

# Ekonkar Singh

Email: [ekonkar.singh.s@gmail.com](mailto:ekonkar.singh.s@gmail.com) | LinkedIn: [linkedin.com/in/esingh-1](https://linkedin.com/in/esingh-1)

---

## Experience

### IT Analyst (Security and Compliance)

Shared Services Canada | May 2023 – April 2024

- Configured Microsoft 365 environments to meet compliance standards, enhancing security.
- Maintained secure records of cloud configurations and access logs.
- Reduced identity issues by 26% through effective Azure AD administration.
- Aligned IT configurations with risk management frameworks and Government of Canada standards.
- Collaborated with diverse teams to ensure compliance with classification markings.
- Led weekly Microsoft 365 training sessions to improve operational efficiency.
- Automated processes, reducing manual workloads and improving efficiency.

### Network Specialist

Alstom, Thunder Bay | June 2022 – August 2022

- Analyzed network performance and addressed anomalies to ensure system resilience.
- Conducted forensic analysis of host logs to identify vulnerabilities and optimize security postures.
- Created benchmarks for advanced malware detection and remediation processes.

### Information Systems Administrator

McDonald's | January 2021 – May 2022

- Managed secure server environments, enhancing uptime by 15% through optimized configurations.
- Designed secure frameworks for network administration and streamlined anomaly detection capabilities.

---

## Key Projects

### Agentless Network Access Control (NAC) System

- Developed an agentless NAC system using Bash, RADIUS, and Slack for real-time monitoring.
- Enforced posture checks and authentication policies without client-side dependencies.
- Automated system alerts via Slack, reducing manual oversight.
- Delivered a scalable and resource-efficient solution for network access control.

### AI-Based Explicit Content Detection System

- Developed an AI solution using AWS Rekognition to detect explicit content in images.
- Deployed the model on AWS Lambda for scalable and efficient processing.
- Automated real-time alerts for detected violations via Slack and email notifications, reducing manual review workload by 40%.

### **SSH Attack Pattern Analyzer**

- Deployed a honeypot VM to monitor SSH attack attempts, storing logs securely on Azure Blob Storage.
- Conducted statistical analyses using Python and R, creating geo-mapped visualizations in Power BI.
- Delivered actionable insights into cyber threat patterns and attacker origins.

### **Cloud Compliance Tool – ScubaGear**

- Designed and implemented automated compliance checks for cloud infrastructure.
  - Improved compliance assessment speed by 30%, aligning with government standards.
- 

## **Education**

### **Bachelor of Science in Computer Science**

*Lakehead University | January 2021 – December 2024*

- **Honors:** President's List (2021–2024)
  - **Relevant Coursework:** Machine Learning, Malware Analysis, Cloud Security, Statistical Modeling
- 

## **Certifications**

- **Microsoft:** AZ-900 (Azure Fundamentals), DP-600 (Fabric Analytics Engineer Associate)
  - **CompTIA:** Security+
- 

## **Skills**

### **Artificial Intelligence and Machine Learning**

- Python Libraries: scikit-learn, TensorFlow, pandas, NumPy
- AWS Rekognition, SageMaker
- Data Modeling and Visualization (MATLAB, Matplotlib)

### **Cybersecurity**

- Threat Detection and Response, SIEM Tools
- Vulnerability Management, Incident Analysis
- Identity and Access Management (IAM), Zero Trust Architecture
- NIST, ISO 27001 Compliance Standards

### **Cloud Computing**

- Platforms: AWS, Microsoft Azure, Microsoft 365
- Expertise in Cloud Security and Risk Management

### **Networking and Systems**

- SD-WAN Technologies (VMware VeloCloud)
- Linux Administration, Shell Scripting, Wireshark