Phuong Dang

+84337363152 | powoftech@gmail.com | linkedin.com/in/powoftech | github.com/powoftech

Education

Ho Chi Minh City University of Technology and Education
Bachelor of Engineering in Information Technology — *Aug. 2021 – Dec. 2025*

- **Cumulative GPA:** 3.24/4.0
- **Academic Excellence:** Achieved A/A+ grades in critical courses such as **Cloud Computing**, Data Structures & Algorithms, Object-Oriented Programming, and IT Project.
- **Specialized Coursework:** Developed a strong theoretical foundation in DevOps-related topics through courses in Operating Systems, Networking Essentials, Information Security, and Web Security.
- **Practical Application:** Completed multiple project-based courses, including ”Project on Software Engineering” (Grade: A), demonstrating the ability to apply software engineering principles to solve practical problems.

Experience

First Cloud Journey Trainee — April 2025 – Present
AWS Study Group — *Ho Chi Minh City, Vietnam*

- Completed an intensive AWS bootcamp covering core platform areas—**Networking, Compute, Storage, Security, Database**—through hands-on labs to deploy, secure, and operate workloads.
- Built and presented a capstone **workshop** that deployed an AWS-based system; documented architecture, deployment steps, and troubleshooting; see Projects for implementation details.
- Engaged in a collaborative, project-based learning environment, working with peers and receiving direct mentorship from AWS professionals to troubleshoot and resolve complex technical challenges.
- Actively supported the organization of official AWS community events in Vietnam, and was selected to participate in exclusive private training sessions on advanced cloud topics.

Projects

Secure Container Pipeline on AWS | *Workshop* | *GitHub Repository* — July 2025 – Aug. 2025

- Built a GitHub Actions pipeline (OIDC to AWS) to build a Node.js container, push to Amazon ECR, and gate releases with vulnerability scanning on high/critical issues and immutable image tags.
- Hardened Kubernetes workloads with `securityContext` best practices (non-root user, read-only root FS, no privilege escalation, drop all Linux capabilities).
- Enforced policy-as-code using Kyverno (block `:latest` images; require non-root) and validated with test pods (allowed/blocked cases).
- Deployed a 2-replica app to Amazon EKS and exposed it via a Kubernetes `LoadBalancer` service.
- Documented runtime threat detection with Falco for cluster security visibility.

Technologies Used: Amazon EKS, Amazon ECR, IAM, GitHub Actions, Kubernetes, Docker, eksctl (IaC), Kyverno, Trivy, Node.js, YAML

Technical Skills

Cloud Platforms: AWS (Amazon EKS, Amazon ECR, VPC, IAM), Foundational knowledge of Azure and GCP concepts
Containerization & Orchestration: Kubernetes, Docker
Infrastructure as Code (IaC): eksctl, Terraform (Conceptual)
CI/CD & DevOps Tools: GitHub Actions
DevSecOps & Security: Kyverno (Policy-as-Code), **Trivy** (Vulnerability Scanning), **Falco** (Runtime Threat Detection)
Programming & Scripting: Node.js, Python, Bash