KUNAL JOSHI

(+91) 9602201321 | Mumbai, India | joshikunal16@gmail.com | linkedin.com/in/joshikunal16 | joshikunal.com

Cloud & AI Security Architecture | Enterprise Solutions | Governance & Automation

Cloud & AI Security Architect with 8+ years at AWS designing, securing, and delivering enterprise-grade systems end to end. Deep specialist in identity & access management and applied cryptography (KMS, CloudHSM, PKCS#11), with hands-on delivery for regulated financial customers, multinational banks, brokerages, and large lending institutions. Increasingly focused on **security for AI agent systems**, identity propagation, delegated authorization, and least-privilege for agentic and MCP architectures.

AREAS OF EXPERTISE

- AI & Agentic Systems Security
- Data Protection & Encryption
- Identity and Access Management
- AWS Security Architecture Design
- Cloud-Native SIEM / Security Operations
- Infrastructure as Code (IaC)

TECHNICAL PROFICIENCIES

Development: Python, Java, C/C++ | **IAM:** OAuth, SAML, AWS IAM, Identity Center, federation, SSO, JIT access | **Cryptography:** AWS KMS, CloudHSM, PKCS#11, JCE, OpenSSL dynamic engine, Encryption SDK | **AI / Agent Security:** agentic identity & delegated authorization (RFC 8693 token exchange), A2A & MCP authorization, Amazon Bedrock & AgentCore, secure RAG pipelines, LLM guardrails | **Security Operations:** Cloud SIEM/SOC (OpenSearch), threat hunting | **Cloud:** AWS security architecture & automation, IaC, CI/CD

HONORS & ACHIEVEMENTS

ACM ICPC 2016**-Kolkata finals Rank 58 | Qualified - Google Code Jam** (2017-18)
#2223 - Round 1 Code Jam (2017) **| AIR 98 - Tata Codevita** (2016)

EDUCATION & CERTIFICATES

B. Tech. in Computer Science, College of Technology and Engineering – Udaipur, India (2017)
Anthropic Claude Certified Architect | AWS Certified AI Practitioner | AWS Certified Security Specialty | AWS IAM SME | AWS CloudHSM SME | AWS KMS SME

PROFESSIONAL EXPERIENCE

CLOUD SECURITY ARCHITECT | Amazon Web Services – Mumbai, India **May 2024 – Present**

- **Led cloud security assessments for enterprise customers**, including pre-IPO firms, multinational banks, brokerages, and large private lending institutions, engaging CTOs and CISOs through steering sessions, assessment readouts, and prioritized remediation roadmaps.
- **Advise enterprise customers on securing GenAI and agentic workloads on AWS**, model access control, secure RAG pipelines, and identity/authorization patterns for agent architectures (Amazon Bedrock, AgentCore).
- **Transformed security requirements into robust AWS cloud architectures integrated with AWS security services** like AWS IAM (Identity and Access Management), KMS, CloudTrail, and GuardDuty to enhance threat intelligence and access control measures.
- Delivered projects to customers to strengthen their **Identity and Access Management (IAM) posture** by implementing IAM best practices, such as the principle of least privilege, multi-factor authentication, credential rotation, Single Sign-On through identity providers such as Azure AD/Okta, and Just-In-Time (JIT) access.
- **Engineered and implemented end-to-end AWS security solutions for enterprise customers,** ensuring compliance with cloud security principles and safeguarding sensitive financial data in accordance with Indian regulatory standards.
- **Architected and deployed robust security architecture and action plans,** fortifying AWS security pillars such as identity and access management, logging and monitoring, incident response, data protection, and infrastructure security.
- **Designed and executed scalable security solutions,** integrating automated least privilege policies, patch management, IaC pipelines, Cloud Native SIEM using OpenSearch, and security scanners to enhance compliance and threat mitigation across multiple customer environments.
- **Researching identity and authorization patterns for agentic AI systems**, on-behalf-of flows (RFC 8693), agent-to-agent trust, and applying least-privilege principles to autonomous agents and MCP-based tools.

CLOUD ENGINEER II – SECURITY | Amazon Web Services – Bangalore, India **Dec 2017 – May 2024**

- **Served as technical advisor to enterprise customers**, resolving complex issues across AWS security services, access control (IAM, Cognito, SSO), encryption management (KMS, CloudHSM), and threat detection (GuardDuty, Inspector).
- **Designed AWS security training frameworks** covering identity and access management, CloudHSM, Single Sign-On (SSO), and Secrets Manager, enabling internal teams to implement robust authentication and encryption strategies.
- **Recognized as a Subject Matter Expert in AWS IAM services,** providing deep expertise in Federation, SAML, and SSO implementations.
- Educated and empowered AWS clients by **publishing knowledge center content on IAM tag-based restrictions.**
- **Collaborated with cross-functional engineering teams to identify and fix SDK issues,** enhancing cross-language compatibility and improving performance across Python, Java, C++, C#, JavaScript, Ruby, Go, and PHP.
- **Expedited cloud adoption** by seamlessly onboarding **60+** applications into AWS Single Sign-On Cloud Application Catalog.
- **Served as a Cryptography Subject Matter Expert (SME), specializing in AWS KMS and CloudHSM,** resolving escalations and optimizing cryptographic operations using Java JCE, PKCS#11, and OpenSSL dynamic engine.

PROJECTS

Cloud Native SIEM and SOC (For a leading stock brokerage firm)

- Engineered and implemented Cloud native SIEM (Security Information and Event Management) using AWS OpenSearch.
- Developed custom Java log-processing pipeline handling structured and unstructured security data, with the complete system capable of processing 10+ million events per minute.
- Integrated public and privately subscribed threat intelligence with the log ingestion pipeline.
- Developed custom logic to integrate AWS Incident Manager with AWS OpenSearch for incident-case management and paging alerts.
- Achieved near real time alerting (from log generation) and visualization for log volume of ~1TB per day without downtimes.

KMS Key Policy – Least privilege orchestrator (For a leading multi-national bank)

- Engineered cloud-based solution to identify and remediate excessive cryptographic key privileges, supporting PCI-DSS and SOC 2 compliance.
- Developed analytics engine processing high-volume CloudTrail logs to identify key usage patterns and recommend least-privilege policies.
- Built automated GitHub integration with approval workflows to visualize, track, and audit policy changes across thousands of KMS keys.

IAM Policy - Least Privilege Orchestrator with Compliance Automation (For a leading multi-national bank)

- Engineered a full-stack IAM governance platform to identify and remediate excessive permissions for IAM users and roles across a complete AWS Organization, supporting SOC 2 and ISO 27001 compliance requirements, with an AWS CloudScape UI with role-based access control (RBAC) for security teams.
- Automated access reviews and entitlement management by analyzing organization-wide AWS CloudTrail logs to identify usage patterns and recommend least-privilege policies.
- Integrated SAML-based authentication with AWS Identity Center and implemented two-person-review (2PR) approval workflow for policy remediation, ensuring segregation of duties and audit trail compliance.
- Improved security posture by remediating excessive permissions for thousands of IAM users/roles across hundreds of AWS accounts, reducing attack surface.

AWS CloudHSM Key Management Dashboard (personal)

- Developed a dashboard to configure CloudHSM connections through a web interface and manage cryptographic keys with a clean UI.
- Supports creating AES, RSA, and EC keys, searching existing keys, and deleting keys when needed.
- Built with React on the frontend and FastAPI on the backend, using PyKCS11 to connect directly to CloudHSM cluster.
- https://github.com/joshikunal94/cloudhsm_management_dashboard