Monika Uppalapati | IAM Engineer

4697011818 | m.uppalapati02@gmail.com

PROFESSIONAL SUMMARY

- IAM Solutions: Proficiency in implementing and managing IAM solutions such as Okta, Microsoft Entra ID (Azure AD), and AWS IAM.
- Authorization Mechanisms: Strong understanding of authorization mechanisms such as RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), and PBAC (Policy-Based Access Control).
- Migration of identities and SSO application from Okta to Microsoft Entra ID (Azure AD).
- Led initiatives to enforce secure coding practices, including input validation, output encoding, and parameterized queries, across development teams. Conducted code reviews and guided to ensure adherence to OWASP Top 10 security principles, resulting in a significant reduction in vulnerabilities and improved overall application security posture.
- Implemented end-to-end Identity and Access Management (IAM) lifecycle management solutions to streamline user provisioning, de-provisioning, and access governance processes. Utilized Azure Active Directory (Azure AD) features such as user lifecycle policies, group-based access controls, and automated provisioning/de-provisioning workflows to ensure efficient management of user identities and access rights across Azure-hosted applications.
- Collaborated with stakeholders to gather requirements, design IAM workflows, and customize SailPoint IdentityIQ to meet specific business needs and security policies.
- Integrated SailPoint IdentityIQ with diverse enterprise systems, including HR systems, Active Directory, and cloud applications, to establish a centralized identity governance framework.
- Developed custom connectors and workflows in SailPoint IdentityIQ to automate user provisioning, de-provisioning, and access recertification processes, reducing manual effort and minimizing security risks.
- Directory Services: Experience with directory services like Active Directory, LDAP, and Lightweight Directory Access Protocol (LDAP).
- Identity Governance and Administration (IGA): Managed user lifecycle management, access certification, and role management with SailPoint IdentityIQ.
- Privileged Identity Management: Administered Azure Privileged Identity Management (PIM) to enhance security by managing, controlling, and monitoring access to critical resources.
- Single Sign-On (SAML & OpenIDConnect): Expertise in implementing SSO solutions to streamline user authentication across multiple applications.
- Multi-Factor Authentication (MFA): Understanding of MFA techniques to enhance security by requiring multiple forms of verification for user authentication.
- Identity Federation: Experience in setting up identity federation to enable single sign-on across multiple domains or organizations.
- Security Standards and Compliance: Knowledge of security standards such as ISO 27001, NIST, GDPR, HIPAA, and regulatory compliance requirements related to IAM.

TECHNICAL SKILLS

IAM	**Microsoft Entra ID (Azure AD), Okta, AWS IAM & SSO,**
Amazon Web Services	**CloudWatch, Cloud Formation, IAM, IAM Identity Center**
IGA	**SailPoint IdentityIQ**
Scripting	**PowerShell, Python**
Visualization Tool	**Tableau and Power BI**
Methodologies	**Agile, Scrum, and SDLC**
Languages	**Java, HTML, CSS.**
On-Prem	**Active Directory**

WORK EXPERIENCE

Western Reserve Group, USA **April 2023 – Present**
IAM Engineer

As an IAM (Identity and Access Management) Engineer at Western Reserve Group, my responsibilities include:

- IAM Solution Design: Designing IAM solutions tailored to Western Reserve Group's business needs, considering factors such as scalability, security, and compliance.
- Implementation and Configuration: Implementing IAM solutions such as Okta, and Microsoft Entra ID(Azure AD) configuring user directories, authentication mechanisms, and access controls.
- Identity Lifecycle Management: Developing and maintaining processes for user provisioning, de-provisioning, and access certifications to ensure timely and accurate management of user identities with SailPoint IdentityIQ.
- Access Control Management: Defining and enforcing access control policies, including role-based access control (RBAC) based on least privilege principles.
- Privileged Identity Management: Administered Azure Privileged Identity Management (PIM) to enhance security by managing, controlling, and monitoring access to critical resources.
- Single Sign-On (SSO) Integration: Integrating SSO solutions based on SAML and OpenIDConnect to streamline user authentication across Western Reserve Group's applications and systems, enhancing user experience and security.
- Multi-Factor Authentication (MFA): Implementing Azure MFA solutions to strengthen authentication mechanisms and protect against unauthorized access to sensitive resources.
- Governance: Created and launched access certifications, application onboarding, and approval automation using SailPoint IdentityIQ.
- Incident Response and Troubleshooting: Collaborating with the security team to investigate and respond to security incidents related to identity and access controls, implementing corrective measures to prevent future incidents.
- Continuous Improvement: Staying updated on emerging IAM technologies, best practices, and security threats, proactively identifying opportunities to enhance Western Reserve Group's IAM posture.
- Automation: Automated Entra ID management tasks using PowerShell and Python to enhance efficiency and streamline identity management processes.

Amazon, USA **July 2022 - March 2023**
IAM Engineer

- Contributed significantly to a dedicated team tasked with architecting a Warehouse Management System for Distribution Center Technologies (DCT).
- IAM Solution Architecture: Designing and architecting IAM solutions that meet the unique requirements and scale of Amazon's diverse business units and services.
- IAM Service Implementation: Implementing and configuring IAM services such as AWS IAM, AWS Single Sign-On (SSO), and other identity services to manage access to Amazon's vast array of cloud services and resources.
- Access Control Policies: Developing permission sets, role-based access control (RBAC), resource-based policies, and Service control policies to ensure least privilege access across Amazon's cloud infrastructure.
- Compliance and Governance: Ensuring that IAM solutions adhere to regulatory compliance requirements such as GDPR, PCI DSS, HIPAA, and industry best practices, and implementing governance processes for access management.
- Identity Lifecycle Management: Developing and maintaining processes for user provisioning, de-provisioning, and access review to manage the entire identity lifecycle effectively.
- Incident Response and Security Monitoring: Collaborating with Amazon's security teams to detect and respond to security incidents related to identity and access controls, and implementing preventive measures to mitigate future risks.
- IAM Automation and Scalability: Leveraging automation tools and scripts to streamline IAM processes and ensure scalability to support Amazon's dynamic and rapidly growing environment.
- Continuous Improvement and Innovation: Staying abreast of emerging IAM technologies and industry trends, and driving continuous improvement and innovation in IAM solutions to enhance security, efficiency, and user experience at Amazon.

Cyient, USA **September 2021 - May 2022**
IAM Intern

- IAM Solution Design: Collaborating with stakeholders to understand business requirements and designing IAM solutions tailored to Cyient's needs, considering scalability, security, and usability.
- Implementation and Integration: Implementing IAM solutions and integrating them with Cyient's existing IT systems, applications, and cloud services to ensure seamless identity and access management across the organization.
- Access Control Policies: Developing and enforcing access control policies, including role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access controls to manage user access to Cyient's resources.
- User Lifecycle Management: Establishing processes for user provisioning, de-provisioning, and access review to efficiently manage the entire identity lifecycle and ensure compliance with regulatory requirements.
- Single Sign-On (SSO): Implementing SSO solutions to simplify user authentication and improve user experience by enabling seamless access to multiple applications and services with a single set of credentials.
- Multi-Factor Authentication (MFA): Implementing MFA solutions to enhance security by requiring additional authentication factors beyond passwords, such as biometrics or OTPs, for accessing sensitive systems and data.

- Privileged Access Management (PAM): Managing and securing privileged accounts and access to critical systems and resources through PAM solutions to minimize the risk of insider threats and unauthorized access.
- Identity Federation: Establishing federated identity relationships with external partners, clients, and service providers to enable secure and seamless access to shared resources and applications.
- Compliance and Governance: Ensuring that IAM solutions comply with industry regulations, standards, and Cyient's internal policies, and implementing governance processes for access management and auditability.
- Incident Response and Security Monitoring: Collaborating with Cyient's security team to detect and respond to security incidents related to identity and access controls, and implementing measures to prevent future incidents.
- IAM Automation: Developing automation scripts and workflows to streamline IAM processes such as user provisioning, access requests, and access revocation, improving operational efficiency and reducing manual effort.
- Training and Documentation: Providing training sessions and creating documentation to educate Cyient employees and stakeholders on IAM best practices, security policies, and procedures.
- Continuous Improvement: Staying updated on emerging IAM technologies, industry trends, and security threats, and driving continuous improvement initiatives to enhance Cyient's IAM posture and security resilience.

TCS, India **April 2019 - Dec 2020**
IAM Engineer

- IAM Solution Design and Architecture: Collaborating with clients to understand their business requirements and designing IAM solutions that align with their strategic goals, considering factors such as scalability, security, and regulatory compliance.
- Access Control and Policy Management: Developing access control policies and mechanisms, including role-based access control (RBAC), on Azure RBAC and Microsoft Entra ID (Azure AD) RBAC.
- Single Sign-On (SSO) Integration: Integrating SSO (SAML & OpenIDConnect)solutions to provide users with seamless access to multiple applications and services using a single set of credentials, improving user experience and productivity using Enterprise applications and App registrations.
- Multi-Factor Authentication (MFA): Implementing Azure MFA solutions to enhance security by requiring additional authentication factors on user accounts and applications using conditional access policies.
- Privileged Access Management (PAM): Managing and securing privileged accounts and access to critical systems and resources through PAM solutions, enforcing least privilege principles, and monitoring privileged activities for compliance and security.
- Identity Federation and External Collaboration: Establishing federated identity relationships with external partners, clients, and service providers to enable secure and seamless access to shared resources and applications across organizational boundaries.
- Compliance and Governance: Ensuring that IAM solutions comply with industry regulations, standards, and client-specific policies, and implementing governance processes for access management, auditing, and reporting.
- Incident Response and Security Monitoring: Collaborating with TCS's security operations center (SOC) to detect and respond to security incidents related to identity and access controls, and implementing measures to prevent future incidents.
- IAM Automation and Orchestration: Developing automation scripts, workflows, and integration connectors to streamline IAM processes such as user provisioning, access requests, and access revocation, improving operational efficiency and reducing manual effort.
- Training and Knowledge Sharing: Providing training sessions, workshops, and documentation to educate TCS employees and clients on IAM best practices, security policies, and procedures, promoting awareness and adherence to IAM guidelines.

Syllogistic Systems, India **May 2018 - July 2018**
Software Developer Intern

- Assessed extensively on Spring Boot for building web services. Deployed MAVEN to automate builds and manage projects.
- Developed applications using Spring, JSP, and AJAX on the presentation layer. The business layer is built using Spring, and the persistent layer uses Hibernate.
- Designed, implemented, and tested the Spring Domain Model for the services using Core Java.
- Configured and deployed the J2EE application on the WebLogic Application Server.
- Developed the backend server with Spring Boot, involving different application layers, including entity/model, DAO/repository, Controller, Service, Business, and Persistence.
- Responsible for implementing new enhancements and fixing defects using Java, JSP, Spring, and Hibernate.
- Performed and participated in code reviews, application builds, CI/CD pipelines, unit test plans, automated builds, and release definitions.
- Provide a radically faster and widely accessible getting-started experience for all spring development by using spring boot.

- Designed and developed web-based modules using Java Servlets and JSP.
- Developed Spring Beans and configured spring using the application Context.xml.
- Implemented user interface guidelines and standards throughout the development and maintenance of the website using JavaScript, jQuery, React.JS, CSS, and HTML.
- Designed Dynamic client-side JavaScript codes to build web forms and simulate processes for web applications, page navigation, and form validation.
- Developed a Single Page Web Application with React.js, Redux, Node.js, REST API, and MongoDB.
- Involved in all stages of the Software Development Life Cycle (SDLC), like application design, development, debugging, and application testing.

EDUCATION

Master of Science: Business Analytics, **Jan 2021 – May 2022**

Texas A&M University, TX

Bachelor of Technology: Computer Science and Engineering, **June 2015 – April 2019**

GITAM University, India