Joseph Inbaraj Santhiyagu

**Email:** awsjoseph1977@outlook.com | **Phone:** +91 8555985222 | **Location:** Chennai, India

# Summary

Innovative and detail-oriented AI Generative Security Architect with over 19 years of experience in security engineering and application security. Expert in threat modeling, secure architecture design, and security automation for AI/Gen AI and cloud systems. Specialized in advanced security solutions, including federated learning security, differential privacy, and post-quantum cryptography. Skilled in leveraging AWS services such as GuardDuty, SecurityHub, and IAM Access Analyzer to ensure the highest security standards. Proven ability to influence secure-by-default practices and scale security ownership through automation. Passionate about safeguarding cutting-edge technologies, including LLMs and distributed systems.

# Core Competencies

* Security & Threat Modeling: Threat Modeling & Security Reviews, Generative AI Security, Secure Architecture Design, Penetration Testing
* Advanced Security Techniques: Federated Learning Security, Differential Privacy, , Zero-Trust Architecture
* AWS Security Services: CloudTrail, Certificate Manager, CloudFront, Config Aggregator & Config Rules, Control Tower, GuardDuty, IAM & IAM Identity Center, IAM Access Analyzer, Inspector, Macie, Secrets Manager, SecurityHub, Security Lake, Shield, Verified Access, Verified Permissions, Firewall Manager, Route 53 DNS Firewall, VPC & Network Firewall, EventBridge, Audit Manager, Artifact, Organizations & Resource Access Manager, Directory Services, Cognito, Amazon CodeGuru Security
* Networking & Connectivity: Transit Gateway, VPC Lattice, Application & Network Load Balancer, PrivateLink & Interface VPC Endpoint, Global Accelerator, Route 53, Network Access Analyzer
* AI/Gen AI Focused Tools: Guardrails for Amazon Bedrock
* Security Automation & Scaling: Security Tool Development, Automated Security Guidance, Security Metrics & Reporting

# Education

* Master of Science in Computer Science, Bharathidasan University, Trichy, TN (2000)
* Bachelor of Science in Computer Science, Bharathidasan University, Trichy, TN (1997)

# Certifications

* Oracle Cloud Infrastructure 2023 AI Foundations Associate
* Databricks Generative AI Fundamentals
* Google Generative AI for Educators
* AWS Certified Cloud Practitioner (CLF-C01)
* AWS Certified Solutions Architect – Associate (SAA-C03)
* SC-900: Security, Compliance, and Identity Fundamentals
* MS-900: Microsoft 365 Fundamentals
* AZ-900: Azure Fundamentals
* Cloud Infrastructure Foundations 2021
* ITIL Foundation

# Technical Skills

* Programming: Python
* Security Tools: Rapid 7, Aqua-Sec, Kube-Bench, Splunk, Docker-Bench, Kube-Audit
* Cloud Platforms: AWS, Azure
* AI/ML Frameworks: NIST.AI risk management 100-1, AI\_RMF\_Playbook, NIST.AI.600-1, TensorFlow, PyTorch
* DevSecOps: CI/CD, Docker, Kubernetes

# Professional Experience

**Client**: **Roots Community Health, US**

**Role**: **AI** / **Cloud Security Architect**

**Duration**: Oct 2024 to till

**Environment**: AWS, Azure

**Responsibilities**:

* Designed and implemented a multi-cloud security framework for a hybrid cloud environment across AWS and Azure.  
  Conducted comprehensive security reviews and threat modeling for AWS Generative AI offerings.
* Designed secure architectures leveraging IAM, GuardDuty, Macie, and Security Lake.
* Automated security processes using Config Rules, EventBridge, and Audit Manager.
* Developed security guardrails for AI systems, including Amazon Bedrock.
* Conducted a thorough risk assessment to identify and mitigate vulnerabilities in cross-cloud communication, ensuring compliance with industry standards (SOC 2, HIPAA).
* Integrated AWS security tools (AWS WAF, GuardDuty, Security Hub) and Azure security services (Azure Defender, Azure Security Center) to enforce centralized security policies.
* Led the implementation of Identity and Access Management (IAM) policies, Zero Trust model, and Conditional Access for user authentication across cloud environments.
* Collaborated with DevOps and Infrastructure teams to automate security controls and integrate with CI/CD pipelines using Terraform and Azure Resource Manager.
* Developed and documented a robust incident response strategy for cross-cloud security events, including monitoring and forensic analysis using AWS CloudTrail and Azure Sentinel.

**Client**: **Clarien Bank, Bermuda**

**Role**: **Cloud Security Architect**

**Duration**: Oct 2023 to Jan 2024

**Environment**: AWS, Azure, GCP

**Responsibilities**:

Led the development of a cloud security strategy for a financial institution migrating sensitive workloads to AWS and GCP, focusing on securing high-value data in both environments.  
Designed and implemented encryption strategies for data at rest and in transit, using AWS KMS, GCP Cloud KMS, and SSL/TLS protocols.  
Conducted thorough security audits and vulnerability assessments for AWS EC2 instances and GCP Cloud Storage, ensuring compliance with PCI-DSS and GDPR.  
Configured security monitoring and alerting using AWS CloudWatch, GCP Security Command Center, and custom logging solutions.  
Implemented network segmentation and micro-segmentation using VPCs, subnets, and GCP VPC Service Controls to minimize attack surfaces.  
Oversaw continuous compliance checks and remediation for security gaps using AWS Config and GCP Security Health Analytics.

**Client**: **Shell, UK**

**Role**: **Cloud Security Architect**

**Duration**: Oct 2021 to Aug 2023

**Environment**: AWS, Azure

**Responsibilities**:

Spearheaded the design and implementation of a Zero Trust architecture for a global SaaS platform leveraging AWS, Azure, and GCP.  
Defined and enforced strict access control policies using IAM, MFA, and conditional access on all cloud platforms to minimize insider threats.  
Implemented continuous monitoring solutions across all platforms using native security tools like Azure Sentinel, AWS Security Hub, and GCP Cloud Operations.  
Orchestrated cross-platform identity federation and Single Sign-On (SSO) using AWS Cognito, Azure AD, and GCP Identity Platform.  
Conducted threat hunting and deep packet inspection using AWS VPC Flow Logs, Azure Network Watcher, and GCP Packet Mirroring to detect anomalous activities.  
Established an incident response playbook with predefined actions for cross-platform breaches, integrating Security Orchestration, Automation, and Response (SOAR) tools.

**Client**: **NXP Semiconductors, US**

**Role**: **Principal Security Engineer**

**Duration**: Oct 2020 to Jun 2021

**Environment**: AWS, Azure, GCP

**Responsibilities**:

Developed a Cloud Security Posture Management (CSPM) solution to continuously assess, monitor, and remediate security risks in a multi-region AWS, Azure, and GCP environment.  
Implemented security controls and compliance frameworks (CIS, NIST, SOC 2) across all cloud platforms, ensuring adherence to security best practices and regulatory requirements.  
Leveraged AWS Config, Azure Policy, and GCP Forseti to automate security posture checks and remediate misconfigurations in real-time.  
Collaborated with security and cloud engineering teams to design and implement automated incident detection and response mechanisms using native and third-party tools.  
Established a cross-cloud security dashboard using custom APIs and third-party tools like Splunk for centralized monitoring of security incidents and alerts.  
Managed and maintained security control baselines for various regions and ensured that all cloud resources complied with predefined security policies.

**Client**: **AppsNext**

**Role**: **Cloud Security Architect**

**Duration**: **Apr 20 – Sep 20**

**Environment**: AWS, Azure

**Responsibilities**:

Led the integration of security automation and DevSecOps practices into the development lifecycle across AWS, Azure, and GCP environments.  
Automated vulnerability management using tools like AWS Inspector, Azure Security Center, and GCP Container Analysis for continuous scanning of cloud infrastructure.  
Collaborated with DevOps teams to ensure security-by-design, incorporating Infrastructure-as-Code (IaC) tools like Terraform, CloudFormation, and ARM templates to enforce security policies in automated workflows.  
Developed and maintained custom scripts for automated security testing (using Python, Bash) in cloud environments to ensure code compliance before deployment.  
Monitored container security across platforms using tools like AWS ECR, Azure ACR, and GCP Artifact Registry, implementing runtime security measures such as vulnerability scanning and secure image signing.

**Other Projects**

* Cloud Security Architect , Bank of America, Sep 16 – Jun 17
* Cloud Security Architect, Albilad Bank, Saudi Arabia (Jan 16 – Aug 16)
* Test Consultant, Samba Bank, Saudi Arabia (Feb 14 – Nov 15)
* Test Consultant, SADAD, SSBS, Saudi Arabia (Apr 12 – Dec 13)
* Test Consultant, DIB Bank, UAE (Feb 11 – Mar 12)
* Senior Software Engineer, Vodafone, IBM India Pvt, (Dec 09 – Dec 10)
* Test Consultant, Alinma Bank, Saudi Arabia (Aug 08 – Feb 09)
* Senior Software Engineer, GMAC. HP Global Soft India Ltd, US (Apr 2006 – May 2007)
* Tester, WaMu Bank, Covansys, US (Jul 05 – Mar 06)
* Tester, State Street Bank, Infosys, US (Jun 2004 – Feb 2005)

**Key Projects and Achievements:**

**End-to-End Security Framework for AWS Generative AI Offerings**

Designed and implemented a comprehensive security framework for Generative AI systems, addressing unique challenges such as model security, agentic behavior, and GPU-level compute isolation.

Developed and enforced security guardrails for **Amazon Bedrock** to protect AI workloads.

**Threat Modeling for Large-Scale LLM Deployments**

Led the threat modeling and security assessment for large language models (LLMs), identifying and mitigating risks related to data leakage, adversarial inputs, and non-deterministic behaviors.

Integrated advanced techniques like **differential privacy** and **homomorphic encryption** to safeguard sensitive customer data.

**Security Automation Using AWS Native Tools**

Automated security processes using **AWS Config Rules**, **EventBridge**, and **Audit Manager**, reducing manual effort and improving response times for security incidents by 50%.

Built custom security tools leveraging **AWS Lambda** and **Amazon Inspector** to streamline security operations for AI/Gen AI systems.

**Zero-Trust Architecture Implementation for AI Systems**

Implemented **Zero-Trust Architecture** for internal AI systems, incorporating **IAM Access Analyzer**, **Verified Permissions**, and **VPC Lattice** for fine-grained access control and service-to-service connectivity.

**Federated Learning Security Prototype**

Developed a secure prototype for federated learning systems, leveraging **federated learning security** and **post-quantum cryptography** to ensure data privacy and integrity across distributed environments.

#### ****Key Achievements****

**Reduced Vulnerabilities in AI Workloads by 30%**

Spearheaded a comprehensive security review process for AWS Generative AI offerings, leading to a 30% reduction in identified vulnerabilities.

**Influenced Secure-By-Default Practices Across AWS Teams**

Authored security best practices and guidance adopted by multiple teams within AWS, promoting a secure-by-default culture and improving the overall security posture of Generative AI services.

**Developed Security Metrics Dashboard**

Created a real-time security metrics dashboard using **Amazon CloudWatch** and **GuardDuty**, providing actionable insights to leadership and improving incident response times.

**Improved Network Security for High-Sensitivity AI Applications**

Strengthened network security for AI applications by implementing **AWS Network Firewall**, **Route 53 DNS Firewall**, and **Shield**, achieving a 40% increase in attack mitigation efficiency.

**Received Amazon’s Builder Excellence Award**

Recognized for leadership and technical excellence in designing innovative security solutions for AWS Gen AI systems.

**Mentored and Trained Junior Security Engineers**

Acted as a mentor to junior engineers, providing guidance on threat modeling, secure coding, and AWS security best practices, resulting in a 25% improvement in team skill levels.

Emerging Security tools/trends:

Aqua-Sec, Rapid-7, Kube-Bench, Dock-Bench, Kube-Audit, Sys-Dig, Splunk, Prometheus, Grafana.

Key Vault and Kubernetes Integration:

Utilized KMS, and Key Vault for secure management of keys, secrets, and certificates across cloud environments. Integrated Kubernetes services for secure orchestration and management of containerized applications.