Technical Paper Report

Operating System Continuous Assessment - 2

Serverless Computing: A Security Perspective

Group Members :

Bhoomi Naik - 52
Janhavi Mandhan - 50
Dipesh Makdiya - 49
Dhiraj Rohra - 61

25 Mar 2025

Serverless computing has emerged as a transformative paradigm, offering developers the ability to deploy applications without managing infrastructure. It primarily operates through Backend as a Service (BaaS) and Function as a Service (FaaS), enabling faster deployment, automatic scaling, and cost-efficient pay-per-use models.

Advantages of Serverless Computing

- **Operational Simplicity:** Developers focus on code rather than infrastructure management.
- **Scalability:** Automatic scaling handles varying workloads.
- **Cost Efficiency:** Users pay only for resources consumed.

Security Benefits

- **Reduced Attack Window:** Short-lived functions limit attackers' opportunities.
- **Fine-Grained Permissions:** Functions operate with minimal access privileges.
- **DDoS Resistance:** Platforms manage sudden spikes in traffic efficiently.

Security Challenges

Despite its advantages, serverless computing introduces new security concerns:

- **Increased Attack Surface:** Numerous functions and APIs expand potential entry points.
- **Infrastructure Dependency:** Developers rely on cloud providers' security mechanisms.
- **Denial of Wallet (DoW) Attacks:** Attackers may maliciously invoke functions to generate high bills.
- **Shared Infrastructure Risks:** Multi-tenant environments increase the risk of side-channel attacks.

Attack Vectors

- **Application-Level Attacks:** SQL Injection, XSS, Command Injection, and broken authentication.
- **Infrastructure-Level Attacks:** Side-channel attacks, race conditions, and persistent malware in containers.

Countermeasures

- Implement strict **Identity and Access Management (IAM)**.
- Monitor function activity using **cloud-native security tools**.
- Set budget alerts to mitigate DoW attacks.
- Regularly update functions and use secure coding practices.

Conclusion

Serverless computing provides flexibility and operational advantages but requires a collaborative security approach between developers and cloud providers. By implementing robust security measures, organizations can mitigate potential risks while benefiting from the advantages of serverless computing.