PATTNAM SHAHID

shahidpattnam123@gmail.com | 8555861805 | www.linkedin.com/in/shahid-pattnam

CAREER OBJECTIVE:

To leverage foundational knowledge of Microsoft Azure services in designing and managing cloud solutions, while continuously learning advanced networking, security, and automation practices to contribute to organizational growth.

EDUCATIONAL QUALIFICATIONS:

Bachelor of technology (Mechanical Engineering) | (2023)
•CGPA:6.5.
Diploma (Mechanical Engineering) | (2019)
• CGPA:7.25.
School Secondary Certificate (SSC)| (2016)
• CGPA:7.3.

TECHNICAL SKILLS:

- **Cloud Platforms:** Microsoft Azure, Azure Virtual Machines (VMs), Azure Storage, Network Security Groups (NSG), Azure Load Balancer, Azure Application Gateway, Azure Active Directory (Azure AD), Azure SQL Database, Azure Backup, Recovery Services Vault, Azure CLI, Azure PowerShell, Azure App Services, Azure Monitor, Azure Key, Vault, Azure Resource Manager (ARM), Azure Regions & Availability Zones
- **Operating Systems:** Basics of Linux. Windows
- **Monitoring Tools:** Azure Monitor.
- **Version Control:** Git, GitHub.
- **Orchestration:** Kubernetes(Beginner)

PROJECTS:

1.**Title: 3-Tier Architecture NSG**

Tools: Azure Networking Services, Infrastructure & Networking, Compute & Operating System.

Description: Deployed Azure Network Security Groups (NSGs) in a 3-tier architecture (web, application, database) to enforce secure and segmented traffic flow. Configured custom NSG rules to control inbound and outbound traffic across each tier, reducing unauthorized access and enhancing data isolation. Achieved a 40% improvement in network performance and security reliability.

Responsibilities:

• **Understanding Azure NSG Concepts:** Learn about Azure Network Security Groups, their role in managing and filtering network traffic.

• **Researching 3-Tier Architecture**: Gain an understanding of the 3-tier architecture (web, application, and database layers) and how NSGs apply security policies to each tier.

• **Configuring NSG Rules:** Assist in configuring NSG rules to control inbound and outbound traffic for each tier (web, application, database).

•**learning Security Best Practices**: Gain knowledge on best practices for securing network traffic in Azure environments, including the principle of least privilege, segmentation, and multi-layer security.

2.**Title:** 2-Tier Web Application Architecture on Microsoft Azure.

Tools: Azure Virtual Network, NSGs, Load Balancer (Public & Private), Linux VMs, Nginx, Tomcat.

Description: Designed and deployed a secure and scalable 2-tier cloud architecture on Microsoft Azure, consisting of Web, App, and DB servers. The project implemented public and private load balancers to manage external and internal traffic, ensuring high availability, resilience, and controlled access. Infrastructure was automated using Terraform/ARM templates, with Linux VMs hosting Nginx (Web tier) and Apache Tomcat (App tier) for application delivery.

Responsibilities:

- Architected and implemented a 2-tier infrastructure with Web, App, and DB servers on Azure.
- Configured Virtual Network (VNet) with segmented subnets (web, app, load balancer) for secure traffic flow.
- Deployed Linux VMs and installed Nginx and Apache Tomcat to host web and application services.
- Set up Public Load Balancer for external traffic distribution and Private Load Balancer for internal tier communication.
- Applied Network Security Groups (NSGs) and routing rules to enforce access control and secure communication.