Technological Institute of the Philippines
Manila Campus

College of Information and Technology
Education Bachelor of Science in Information
Technology

Research Works on Cloud Application Data Security

CITE007 A- IT32S1
INFORMATION ASSURANCE AND SECURITY

Submitted By:

Obina Holy Twinkle S

Date:
04/14/2025

Secure Application Development

What are the best practices for secure cloud application development?

Using secure coding standards, offering least privileged access, and encrypting data are best practices for cloud app development. In addition to ensuring secure coding, regularly update your dependencies, never hard code your credentials, and use HTTPS to secure communication. These practices will help you mitigate the most common attack vectors.

How can common vulnerabilities in cloud applications be prevented?

You can mitigate common vulnerabilities such as SQL injection, XSS and misconfiguration using input validation, appropriate error handling, secure authentication methods, and automation vulnerability scanners such as Snyk or SonarQube. Security testing should be part of the development lifecycle to find problems earlier.

Web and API Security

What are the main threats to web applications in cloud environments?

Cloud web applications can have pitfalls like broken access control, misconfigured services, exploitable APIs, and DDoS to name a few. APIs are exposed differently and need to be protected differently, for example rate limiting, validation and secure access tokens, in order to manage abuse.

How do authentication and authorization mechanisms (e.g., OAuth, JWT) secure cloud APIs?

OAuth enables apps to access user resources in a safe and secure way without sharing passwords. JWT (JSON Web Tokens) allow apps to confirm user identity and track access rights with signed tokens. These methods ensure only the authenticated and authorized can access APIs.

Secure DevOps Practices

What is DevSecOps, and how does it enhance cloud security?

DevSecOps provides multiple opportunities to consider security, including considerations during the application lifecycle, via automated security checks of both static and dynamic analysis, and promoting the ability for development, security, and operations teams to work together to proactively identify and remediate vulnerabilities in a continuous nature.

How can security be integrated into CI/CD pipelines?

Security can be built into continuous integration and continuous delivery (CI/CD) pipelines using automated tools that can be deployed in the CI/CD pipeline pipeline to poll for vulnerabilities, seek secrets being stored in code, and terminate a deployment that is not aligned with security policies. Tools such as OWASP ZAP, SonarQube, and GitHub Actions can be leveraged to provide application security within a CI/CD environment without major delays to the development pipeline practice.

Data Encryption and Key Management

What are the key differences between data-at-rest and data-in-transit encryption?
Data-at-rest encryption protects data that is stored including disks, databases, and backups; while data-in-transit encryption protects data that is being transported across networks (for example: HTTPS). Data-at-rest and data-in-transit encryption is needed to mitigate the risks of unauthorized access to stored data or interception of data being transported.

How do cloud providers manage encryption keys securely?
Data-at-rest encryption protects data that is stored including disks, databases, and backups; while data-in-transit encryption protects data that is being transported across networks (for example: HTTPS). Data-at-rest and data-in-transit encryption is needed to mitigate the risks of unauthorized access to stored data or interception of data being transported.

References

OWASP Foundation. (n.d.). *OWASP Secure Coding Practices - Quick Reference Guide*. Retrieved from https://owasp.org

OWASP Foundation. (n.d.). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. Retrieved from https://owasp.org

OWASP Foundation. (n.d.). *OWASP API Security Top 10*. Retrieved from https://owasp.org

OWASP Foundation. (n.d.). *OWASP Authentication Cheat Sheet*. Retrieved from https://cheatsheetseries.owasp.org

OWASP Foundation. (n.d.). *OWASP CI/CD Security Guidance*. Retrieved from https://owasp.org

Amazon Web Services (AWS). (n.d.). *AWS Security Best Practices*. Retrieved from https://docs.aws.amazon.com/security

Amazon Web Services (AWS). (n.d.). *AWS Key Management Service (KMS) Documentation*. Retrieved from https://docs.aws.amazon.com/kms

National Institute of Standards and Technology (NIST). (n.d.). *DevSecOps Practices and Implementation*. Retrieved from https://csrc.nist.gov