EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

A Research Internship / Industry Internship
on
" Secure Serverless API using AWS API Gateway, Lamda, IAM and WAF"

Subject Code : 21INT82

Divya Lakshmi B(1EP21CS026)

Under the Guidance of

Mrs. Shilpa Patil
Assistant Professor,
Department of CSE, EPCET

Contents

Introduction

- **Cloud Security in Serverless Architectures :** In modern cloud computing, securing applications built using **serverless services like AWS Lambda and API Gateway** is vital. The serverless model removes infrastructure management but demands strong controls for identity, access, and traffic monitoring.

- **Project Focus: Securing Serverless APIs with AWS :** This project implements a secure REST API using **AWS Lambda, API Gateway, IAM, and AWS WAF**, ensuring protection against unauthorized access and web threats while demonstrating best practices in serverless application security.

About the Company

- **Founded**: 2006, Seattle, USA
- **Name**: Amazon Web Services (AWS)
- **Founder**: Andy Jassy (as part of Amazon by Jeff Bezos)
- **Services**: Cloud computing (IaaS, PaaS, SaaS),Storage (S3), Serverless (Lambda), Databases, Security,AI/ML, Analytics, Networking
- **Training** : Offers certifications, online labs, and AWS Academy courses

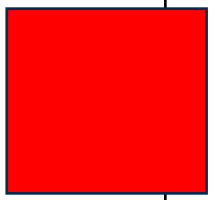
Amazon Web Services (AWS) is a leading cloud service provider offering scalable, secure, and cost-effective cloud computing solutions

Aim /Objectives/ Future Implications

- **Aim** : To deploy and secure a REST API on AWS using serverless architecture.
- **Objectives:**
  - Use API Gateway with Lambda for compute
  - Secure API using IAM and WAF
  - Log and monitor access patterns
- **Future Implications:** Extend for user authentication, API rate limiting, and real-time analytics.

Internship Timeline

Task	January	February	March	April	May
Requirement specification and Analysis					
Design					
Test Case					
Coding with unit testing					
Testing					
Documentation					





Technical Skills/Knowledge Gained

- **Skills**: AWS CLI, IAM Policies, REST APIs, Python (Boto3), Cloud Security
- **Tools**: AWS Console, Postman, Python, Terminal
- **Framework**: Serverless REST architecture
- **Technology Stack**: AWS Lambda, API Gateway, IAM, WAF
- **Database Used**: None (Stateless API)

Tools/ Frameworks/Database/ Technology Stack

- **Cloud Platform:**
  - Amazon Web Services (AWS)
- **Key Services Used:**
  - API Gateway – For REST API endpoint
  - AWS Lambda – For serverless backend
  - IAM – For access control and secure authorization
  - AWS WAF – For web security and IP filtering
- **Programming Language:**
  - Python – Used for Lambda function and API testing
- **Tools:**
  - Postman – For API testing
  - AWS CLI – For command-line AWS operations
  - VS Code / Any IDE – For writing Lambda and test scripts
- **Security Mechanism:**
  - SigV4 Signing for IAM-based API request authentication

Hardware and Software Requirements

- **Hardware :**
  - Windows PC or MacBook
  - RAM: 4GB or higher (8GB+ recommended)
  - Internet: Stable connection
- **Software requirement:**
  - Python 3.x
  - AWS CLI
  - Visual Studio Code
  - Postman
  - Web Browser for AWS Console

Internship Implementation

Step-by-step AWS Lab Setup:

1. Lambda Function Creation
2. API Gateway Setup with REST API
3. Integration with Lambda
4. Deploy Stage */dev/hello*
5. Enable IAM Authorization
6. Apply WAF WebACL to API Gateway
7. Use AWS CLI to test IAM access
8. Test protection via WAF rules

Learning Outcomes

- **Gained practical skills in:**
  - Serverless deployment
  - IAM configuration
  - API security
  - WAF setup and testing
- **Outcome Mapping**:
  - CO1: Cloud architecture understanding
  - CO2: Hands-on deployment
  - CO3: Secure API communication

Outcome Analysis

Through this project, I developed practical skills in deploying a secure, serverless API using AWS services like Lambda, API Gateway, IAM, and WAF. I gained a deep understanding of how cloud-based applications are protected through authentication and traffic filtering. The outcomes of this project align with key learning objectives such as cloud architecture understanding, secure application deployment, and real-world security configurations using IAM and WAF.

Challenges Faced

- WAF rule configuration blocking own IP
- IAM Signature V4 authentication errors
- API Gateway test failures due to missing permissions
- Debugging endpoint errors like "Missing Authentication Token

References

- AWS Documentation:
  - Lambda: https://docs.aws.amazon.com/lambda
  - API Gateway: https://docs.aws.amazon.com/apigateway
  - IAM: https://docs.aws.amazon.com/iam
  - WAF: https://docs.aws.amazon.com/waf
- AWS Well-Architected Framework
- Online Courses & AWS Labs

THANK YOU