

BALACHANDAR M

balachandarm.works@gmail.com | +91 9751631759 | Tenkasi, Tamil Nadu | linkedin.com/in/m-balachandar

balachandar.tech | github.com/mubalachandar

SUMMARY

AWS Certified Cloud Practitioner and CSE student specializing in cloud infrastructure and automation. Hands-on experience deploying and securing AWS environments using EC2, VPC, IAM, and S3. Proficient in Python (Boto3), Bash scripting, and Linux administration. Built real-world projects focused on cloud resource monitoring, network auditing, and infrastructure hardening. Seeking a Cloud Engineer role to deliver scalable, secure cloud solutions.

EDUCATION

Bachelor of Engineering in CSE (AIML), RATHINAM TECHNICAL CAMPUS 09/2023 – Present
CGPA: 7.45/10

Higher Secondary Certificate (HSC), SMA MATRIC HR SEC SCHOOL 06/2022 – 04/2023
Marks: 84.3/100

CERTIFICATES

AWS Certified Cloud Practitioner
Amazon Web Services Apr 2026 – Apr 2029

AWS Academy Graduate – Cloud Foundations
Amazon Web Services Jan 2026

Cybersecurity Analyst Job Simulation – IAM & Access Management
Tata (Forage) Jan 2026

SKILLS

Cloud Platforms: AWS (EC2, S3, VPC, IAM, CloudWatch, SNS, CloudFront)

Languages: Python, Bash Scripting

Automation: Boto3, Git, AWS CLI

Networking: TCP/IP, DNS, Subnetting, VPC, Security Groups, NACLs

Security: IAM Policies, Least Privilege, S3 Bucket Policies, MFA, Access Control

Tools: Nmap, Wireshark, AWS Console, GitHub, VS Code

OS: Linux (Ubuntu, RHEL), Windows

PROJECTS

AWS Cloud Infrastructure Deployment with Security Hardening, 11/2025 – 12/2025
AWS | EC2 | VPC | IAM | S3 | Security Groups | NACLs

- Architected a **multi-tier AWS infrastructure** with custom VPC, public/private subnets, and route tables enforcing network segmentation using Security Groups and NACLs to minimize attack surface.
- Implemented **IAM roles with least-privilege policies** for secure, credential free EC2 to S3 communication aligning with AWS Well Architected Framework security best practices.
- Deployed dual-layer access controls via **Security Groups and NACLs**, restricting traffic to required ports only reducing infrastructure attack surface by **70% vs default configurations**.

Automated AWS Resource Monitor with Alerts, 01/2026 – 02/2026
Python | Boto3 | AWS CloudWatch | SNS | S3 | EC2 | GitHub

- Built a **Python + Boto3 cloud auditing tool** that scans AWS environments for misconfigurations including public S3 buckets and missing encryption enabling proactive cloud governance.
- Integrated **AWS SNS alerts** to notify in real-time on policy violations eliminating manual infrastructure monitoring and reducing incident response time.
- Automated scans via **CloudWatch Events (cron)** with version controlled code on GitHub demonstrating end-to-end DevOps and cloud automation practices.

Linux Server Hardening + Network Audit Script, 03/2026 – 05/2026
Bash | Nmap | Wireshark | AWS EC2 | Linux | GitHub

- Developed a **Bash automation script** on AWS EC2 that audits open ports via Nmap, reviews active sessions, and parses /var/log/auth.log for unauthorized SSH access and brute-force attempts.
- Automated **Linux server hardening** disabling unused services, enforcing file permission policies, and generating structured audit reports — cutting manual review time by **65%**.
- Analyzed **live network traffic** using Wireshark/tcpdump on EC2 to detect anomalous packets and unencrypted data flows validating end-to-end infrastructure security posture.

EXTRACURRICULARS

IEEE Member 12/2025
IEEE (Institute of Electrical and Electronics Engineers)

Rajya Puraskar 01/2025
The Bharat Scouts and Guides

LANGUAGES

English
Fluent

Tamil
Native