Vamshidhar Reddy Vemula

Cloud Security Architect

Mobile: +14302521472 **Email: vvamshidharreddy1@gmail.com**

PROFESSIONAL SUMMARY:

Accomplished Security Architect and Cloud Engineer with over 10+ years of progressive experience designing, building, and securing scalable enterprise applications and cloud-native architectures. Proven expertise in full-stack development, security engineering, microservices, and secure DevOps pipelines. Published researcher in AI, Cloud Security, and Blockchain technologies with approved patents. Recognized for leadership in cloud security innovations, contributions to the cybersecurity community, and mentoring the next generation of technologists. Committed to advancing security architecture standards and industry best practices.

AREAS OF EXPERTISE:

Cloud-Native Architecture & AI Infrastructure: Designing and securing scalable microservices on AWS, with emphasis on IAM, OAuth2, and Zero Trust principles.

AI and Cloud Security Innovation: Developing AI-driven threat detection frameworks, secure migration tools, and blockchain-based verification systems.

DevSecOps and Secure SDLC: Implementing security best practices across CI/CD pipelines using Jenkins, SonarQube, Docker, and Kubernetes.

Research and Intellectual Property: Authoring research publications on cloud security, AI, and blockchain; contributing to patent filings in cybersecurity innovation.

Platform Modernization and Enterprise Transformation: Driving cloud-first initiatives, microservices modernization, and platform resiliency strategies.

Leadership and Community Contributions: Mentoring emerging engineers, peer-reviewing research, judging hackathons, and promoting cybersecurity awareness.

RESEARCH EXPERIENCE:

"AI-Enhanced Self-Healing Cloud Architectures for Data Integrity, Privacy, and Sustainable Learning"
Published in IGI Global, 2025
"Integrating Green Infrastructure With AI-Driven Dynamic Workload Optimization for Sustainable Cloud Computing"
Published in IGI Global, 2024
"Intelligent Security Scheme for Backdoor Attacks in High Speed Heterogeneous Communication Network"
Published in IEEE, 2024
"AI-Powered Leadership: Shaping the Future of Management"
Published in IGI Global, 2024
"Cognitive Artificial Intelligence Systems for Proactive Threat Hunting in AI-Driven Cloud Applications"
Published in AVE Trends in Intelligent Computing Systems, 2024

"AI in Performance Management: Data-Driven Approaches"
Published in IGI Global, 2024
"Recent Advancements in Cloud Security Using Performance Technologies and Techniques"
Published in IEEE, 2023
"Privacy-Preserving Techniques for Secure Data Sharing in Cloud Environments"
Published in IEEE, 2023
"Multi-Cloud Security Orchestration Using Deep Reinforcement Learning"
Published in International Journal of Professional Studies, 2023
"Adaptive Threat Detection in DevOps: Leveraging Machine Learning for Real-Time Security Monitoring"
Published in International Machine Learning Journal and Computer Engineering, 2022
"Integrating Zero Trust Architecture in DevOps Pipeline: Enhancing Security in Continuous Delivery Environments"
Published in Transactions on Latest Trends in IOT, 2022
"Blockchain Beyond Cryptocurrencies: Securing IoT Networks with Decentralized Protocols"
Published in International Journal of Interdisciplinary Finance Insights, 2022
"Mitigating Insider Threats through Behavioural Analytics and Cybersecurity Policies"
Published in International Meridian Journal, 2021
"Blockchain-Enabled Secure Access Control Frameworks for IoT Networks"
Published in International Numeric Journal of Machine Learning and Robots, 2020

PATENTS:

Artificial Intelligence Based Cloud Data Security Detector
409867-001. Issued Aug 3, 2024

A Cloud computing based digital forensic investigation system implemented with ML configurations
GUMBLIIP2023/205. Issued Oct 16, 2023

PROFESSIONAL EXPERIENCE:

Wells Fargo, Phoenix, AZ. Sep 2021 – Present

Principle Engineer – Cloud Security
Project: Part of Strategic Services & Advanced Technology (SSAT) division with the goal of Technology Simplification and Transformation. Leading the migration of Wells Fargo's Enterprise Content Management API Platform to cloud-native microservices on the private cloud. Focused on cloud security architecture, API Gateway integration, and platform hardening for critical banking applications.

Responsibilities:

- Designed and implemented secure API routing strategies, enabling direct traffic flows from API Gateway to PCF-based microservices.
- Architected secure routing strategies, enabling API Gateway (Apigee Edge) to securely expose microservices deployed on PCF (Pivotal Cloud Foundry).
- Developed hardened authentication modules using JWT and signed URL mechanisms, safeguarding API communications against token spoofing and replay attacks.
- Integrated HARD-ROCK mTLS (mutual TLS) authentication across cloud microservices, enhancing platform-wide secure handshake protocols.
- Designed and implemented dynamic service discovery mechanisms, leveraging Eureka service registry and Apigee proxies.

- Built automated CI/CD pipelines (Jenkins) integrating SonarQube static code analysis, containerization with Docker, and security validation.
- Conducted API traffic analysis, incident tracebacks, and anomaly detection using Apigee's Trace and API Analytics tools.
- Spearheaded secure microservice development using Spring Boot, enforcing secure coding standards aligned with OWASP Top 10.
- Drove adoption of centralized logging and monitoring frameworks using Redis and Cloud Watch, improving threat detection SLAs by 40%.
- Mentored development teams on secure SDLC practices, achieving 30% reduction in vulnerabilities during release audits.

Salesforce, Denver, CO. Jan 2021 – Sep 2021

Cloud Platform Engineer

Project: Led modernization of Salesforce's philanthropic B2B/B2C platform, building a global donation, volunteering, and campaign application suite using secure cloud-native architectures on AWS.

Responsibilities:

- Designed and deployed Spring Boot microservices integrated with AWS native services, enhancing platform resiliency, security, and scalability.
- Implemented secure OAuth2 authentication and session management for NGO onboarding, donation workflows, and volunteer engagement APIs.
- Built and maintained scalable RESTful API ecosystems documented via Swagger/OpenAPI, enabling secure partner and mobile integrations.
- Established CI/CD pipelines using Jenkins and AWS CodePipeline for fully automated, secure deployments.
- Integrated centralized monitoring and alerting using AWS CloudWatch, improving MTTR (mean time to recovery) for cloud services.
- Enabled secure front-end development using Angular 8, ensuring CSRF/XSS protections and secure data exchanges via REST APIs.
- Designed dynamic routing components in AngularJS with token-based API calls to backend microservices.
- Developed cost optimization strategies for AWS workloads, reducing overall cloud infrastructure spend by 22%.
- Contributed to system hardening efforts including API rate limiting, DDoS mitigation, and encrypted data-in-transit standards.

US BANK, Denver, CO. Feb 2019 – Dec 2020

Cloud Security and Operations Engineer

Project: Modernized US Bank's financial services infrastructure, focusing on secure cloud migration, microservices transformation, and DevOps pipeline hardening for mortgage, investment, and consumer banking applications.

Responsibilities:

- Led migration from legacy monolithic systems to secure, containerized microservices deployed on PCF (Pivotal Cloud Foundry) and AWS environments.
- Implemented security controls in microservices architecture including OAuth2-based secure API interactions, encryption in transit (SSL/TLS), and role-based access control (RBAC).
- Designed and configured centralized security logging and real-time monitoring using Splunk and AWS Cloud-Watch for production workloads.
- Built secure CI/CD pipelines using Jenkins integrated with SonarQube for automated vulnerability scanning and compliance checks.
- Architected cloud deployment blueprints ensuring adherence to PCI DSS, SOX, and internal InfoSec standards.
- Led API Gateway integration projects using Apigee for secure external API exposure with token-based authentication, rate-limiting, and threat protection policies.
- Conducted security audits and patching across containerized workloads reducing vulnerability exposure window by 40%.
- Implemented database encryption strategies and data masking for personally identifiable information (PII) compliance.

HortonWorks/Cloudera, Sunnyvale, CA. Nov 2017 – Jan 2019

Cloud Platform Engineer – Big Data Security & Modernization

Responsibilities:

- Built and secured enterprise-scale Hadoop Data Lakes integrating Spark Streaming, Kafka, HDFS, and AWS S3 storage.
- Deployed scalable cloud infrastructure using AWS EC2 instances, configuring IAM roles, VPCs, and security groups for fine-grained access control.
- Implemented strong authentication mechanisms (Kerberos, LDAP integration) for secured Hadoop ecosystem services.
- Developed data ingestion pipelines with Apache NiFi ensuring secure, encrypted, real-time data movement.
- Automated big data cluster deployments using Ansible playbooks and infrastructure-as-code principles.
- Led initiatives to encrypt sensitive datasets at rest and in transit using AWS KMS and SSL configurations.
- Designed Cross-Cloud VPN tunnels between on-premise networks and AWS for secure hybrid deployments.
- Conducted penetration testing and vulnerability scanning across big data clusters to ensure compliance with HIPAA regulations.

Yana Software Pvt Ltd, Hyderabad, IN. Jan 2016 – Oct 2017

Cloud Engineer

Responsibilities:

- Assisted in migration of legacy web applications to cloud-native, containerized deployments using Docker.
- Developed secure backend services using Spring MVC, integrating encryption modules for sensitive customer data handling.

- Automated build and deployment pipelines using Maven, Jenkins, and Git, adhering to secure DevOps practices.
- Worked on configuring SSL for secure web services communications and database connections.
- Conducted daily vulnerability assessments and remediated high-severity issues as part of DevSecOps tasks.

PRAVA Realty Management, Bangalore, IN. Aug 2012 – Dec 2015
Cloud Security Intern

Responsibilities:

- Designed and developed RESTful APIs with secure token-based authentication to enable seamless customer interactions.
- Integrated AJAX, JSON, and REST services ensuring encrypted, secure data exchanges with backend systems.
- Built automation scripts to ingest customer billing data into secured MySQL databases.
- Developed monitoring dashboards for call center applications using open-source tools and integrated early anomaly detection systems.
- Supported cloud migration projects by analyzing and documenting security configurations and access controls.

EDUCATION:

- **Master Of Science in Computer Science**

  Texas A&M University – Commerce, Texas, USA June 2018 – May 2020

- **Bachelor of Technology – Electronics and Communication Engineering**

  Jawaharlal Nehru Technological University, Hyderabad Aug 2012 – June 2016

AWARDS & RECOGNITION:

GLOBEE AWARDS FOR CYBERSECURITY – 2025
Bronze Globee Winner for AI-Driven Threat Detection

TITAN INNOVATION AWARDS – 2024
Gold Winner for Best Artificial Intelligence Technology Innovation

VOLUNTEERING:

- Distinguished Jury Member – Claro Awards
- Peer Reviewer – IEEE
- Reviewer for NCWIT Aspirations in Computing Applications – NCWIT
- Judge – Future City Competitions
- Peer Reviewer – IGI Global Scientific Publishing