Mrugesh Patel, M.Sc.

mrugeshpatelb@gmail.com
(312) 998-3515
LinkedIn

Network Engineering
Cisco Meraki, ASA, and Palo Alto Automation Expert

Performance-focused and highly analytical professional with remarkable expertise in managing, maintaining, and updating various networks, routers, as well as switches to ensure maximum security and performance. Top strengths in Palo Alto, Cisco ASA, and Meraki SD-WAN. Documented history in firewall management and several router / switch technologies, including Meraki SD-WAN and Palo Alto. Proven expertise in utilising Python to manage and automate Palo Alto firewall and Cisco Meraki SD-WANoperations, while using F5 Load Balancer and network scripting. Strong knowledge of Palo Alto, Juniper, Checkpoint, Cisco ASA and Meraki SD-WAN, and F5 ASM Firewall. Known problem-solver; capable of conducting in-depth analyses, determining root causes, and eliminating complex issues that impact network capabilities. Exceptional leadership and management skills with ability to train internal teams and deliver projects for improving corporate network services, implementing new capabilities, and remediating problem areas.

- Expert at driving smooth migration and upgrade of complex wireless platforms from old legacy firmware to new, latest technology for faster connectivity and performance.
- Dedicated to providing high-level technical support to end users in resolving network issues to attain full satisfaction.
- Passionate for creating change record in various ticketing systems for service requests to enable successful firewall policy changes.
- Detail-oriented individual; adept at developing new VPN tunnels to vendor and remote networks for succesful transfer of sensitive, confidential, and encrypted data over WAN connections.

Technical Proficiencies

Languages:	Java, Python
Tools:	F5 Load Balancer, Web Proxy, Microsoft Word and Excel, Adobe PDF, Dynovis Proprietary Quality Control Tools, MS Visual Studio 2012, MySQL,DNS, Netblox, Observioum, Splunk, EVE-NG, Putty, SecureCRT, ServiceNOW, Visio, Terraform.
Hardware:	Cisco Routers and Switches, Cisco Meraki, Automation Palo Alto Firewall and Meraki SD-WAN, DNS Server,F5 LTM, GTM, ASM, WAF, Cisco ASA, Checkpoint, Riverbed, Cisco SDWAN, Viptela, VeloCloud, Aruba SDWAN, Juniper.

Career Experience

Camping World- Chicago, IL **Dec 2023- Current**
Sr Network Security Engineer
Technical Scope: Firewall, AVI Load Balancer, NSX Networking, Azure Cloud Networking

Experienced Network Security Engineer with a strong track record in designing and deploying Palo Alto firewall solutions, implementing secure network segmentation strategies, and optimizing firewall performance. Skilled in monitoring network traffic, troubleshooting complex issues, and conducting thorough security assessments. Proficient in NSX, AVI, and Global Protect deployments, with hands-on expertise in automation, documentation, and compliance. Adept at mentoring junior engineers and staying current with evolving security trends to enhance organizational security posture.

- Design and deploy Palo Alto firewall solutions to protect network infrastructure against emerging security threats.
- Develop and implement firewall policies, rules, and configurations to maintain network security and ensure compliance with industry standards.
- Assist in developing a segmentation strategy to ensure security and compliance for the business while avoiding disruption to operations.
- Perform firewall capacity planning and optimization to meet the organization's evolving needs.
- Monitor and analyze network traffic to identify and mitigate security vulnerabilities and incidents.
- Troubleshoot complex firewall issues, collaborating with cross-functional teams to provide effective solutions.
- Conduct regular security assessments and audits of firewall systems, recommending and implementing improvements as needed.
- Stay up to date with the latest network security trends, vulnerabilities, and best practices.

- Mentor and provide technical guidance to junior engineers, fostering a collaborative and knowledge-sharing environment.
- Conduct thorough security assessments to identify vulnerabilities and ensure the robustness of network defenses.
- Develop automation scripts and provide training to improve efficiency and effectiveness in security operations.
- Create and maintain comprehensive documentation for firewall configurations, policies, and procedures.
- Provide ongoing security engineering support to ensure the integrity and availability of network systems.
- Analyze and evaluate new security technologies and tools to enhance the organization's security posture.
- Deploy and provide day-to-day support for NSX and AVI technologies, ensuring seamless integration with existing infrastructure.
- Assess and implement new features and versions of Palo Alto Firewall.
- Design and deploy AVI load balancer VIP and GSLB configuration.
- Maintain and troubleshoot NSX environment.
- Migrate NSX-T Load balancer to AVI.
- Deploy Global Protect as Client VPN.

Mastercard · Contract **Aug 2023 - Dec 2023**
Senior Information Security Engineer

Security Engineering Professional with expertise in conducting comprehensive security assessments, identifying risks, and providing actionable recommendations. Skilled in reviewing solution designs, data flow diagrams, and network changes to ensure alignment with security standards. Proven ability to develop and automate assessment workflows, deliver training to engineering teams, and support secure technology integration in large-scale data center projects. Adept at collaborating with cross-functional teams and presenting security findings to stakeholders to drive informed decision-making.

- Review ongoing security assessment engagements.
- Focusing on solution designs Data flow diagrams, software business cases, implementation plans, and network changes
- Meet with the project teams to gather necessary documentation and understand the context of each assessment.
- Begin the initial analysis of the assessments, identifying potential security risks and areas of improvement.
- Identify opportunities for automating assessment workflows, particularly in the analysis and reporting stages.
- Collaborate with the development team to start creating scripts or tools to automate assessment processes.
- Begin preparations for providing training sessions to other security engineers on the automation tools and workflows.
- Continue the development of scripts and tools for assessment automation.
- Prepare training materials and resources for the upcoming training sessions.
- Conduct initial training sessions for other security engineers, focusing on using the newly developed automation tools.
- Give attention to providing security engineering support for technology imperatives related to new data center build-outs.
- Collaborate with the data center project teams to ensure security requirements are integrated into the design and implementation phases
- Analyze new and existing technologies, with a focus on identifying potential security risks.
- Provide recommendations and reports on areas of security risk and alignment with Client policies and technical standards
- Collaborate with other corporate security teams to evaluate new technologies in the context of security.
- Work on defining security requirements for integrating new technologies into the organization's environment.
- Complete the analysis of ongoing security assessment engagements.
- Prepare comprehensive reports and recommendations based on the assessments.
- Present findings and recommendations to relevant stakeholders.

Jones Lang Lasalle – Chicago, IL **OCT 2022 – MAY 2023**
Cloud Network Security Engineer
Technical Scope: Firewall, Azure and AWS Cloud Networking

Utilize Azure and AWS services to evaluate and resolve complex network issues across Cloud networks. Assist client in designing, managing, and rolling out Meraki SD-WAN architecture. Deliver assistance in maintaining and updating cloud network infrastructure. Expand personal knowledge in terms of Palo Alto, Cisco ASA and Meraki, as well as F5 ASM Firewall. Conduct troubleshooting activities for resolving user and network issues, such as Splunk, and Thousand Eye.

- Secured CI&A Team Award at JLL.

- Demonstrated expertise in configuring and maintaining Cisco Identity Service Engine (ISE) with deep technical knowledge.
- Proficient in 802.1x authentication, ensuring secure network access control.
- Experienced in troubleshooting policy configuration between Cisco ISE and Junos OS, ensuring seamless integration and functionality.
- Utilized Azure Traffic Manager and Azure Load Balancer to optimize network traffic distribution and ensure high availability of applications and services.
- Familiarity with Azure Network Watcher and Azure Monitor for network traffic analysis, troubleshooting, and proactive monitoring of network performance and health.
- Implements and designs core Azure networking infrastructure, including Virtual Networks (VNet), Subnets, and CIDR ranges, ensuring optimal network architecture.
- Configures and manages hybrid networking connections to load balance traffic and optimize network routing between on-premises and Azure environments.
- Establishes private access to Azure services, implementing secure connectivity and controlling network traffic to safeguard sensitive data.
- Implements network security measures and conducts monitoring and analysis of traffic flows to identify potential threats and vulnerabilities.
- Worked under time pressure constraints to deliver modeling results within project timelines, providing clear and articulate reports outlining any issues encountered during testing and the steps taken to resolve them.
- Collaborated closely with stakeholders in Global Network Engineering, Global Network Architecture, and Global Network Operations teams to understand network designs and configurations with the overall network architecture.
- Worked in coordination with project managers to complete testing network equipment configurations on time, ensuring smooth project implementation and adherence to project timelines.
- Designed, implemented, and maintained network systems for middle to large companies with multiple locations, ensuring seamless connectivity and optimal performance.
- Managed and supported CISCO NEXUS and Catalyst switches, configuring VLANs, optimizing routing protocols, and resolving network issues promptly to minimize downtime.
- Configured and maintained CISCO ASA and FirePower Firewalls, implementing robust security measures to protect the network infrastructure from external threats.
- Collaborated with cross-functional teams to develop and execute change management processes, coordinating network changes to ensure minimal disruption to operations.
- Demonstrated an expert level understanding of BGP, effectively configuring and troubleshooting routing protocols to optimize network connectivity.
- Utilized network management tools such as ASDM and Panorama to monitor and analyze network performance, proactively identifying and resolving issues.
- Created comprehensive documentation of network designs, configurations, and processes, ensuring accurate and up-to-date information for future reference and audits.
- Effectively communicated technical information to both technical and non-technical partners, facilitating clear understanding and collaboration.
- Improved skills of junior network engineers on Palo Alto Firewall policy.
- Enabled successful firewall policy change by developing change record in IBM / ServiceNow ticketing system for all service requests.
- Designee and develop Express routes in Azure
- Worked on Express Route, VPN connections with private, public cloud as well as On prem Networking (hybrid Environment)
- Design and developed GW and SD Wan solutions for hybrid environment.
- Troubleshoot using AWS EC2 for any network related errors
- Worked on Automating Firewall policy implementation using scripts and Terraform.
- Experienced in Threat detection and analysis, Intrusion detection and prevention systems (IDS/IPS),Security information and event management (SIEM), Vulnerability assessment and management, Incident response and mitigation, Network traffic analysis
- Penetration testing and ethical hacking
- Used Terraform and Octopus Deploy for automation of network architecture in Azure Cloud.
- Utilize Azure and AWS services to evaluate and resolve complex network issues across Cloud networks, including making changes to firewall and Web Application Firewall (WAF) configurations.
- Assist clients in designing, managing, and rolling out Meraki architecture, ensuring robust security measures are in place.

- Deliver assistance in maintaining and updating cloud network infrastructure, with a focus on firewall and WAF configurations.
- Expand personal knowledge in terms of Palo Alto, Cisco ASA, Meraki, Aruba and F5 ASM Firewall, specifically in relation to complex configurations and changes.
- Conduct troubleshooting activities for resolving user and network issues, such as Splunk and ThousandEye, with a specific focus on firewall and WAF-related issues.
- Demonstrated ability to optimize Splunk configurations and fine-tune search queries for improved performance and efficiency.
- Knowledge of best practices for Splunk deployment, including index sizing, data retention, and data lifecycle management.
- Familiarity with Splunk apps and add-ons for specific use cases, such as security monitoring, log management, and IT operations.
- Experience in creating and maintaining Splunk dashboards, reports, and alerts to monitor network health, identify anomalies, and facilitate troubleshooting.
- Strong understanding of Splunk data onboarding processes, including data source identification, parsing, and normalization.
- Knowledge of Splunk search language (SPL) and advanced search techniques for data analysis and visualization.
- Traffic optimization and routing
- Network monitoring and management in hybrid environments
- Demonstrated proficiency in designing and implementing scalable and secure network architectures on GCP. Deep understanding of networking concepts such as VPCs, subnets, firewall rules, load balancers, and VPN connectivity.
- Extensive experience in configuring and managing GCP networking services, including Google Cloud Virtual Private Cloud (VPC), Cloud Router, Cloud VPN, Cloud DNS, and Cloud Load Balancing. Proven ability to optimize network performance and ensure high availability.
- Proficient in working with Azure Network resources such as virtual networks, public and private IPs, virtual network peering, routing, firewall, custom policies, CIDR range, and Azure Virtual NAT.
- Demonstrated experience in designing and configuring Azure virtual networks, ensuring secure and efficient communication between virtual machines and resources.
- Skilled in implementing and managing routing protocols within Azure networks to optimize network traffic flow.
- Knowledgeable in Azure firewall configuration, including the setup of custom policies and rule sets to enforce network security.
- Proficient in IP address management within Azure, including allocation and assignment of public and private IPs.
- Experienced in setting up and managing Azure Virtual Network Peering to establish secure and efficient connectivity between virtual networks.
- Familiarity with Azure CDN (Content Delivery Network) and its associated resources, including configuration and optimization for content caching and distribution.
- Skilled in implementing Azure load balancing resources to ensure high availability and scalability for applications and services.
- Strong proficiency in using Terraform to define, provision, and manage cloud infrastructure resources on GCP. Expertise in writing reusable and modular Terraform code to automate infrastructure deployment and ensure consistency across environments.
- Implemented and managed Infoblox DNS, DHCP, and IPAM (DDI) solutions for large-scale enterprise networks, ensuring efficient IP address management and seamless network services.
- Designed and deployed highly available and scalable Infoblox Grid architectures, incorporating DNS and DHCP redundancy, load balancing, and failover mechanisms to ensure uninterrupted network operations.
- Excellent communication and interpersonal skills, enabling effective collaboration in a fast-paced team environment.
- Proven problem-solving experience in networking, telecom, and video networking.
- Extensive knowledge and experience in installing, monitoring, managing, and troubleshooting Cisco equipment, including Nexus switches.
- Strong background in multi-vendor security devices, such as ASA, Palo Alto, Client VPN, SSL VPN, IDS/IPS.
- Proficient in supporting VPN technologies, including SDWAN and IPSEC.
- Willingness to travel globally to support facilities and Mergers and Acquisitions.
- Expertise in SAN networking design and support, including Fiber Channel and iSCSI
- Deployed Aruba SDWAN as proof of concept.
- Diligently maintains documentation of LAN/WAN infrastructure and security policies.
- Available for 24x7 on-call rotations.
- Able to translate business requirements into technology solutions effectively.

- Proven experience in supporting, monitoring, and implementing Voice and Video solutions.
- Experience in working independently with strong time management skills.
- Familiarity with a global support environment.
- Strong problem-solving and analytical skills.
- Self-motivated and continuously strives to develop and expand skill set.
- Industry certifications demonstrating technical proficiency.
- Exceptional organization and documentation skills.
- In-depth knowledge of networking topologies, TCP/IP, DNS, DHCP, SNMP, BGP, OSPF, LAG, Spanning Tree, VOIP, SIP.
- Experience in circuit provisioning.
- Proficient in managing On-Premises and Colocation data centers.
- Familiarity with mixed operating system environments.
- Experience with Virtualization, including VDI.
- Project management experience.
- Configured and maintained DNS zones, DNSSEC, and DNS forwarding, ensuring secure and reliable DNS resolution and mitigating DNS-related vulnerabilities.

Jones Lang Lasalle – Chicago, IL **AUG 2017 – OCT 2022**

Network Engineer

Technical Scope: Firewall, Load Balancer, Web Proxy

Utilize Observium, scrutinizer, Cisco ASA, Palo Alto, F5 Load Balancer, as well as Cisco switch and routers to evaluate and resolve complex network issues across remote sites and datacenter. Helped client in designing, managing, and rolling out Meraki architecture at remote client sites. Leverage skills in Cisco ScanSafe and Umbrella to allow and block internet sites for JLL users and other owned machines.

- Secured CI&A Team Award at JLL, became SME for Meraki technology.
- Utilizes network monitoring tools and technologies to ensure the availability, performance, and integrity of Azure network infrastructure.
- Utilized 802.1X authentication and radius authentication for user connectivity over LAN and Wifi.
- Extensive experience in configuring and maintaining Cisco Identity Service Engine (ISE) with deep technical knowledge.
- Proficient in setting up and troubleshooting 802.1x authentication using Cisco ISE for secure network access control.
- Implemented and maintained user authentication and authorization policies using Cisco ISE, ensuring secure access to network resources.
- Collaborated with cross-functional teams to develop and enforce network access policies based on industry best practices and compliance requirements.
- Conducted regular audits and assessments of Cisco ISE configurations to identify and address any security vulnerabilities or policy gaps.
- Worked closely with network administrators and security teams to resolve issues related to Cisco ISE, ensuring smooth network operations.
- Collaborates with cross-functional teams to develop and enforce network security policies and procedures.
- Conducts periodic audits and assessments of network security controls and implements necessary enhancements.
- Stays updated with the latest industry trends and best practices in network security and monitoring, implementing relevant technologies and strategies to enhance network resilience and protect against emerging threats.
- Demonstrated expertise in designing and implementing core Azure networking infrastructure, including Virtual Networks (VNet), Subnets, and CIDR ranges, ensuring efficient and secure network connectivity. Proven ability to collaborate with cross-functional teams, including network architects, security specialists, and operations personnel, to design and implement network security solutions and enforce best practices within Azure environments.
- Improved skills of junior network engineers on migration from Cisco platform to Cisco Meraki by providing training.
- Identified and eliminated chance of security breaches to datacenter, remote sites, and connectivity to datacenter, internet, as well as VPN connection to individuals and site-to-site network.
- Prevented potential network risks via establishment of internal and external firewall policy in datacenter and remote site in terms of implementation, monitoring, and management.
- Accelerated network performance and speed through design of F5 virtual servers and nodes as well as deployment of F5 global Load Balancer for user VPN appliance connections to datacenters based on locations.
- Steered upgrade of all wireless platforms to Wi-Fi 6 industry latest technology, while transitioning all AP's and WLC's to 9000 series.
- Employed Scrutinizer, Observe, Splunk, and Thousand Eye to troubleshoot user and network issues.
- Deployed and configured Cisco ASR 1000, 7000, 9000 series routers.

- Deploying and decommission of VLANs on core ASR 9K, Nexus 7K, 5K and its downstream devices.
- Configure and deploy L2 / L3 protocols STP, VTP, PVST, Ether channels, VLAN, PVLAN, ISL trunk, OSPF, EIGRP, Static, BGP and MPLS, Redundancy protocols HSRP, VRRP and GLBP
- Configuring RIP v1&2, OSPF, EIGRP, BGP, MPLS, Frame Relay and PBR.
- Configuration of static NAT, dynamic NAT and dynamic NAT overloading, DNS.
- Developed and enforced DNS and DHCP security policies, including DNS firewall rules and DHCP lease controls, to safeguard the network against DNS attacks and unauthorized access.
- Automated routine tasks and streamlined IP address provisioning processes using Infoblox APIs and scripting languages (Python, Perl, or Bash), resulting in improved operational efficiency and reduced manual errors.
- Conducted network audits and assessments, identifying and resolving IP conflicts, DNS misconfigurations, and DHCP performance issues, resulting in enhanced network stability and optimized resource utilization.
- Experience in integrating Splunk with other systems and tools, such as ticketing systems, identity and access management (IAM) platforms, and threat intelligence feeds.
- Knowledge of Splunk deployment best practices for high availability, scalability, and disaster recovery.
- Understanding of network protocols and technologies, such as TCP/IP, DNS, DHCP, VPN, firewalls, and load balancers, to effectively leverage Splunk for network troubleshooting and monitoring.
- Utilized Observium, scrutinizer, Cisco ASA, Palo Alto, F5 Load Balancer, as well as Cisco switch and routers to evaluate and resolve complex network issues, including making changes to firewall and Web Application Firewall (WAF) configurations.
- Helped clients in designing, managing, and rolling out Meraki architecture at remote client sites, ensuring the appropriate firewall and WAF configurations were in place.
- Leveraged skills in Cisco ScanSafe and Umbrella to allow and block internet sites for JLL users and other owned machines, including implementing and adjusting firewall and WAF rules as needed.
- Identified and eliminated the chance of security breaches to data centers, remote sites, and connectivity, by implementing and managing firewall and WAF configurations.
- Accelerated network performance and speed through the design and configuration of F5 virtual servers and nodes, including implementing firewall and WAF policies.
- Employed Scrutinizer, Observe, Splunk, and Thousand Eye to troubleshoot user and network issues, specifically focusing on firewall and WAF-related problems.
- Proficient in testing network change scripts using network simulation tools like EVE-NG to validate and verify the effectiveness of firewall and WAF configurations prior to deployment.
- Demonstrated ability to work with CIDR ranges in Azure networking, effectively managing IP address allocations and subnetting.
- Proficient in configuring and managing Azure Virtual NAT (Network Address Translation) to provide outbound connectivity for virtual networks.
- Strong troubleshooting skills in identifying and resolving network-related issues within Azure environments.
- Experience in documenting Azure network designs and configurations, providing clear and comprehensive documentation for reference and troubleshooting purposes.

Mississippi College, Office of Global Education – Clinton, MS **Jan 2015- DEC 2015**

Helpdesk / Office Technical Support

Technical Scope: Microsoft Word and Excel

Assisted students in assessing and rectifying complex network issues via phone and physical interactions. Monitored, organized, and updated office documentation, while providing expert-level technical support to supervisors.

- Commended by management for rendering outstanding technical assistance and achieving incident resolution rate of 89% without escalation.
- Obtained 'Achievement Award' for demonstration of exceptional dedication to Office of Global Education.

Dynovis IT Services Private, Ltd. – Ahmedabad, India **DEC 2013 – NOV 2014**

Network Engineer

Technical Scope: Firewall, Routers, Switch Packet Switching · Domain Name System (DNS) · Project Management · Border Gateway Protocol (BGP) · Networking · Cisco Systems Products

Analyzed and resolved network issues for remote sites and data center using Observium, scrutinizer, cisco ASA, Palo alto, F5 Load Balancer, Cisco Switch and Cisco Routers. Organized and updated Network equipment, and provided technical support.

- Deployed and configured Cisco ASR 1000, 7000, 9000 series router.

- Used EVE-NG for LAB and Testing network gears.
- Deploying and decommission of VLANs on core ASR 9K, Nexus 7K, 5K and its downstream devices.
- Configure and deploy L2 / L3 protocols STP, VTP, PVST, Ether channels, VLAN, PVLAN, ISL trunk, OSPF, EIGRP, Static, BGP and MPLS, Redundancy protocols HSRP, VRRP and GLBP
- Configuring RIP v1&2, OSPF, EIGRP, BGP, MPLS, Frame Relay and PBR.
- Configuration of static NAT, dynamic NAT and dynamic NAT overloading
- Create change record in IBM/ ServiceNow ticketing system for any service request in network queue for firewall policy change
- Drive firewall policy in data center and remote site internal and/or external firewall in prospects of implementation and monitoring and managing. Analyzed and resolved network issues for remote sites and data center using Observium, scrutinizer, cisco ASA, Palo alto, F5 Load Balancer, Cisco Switch and Cisco Routers. Organized and updated Network equipment, and provided technical support.
- Deployed and configured Cisco ASR 1000, 7000, 9000 series router.
- Deploying and decommission of VLANs on core ASR 9K, Nexus 7K, 5K and its downstream devices.
- Configure and deploy L2 / L3 protocols STP, VTP, PVST, Ether channels, VLAN, PVLAN, ISL trunk, OSPF, EIGRP, Static, BGP and MPLS, Redundancy protocols HSRP, VRRP and GLBP
- Configuring RIP v1&2, OSPF, EIGRP, BGP, MPLS, Frame Relay and PBR.
- Configuration of static NAT, dynamic NAT and dynamic NAT overloading
- Create change record in IBM/ ServiceNow ticketing system for any service request in network queue for firewall policy change
- Drive firewall policy in data center and remote site internal and/or external firewall in prospects of implementation and monitoring and managing.
- Collaborated with cross-functional teams, including network engineers, security analysts, and system administrators, to integrate Infoblox solutions with existing network infrastructure and ensure seamless interoperability.
- Provided technical support and troubleshooting expertise to resolve complex DNS and DHCP issues, ensuring minimal network downtime and prompt issue resolution.
- Stayed up-to-date with the latest industry trends and Infoblox product developments, participating in training programs and certifications to enhance technical knowledge and skills.
- Actively contributed to infrastructure planning and capacity management initiatives, providing insights and recommendations for optimizing Infoblox deployments and meeting future network requirements.
- Experience with converting Checkpoint VPN rules over to the Cisco ASA solution. Migration from Juniper Net screen SSG-550 to Palo Alto 5000
- Designing, Installation and configuration of MPLS circuits, VPN and SSL VPN connections on checkpoint Firewalls, Juniper & NetScreen VPN Boxes.
- Involved in Replacement of FPCs, PICs on Juniper M320 and T640 router.

Additional Experience

Web Designer/ Customer Relation Manager at Venture Implementations, Ahmedabad, India 2012-2013
Database Developer at Eminence Technologies, Ahmedabad, India, 2010 – 2011

Education & Certifications

Cisco Certified Network Associate (CCNA)
PCNSA(2025)
Master of Science in Computer Science (2017) – Mississippi College, Clinton, MS
Master of Science in Computer Science (2013) – Ganpat University, Kherva, India
Bachelor of Science in Computer Application (2011) – Gujarat University, Ahmedabad, India