 2026**

- Built and deployed staff-facing **Microsoft Copilot Studio agents in Microsoft Teams**, translating departmental workflows into governed AI automations with reusable instructions, controlled data handling, and user-focused interaction design.
- Built a **tracking-link generator agent** for Marketing that standardized UTM campaign URL naming and reduced link creation time from **5–8 minutes to 1–2 minutes** per request.
- Ran **AI office hours** and discovery sessions across Marketing, Development, HR, Business, and Leadership, documenting **8+ AI use cases** and converting staff pain points into secure automation requirements, agent designs, and implementation plans.
- Led weekly **vulnerability management** reviews using **Rapid7 InsightVM** across **600+ endpoints, servers, and SaaS-connected systems**, performing exploit-based validation and false-positive triage while partnering with central IT security and vendors on remediation.
- Remediated a critical **Drupal core vulnerability (SA-CORE-2026-004) same day** on a Pantheon-hosted production site via Composer-based upgrade and staged Dev/Test/Live deployment, delivering a full remediation report to leadership.

Information Security & IT Support Intern **June 2024 – August 2024**

- Coordinated a **data inventory audit** across **500+ assets** and **50+ staff/vendors**, documented incidents using **NIST and MITRE ATT&CK** terminology, and delivered **4 security awareness newsletters** that improved suspicious-email reporting.

Adjunct Professor **September 2025 – December 2025**

University of Maryland, College of Information

- Taught **INST346 and INST464**, responsible for **200+ students** across two courses, after serving as a Graduate Teaching Assistant.

Cybersecurity Co-op | Detection Engineering & Secure Application Review **August 2022 – May 2023**

Dotsquares

- Engineered and deployed a **Snort-based IDS/IPS** on a live university network segment, tuning custom rules across **7+ attack categories** and achieving **95%+ detection and blocking coverage** in controlled attack-scenario testing, with a real-time dashboard over **1M+ daily captured packets**.
- Identified and helped remediate **30+ critical vulnerabilities** in a university e-governance platform, including SQL injection, XSS, authentication/session weaknesses, and input-validation flaws.

Security Researcher | Privacy-Preserving Cloud Search **July 2021 – August 2022**

Charotar University of Science and Technology

- Led a **13.5-month** research effort on privacy-preserving search over encrypted cloud data, comparing **SSE, PEKS, and proxy re-encryption** models; analyzed leakage risks (**index, search-pattern, and access-pattern leakage**, keyword-guessing, file-injection) and synthesized mitigations including **ORAM, PIR**, and secure indexing.
- First-authored a **Springer Nature** conference paper, *Privacy Challenges and Solutions in Implementing Searchable Encryption for Cloud Storage*, published in **ICTIS 2023 (LNNS Vol. 719)**.

Projects

MomentumEngine – Multi-Agent Market Research Desk | Python, SQLite, FastAPI, Next.js, LLM agents

- Designed and built a private multi-agent equities research desk: a deterministic screener narrows **4,500+ securities** a night, agent seats debate each candidate, and a **risk veto is enforced in code**. Every call is graded mechanically from later prices and a weekly review rewrites the rulebook (**63 rule changes, 245 logged hypothesis tests**), backed by **26.9M rows** of market data and **2.3M simulated exits**.

SecureScalr – Secure AWS Architecture | AWS, WAF, IAM, Cloud Security

- Designed and validated a secure multi-tier AWS e-commerce architecture (private EC2 tiers, ALB + Auto Scaling, Multi-AZ RDS, CloudFront-backed S3, **WAF, ACM, IAM, Secrets Manager**); sustained **55K+ JMeter requests** while blocking **1,500+** malicious requests.

Education & Honors

University of Maryland, College Park – Master of Engineering in Cybersecurity **August 2023 – May 2025**

Charotar University of Science and Technology – B.Tech in Electronics & Communication **July 2019 – May 2023**

10th place, AWS AI League – Amazon Bedrock AgentCore agent-building competition, AWS Summit DC **2026**