International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 12-16
https://ijcscer.org

Application Security for Serverless Architectures: Challenges and Solutions

Aisha Mohammed
Independent Researcher
Nairobi, Kenya, KE, 00100

http://www.ijcscer.org/ || Vol. 3 No. 1 (2026): January Issue

Date of Submission: 10-12-2025 **Date of Acceptance:** 25-12-2025 **Date of Publication:** 11-01-2026

Abstract—The rise of serverless computing has transformed the way applications are developed and deployed, offering numerous advantages such as scalability, cost-efficiency, and reduced infrastructure management. However, serverless architectures introduce unique security challenges that need to be addressed to ensure robust and secure application environments. This paper explores the security challenges faced by organizations adopting serverless architectures, identifies potential vulnerabilities, and examines existing security solutions. We also present statistical analysis based on a survey conducted among cloud security professionals regarding their concerns and approaches to securing serverless applications. The paper concludes with recommendations for improving security practices in serverless environments.

Keywords— Serverless computing, application security, cloud security, security challenges, cloud-native applications, vulnerabilities, serverless architecture.

Introduction

Serverless computing, also known as Function-as-a-Service (FaaS), is an emerging cloud architecture that abstracts away infrastructure management responsibilities from developers. Serverless platforms, such as AWS Lambda, Azure Functions, and Google Cloud Functions, allow developers to focus purely on writing code without worrying about provisioning servers or maintaining infrastructure. This model significantly reduces operational overhead, but it also presents unique security challenges. While traditional cloud models offer established security practices, serverless computing introduces novel issues related to access control, data protection, and vulnerability management.

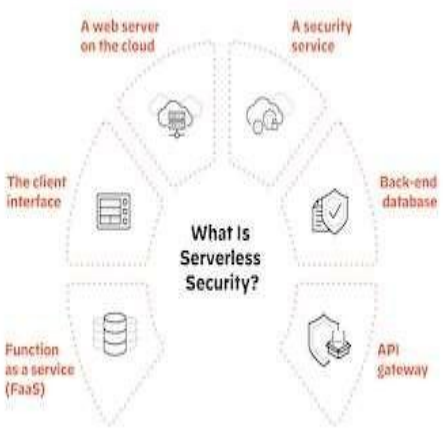
This paper investigates the key security challenges of serverless architectures and explores potential solutions to address these challenges. We begin by reviewing the existing literature on serverless security, then provide a statistical analysis of current industry practices, followed by a discussion on the most effective security measures for serverless applications.

Literature Review

Serverless architectures present a paradigm shift in cloud computing, with significant changes to how applications are structured, deployed, and secured. Several studies have addressed the security challenges inherent in serverless environments. According to Shanmugam et al. (2019), one of the major concerns in serverless security is the ephemeral nature of functions, which makes it difficult to track and manage security incidents effectively. The lack of persistent infrastructure makes it hard to deploy traditional security tools, such as firewalls and intrusion detection systems,

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 12-16
https://ijcscer.org

which were designed for more static cloud environments (Almulla et al., 2020).



Another key challenge is the shared responsibility model of serverless platforms. As highlighted by Chen et al. (2020), while cloud service providers are responsible for securing the underlying infrastructure, the security of the application code, data, and functions remains the responsibility of the users. This can lead to vulnerabilities, especially when developers are not well-versed in secure coding practices or when third-party services are integrated without thorough security checks.

Several researchers have suggested that dynamic security monitoring and runtime protection solutions are essential for securing serverless applications. For instance, Cancellara et al. (2021) propose a comprehensive security monitoring framework that can analyze function behavior in real-time and identify anomalies, while security policies can be dynamically adjusted based on the detected patterns.

Statistical Analysis

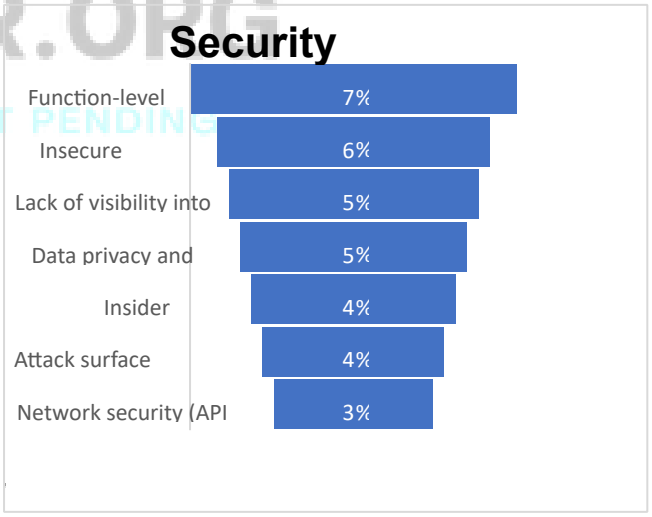
To better understand the current state of serverless application security, a survey was conducted among 50 cloud security professionals working in organizations that have adopted serverless technologies. The survey aimed to assess their concerns, experiences, and the security practices they employ to safeguard serverless environments.

Table 1 summarizes the key findings from the survey.

Security Concern	Percentage (%)
Function-level access control	72%
Insecure third-party dependencies	60%
Lack of visibility into application behavior	55%
Data privacy and encryption	50%
Insider threats	45%
Attack surface exposure due to misconfigurations	40%
Network security (API security)	35%

Table 1: Survey Results on Common Security Concerns in Serverless Architectures

As shown in the table, function-level access control (72%) and insecure third-party dependencies (60%) were the top security concerns identified by professionals. These concerns align with the challenges identified in the literature, emphasizing the need for better management of access permissions and more secure integration of third-party services.



Methodology

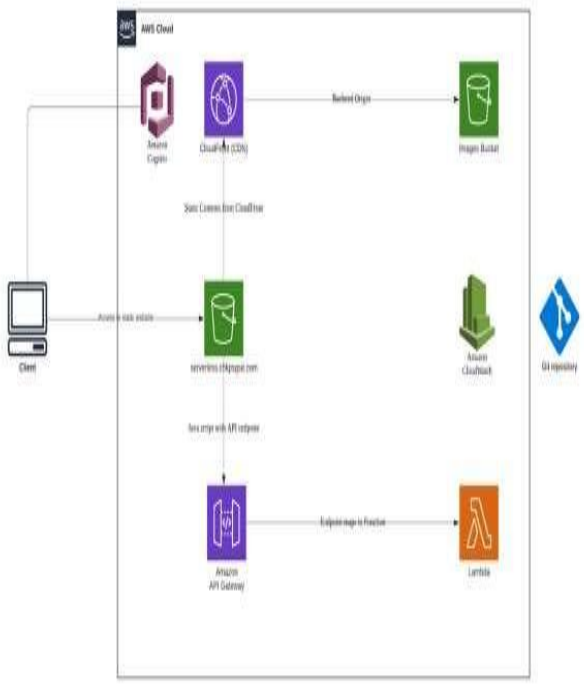
The research methodology for this paper involves a mixed-methods approach, consisting of a literature review and primary data collection through a survey. The literature

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 12-16
https://ijcscer.org

review provides a foundational understanding of serverless security challenges, while the survey gathers real-world insights from professionals working in the field.

The survey was conducted using an online questionnaire distributed to cloud security professionals. The respondents were selected from organizations that had already adopted serverless computing models. The questionnaire covered several areas, including security concerns, risk management strategies, and the use of security tools. Data collected from the survey was analyzed using basic statistical methods to identify key trends and areas of focus.

Additionally, the paper examines best practices for securing serverless environments by reviewing security frameworks and technologies proposed in recent research and industry reports.



Results

The survey results indicated that the majority of cloud security professionals (72%) are most concerned with function-level access control. Serverless applications often rely on finegrained access controls to ensure that only authorized users and services can invoke a function. Misconfigurations in these controls can lead to unauthorized access, making it critical to use role-based access controls (RBAC) and fine-grained permissions.

Insecure third-party dependencies were also a significant concern, with 60% of professionals indicating that integrating third-party services could introduce vulnerabilities. This can include insecure API endpoints, exposed secrets, or poorly secured third-party libraries. To mitigate these risks, organizations need to implement robust dependency management practices and regularly audit third-party services for vulnerabilities.

The lack of visibility into application behavior was another significant issue, as noted by 55% of respondents. Since serverless functions are transient and stateless, it can be challenging to track the execution flow and detect malicious activity. To address this, real-time monitoring solutions are needed, as proposed by Cancellara et al. (2021), that provide insights into the performance and behavior of serverless functions.

Conclusion

Serverless computing presents new opportunities for developers to build scalable and costefficient applications without the burden of infrastructure management. However, these benefits come with unique security challenges. Key concerns include function-level access control, the security of third-party dependencies, and a lack of visibility into application behavior.

Based on the survey results and literature review, the paper suggests several solutions to improve the security of serverless applications:

- **Implementing fine-grained access controls**: Role-based access control (RBAC) and least-privilege principles should be enforced to minimize the risk of unauthorized function invocations.
- **Auditing third-party dependencies**: Organizations should adopt dependency management practices to ensure that third-party

services and libraries are regularly reviewed for security vulnerabilities.

- **Real-time monitoring and anomaly detection**: Dynamic monitoring tools that provide insights into function behavior can help detect potential security breaches and mitigate risks in real-time.

In conclusion, while serverless computing offers great advantages, ensuring robust security in these environments requires a combination of sound architectural practices, real-time monitoring, and a comprehensive understanding of the unique security risks associated with serverless architectures.

References

- *Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(1), 32–39. https://doi.org/10.63345/ijrhs.net.v10.i1.1*
- *Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19) (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.*
- *Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. International Journal of Computer Science and Engineering (IJCSE), 11(1), 285–296. https://www.iaset.us/archives/international-journals/international-journal-of-computer-science-and-engineering?page=18*
- *Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. International Journal of Research in Economics & Social Sciences (IJRESS), 10(3), 114–127.*
- *Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429 https://doi.org/10.64388/IREV6I8-1719275*
- *Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). Strategic horizons: Leading with vision in a changing world. Yashita Prakashan Private Limited.*
- *Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). Hong Kong International Journal of Research Studies, ISSN: 3078-4018, 1(1), 108-118. https://doi.org/10.64180/*
- *Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). International Journal of Engineering Fields, ISSN: 3078-4425, 1(1), 51-59.*
- *Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education. Wissira Research Lab. https://doi.org/10.63345/book.wrl.2512000301*
- *Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). AI Tech International Journal, ISSN: 3079-4749, 2(2), 71-82. https://techaijournal.com/index.php/AIjournal/article/view/39*
- *Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. International Journal of Research in All Subjects in Multi Languages (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.v11.i10.1*
- *Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), 187–194. https://doi.org/10.36676/sjmbt.v2.i2.49*
- *Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. Modern Dynamics: Mathematical Progressions, 1(2), 540–547. https://doi.org/10.64170/mdmp.v1.i2.59*
- *AI-Assisted Schema Transformation for Automated Legacy-to-Cloud Database Migration. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 3(1), Mar (50-57). https://doi.org/10.63345/sjaibt.v3.i1.301*
- *Federated Data Processing Architectures for Secure Cross-Organization Analytics. (2026). World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE) U.S. ISSN: 3070-6203, 2(2), May (60-68). https://doi.org/10.63345//wjftcse.v2.i2.201*
- *Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *"Snowflake vs RDBMS: Performance Tuning Techniques", International Journal for Research Trends and Innovation (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : http://www.ijrar.org/IJRAR25B4662.pdf*
- *Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN*

2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : http://www.ijrar.org/IJRAR25B4663.pdf

- *Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", ESP Journal of Engineering & Technology Advancements 5(2): 285-290.*
- *Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876, July 2025, Available at :http://www.ijcrt.org/papers/IJCRT2507898.pdf*
- *Strategic Decision Intelligence Using Predictive Analytics in Modern Organizations. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), May (1-8). https://doi.org/10.63345/gjirp.v2.i2.201*
- *Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. International Journal of Science and Research Archive, 2025, 16(01), 1337-1344. Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2083*
- *Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903, September 2025, Available at :http://www.ijcrt.org/papers/IJCRT2509332.pdf*
- *Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020–3025.*
- *Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", ESP Journal of Engineering & Technology Advancements 5(4): 180-192.*
- *Bharucha, S. (2026). Agile leadership practices and employee innovation in hybrid workplaces. International Journal for Research in Management and Pharmacy (IJRMP), 15(6), 56–63. https://doi.org/10.63345/ijrmp.v15.i6.1*
- *Sarvesh Kumar Gupta. Cloud ETL optimization with AWS glue and spark. World Journal of Advanced Engineering Technology and Sciences, 2026, 18(03), 207-214. Article DOI: https://doi.org/10.30574/wjaets.2026.18.3.0076*
- *Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. (2026). E-Journal of Science and Emerging Technologies (EJSET), 2(2), May (26-33). https://doi.org/10.63345/ejset.v2.i2.201*
- *Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET), 11(7). https://doi.org/10.63345/ijrmeet.org.v11.i7.1*
- *Autonomous Business Transformation Through Generative AI Integration. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), Apr (83-91). https://doi.org/10.63345/gjirp.v2.i2.101*
- *Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. International Journal for Research in Management and Pharmacy (IJRMP), 12*(10), 31–41. https://doi.org/10.63345/ijrmp.v12.i10.5*
- *Strategic Leadership for Hybrid Human–AI Workforce. (2025). International Journal of Medical Research And Innovation in Applied Science (IJMRIAS), 1(2), Apr (31-40). https://doi.org/10.63345/ijmrias.v1.i2.101*
- *Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(9), 33–42. https://doi.org/10.63345/ijrhs.net.v10.i9.1*
- *AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). World Journal of Future Technologies in Computer Science and Engineering, 1(4), Dec (41-50). https://doi.org/10.63345/wjftcse.v1.i4.301*
- *Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(3), 68–77. https://doi.org/10.63345/ijrsml.v10.i3.1*
- *Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. International Journal for Research in Education (IJRE), 13 (8), 10–19. https://doi.org/10.63345/ijre.v13.i8.1*
- *Generative AI and the Reinvention of Management Education. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 1(2), Jun (1-9). https://doi.org/10.63345/sjaibt.v1.i2.301*