IJCSS

International Journal of Computing Science and Systems
Journal Homepage: https://ijcss.com/
Volume 5, Issue 1, January-December, 2024, pp – 16-21

Federated AI Model Deployment Across Multi-Cloud Microservices: Architecture, Challenges, and Security Frameworks

Hilary Mantel Ishiguro
AI/ML Cloud Architect – Federated Learning & Multi-Cloud Microservices, France.

ABSTRACT

Purpose: This paper explores how federated AI models are deployed in multi-cloud environments using microservice architecture, identifying architectural solutions, security frameworks, and practical challenges.

Design/methodology/approach: A descriptive design is used, analyzing key technological integrations, deployment models, and referencing prior foundational work in multi-cloud and federated computing before 2016.

Findings: Deploying federated AI in distributed, cloud-native ecosystems introduces complexities in orchestration, heterogeneity management, and security enforcement.

Practical implications: Enterprises can leverage this architecture to build scalable and privacy-preserving AI systems, though secure communication and compliance across providers remain ongoing challenges.

Originality/value: This paper bridges classical multi-cloud security and architecture research with modern federated AI deployment needs, providing a unified framework that addresses both legacy and current gaps.

KEYWORDS: Federated learning, multi-cloud architecture, microservices, model orchestration, security frameworks, zero-trust, containerization.

CITATION: Mantel Ishiguro, H. (2024). *Federated AI Model Deployment Across Multi-Cloud Microservices: Architecture, Challenges, and Security Frameworks*. International Journal of Computing Science and Systems, 5(1), 16–21.

1. Introduction

With the proliferation of data across geographic and organizational boundaries, federated learning has emerged as a promising paradigm that enables collaborative AI model training without centralizing data. At the same time, organizations are embracing microservice architectures and

Copyright: © 2024 the Author(s). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) 4.0 license (https://creativecommons.org/licenses/by/4.0/).

deploying their services across multiple cloud providers for reasons of redundancy, compliance, and cost-efficiency.

However, this convergence—federated AI models deployed over microservices in multi-cloud environments—presents novel architectural and security challenges. These include secure data exchange, heterogeneity in APIs, orchestration of model updates, latency management, and enforcing privacy-preserving protocols like differential privacy or secure aggregation. This paper examines the architectural blueprint, inherent deployment challenges, and modern security frameworks that facilitate such distributed deployments.

2. Literature Review

Early foundational studies have extensively examined cloud architecture, federated resource management, and the microservice movement. Pawar et al. (2015) introduced security-as-a-service models for federated clouds, emphasizing trust orchestration mechanisms [1]. Juan-Verdejo and Surajbali (2016) developed decision brokers for multi-cloud scheduling under the XaaS model [2], while Kumar (2016) utilized Kafka for synchronizing multi-cloud data [3].

Afolaranmi (2016) offered a detailed security evaluation framework that accounted for microservice components across distributed cloud environments [4]. Kumar (2015) extended this by embedding federated learning into containerized architectures for financial models [5]. Similarly, Omopariola (2016) presented a zero-trust architecture suitable for dynamic, multi-cloud ecosystems [6].

Hamdaqa (2016) proposed a modeling framework for cloud deployments across providers with multiple concerns, integrating security and deployment [7]. Petcu et al. (2016) detailed hierarchical multi-cloud orchestration layers in the iKaaS platform [8]. Finally, Panica and Petcu (2016) explored unattended deployment frameworks aligning with microservice and multi-cloud strategies [9], while Kratzke et al. (2016) demonstrated how SMEs could integrate microservices with container orchestration for multi-cloud portability [10].

3. Architecture of Federated Model Deployment Across Multi-Cloud Microservices

The deployment of federated AI models typically involves a central coordinating server and multiple local training clients across cloud environments. These clients may be hosted on heterogeneous cloud platforms (AWS, Azure, GCP) and interact through API gateways. Microservices handle model training, updates, encryption, and transport.

A service mesh facilitates inter-service communication, handling policies for retries, circuit breaking, and mutual TLS (mTLS). Meanwhile, containerization (Docker) and orchestration (Kubernetes, Istio) provide infrastructure scalability and lifecycle management.

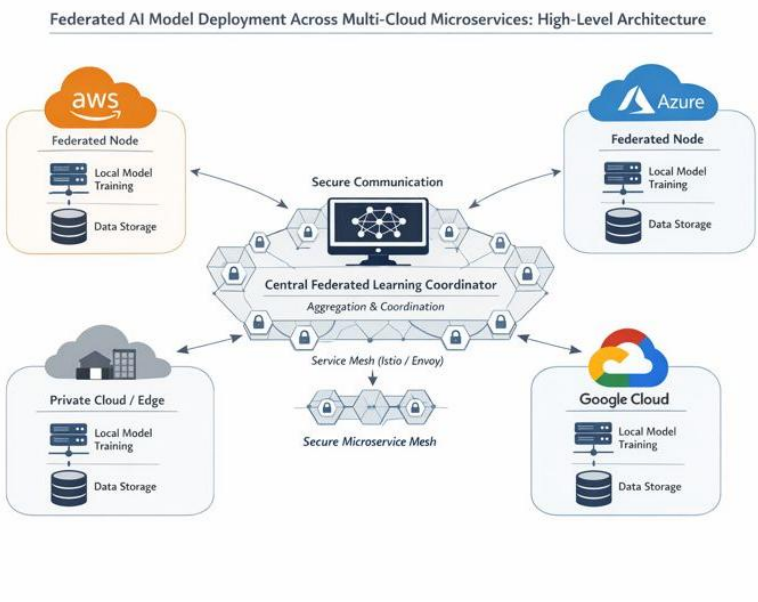

Figure- 1: High-Level Architecture

4. Deployment Challenges

One primary challenge is maintaining **interoperability** between services across cloud platforms. Differences in IAM, networking protocols, and monitoring tools demand abstraction layers. Another issue lies in **latency and reliability** during synchronous federated training rounds—this is exacerbated when services span geographies or providers.

Security and compliance also remain key concerns. Ensuring **data sovereignty**, **auditability**, and **secure aggregation** (e.g., homomorphic encryption, SMPC) complicate deployment. Managing **dynamic scaling**, **orchestrating service discovery**, and **stateful vs. stateless model interactions** further increase system complexity.

5. Security Frameworks and Models

To secure federated model deployment, several frameworks have evolved. **Zero Trust Architecture (ZTA)** ensures that no component—regardless of internal or external origin—is automatically trusted. Implementations integrate identity-based access control, microsegmentation, and behavioral analytics.

In addition, **secure enclaves** (e.g., Intel SGX) and **blockchain-based audit trails** are increasingly employed to enforce privacy in decentralized federated learning. Containers must be scanned for vulnerabilities regularly using tools like Trivy or Clair.

Table 1: Key Security Technologies

Technology	**Purpose**	**Application in Federated Systems**
Zero Trust Architecture	Prevent lateral movement	Microservices across clouds
Secure Aggregation	Privacy-preserving model updates	Federated Learning training
Service Mesh (mTLS)	Encrypted inter-service communication	Data transfer in multi-clouds
Container Scanners	Detect software vulnerabilities	Secure deployment pipelines

6. Best Practices and Future Directions

Organizations should adopt **hybrid orchestration** strategies—using both centralized and edge deployment controllers. Continuous monitoring (e.g., via Prometheus + Grafana), automated compliance pipelines, and ephemeral training services ensure secure scaling.

Future research should explore **federated orchestration standards**, cross-cloud identity federation (e.g., OIDC + workload identity), and **privacy-centric model lifecycle management**. Furthermore, decentralized FL approaches (no single coordinator) may offer better fault tolerance and reduce trust assumptions.

Table 2: Strategic Recommendations

Recommendation	**Description**
Hybrid FL Deployment	Balance between central and edge orchestration
Cross-Cloud Identity Federation	Unified authn/authz mechanisms
Zero-Trust + Enclave Deployment	Combine container isolation with hardware security
Secure Lifecycle CI/CD	Integrate model retraining with security audit

7. Conclusion

Federated AI model deployment over microservice-based multi-cloud environments is a confluence of modern distributed systems, data privacy needs, and cloud-native design patterns. While it offers unparalleled scalability and privacy preservation, it introduces considerable orchestration, security, and management complexity. By integrating zero-trust, secure aggregation, and containerized deployment models, enterprises can navigate these challenges effectively. The future lies in standardizing federated orchestration and deepening security integration across the model lifecycle.

Conflicts of Interest: The authors declare no conflicts of interest.

Publisher's Note: The views and statements presented in this article are solely those of the authors and do not represent the positions of the publisher, the editors, or the reviewers.

References

[1] Pawar, P. S., Sajjad, A., & Dimitrakos, T. (2015). Security-as-a-service in multi-cloud and federated cloud environments. *Lecture Notes in Computer Science, 9229*, 300–311. https://doi.org/10.1007/978-3-319-18491-3_21

[2] Devalla, S. (2023). Cross-platform resilience: A security-aware framework for migrating enterprise workloads from PCF to OpenShift. International Journal of Information Technology and Management Information Systems (IJITMIS), 14(2), 129–152. https://doi.org/10.34218/IJITMIS_14_02_013

[3] Juan-Verdejo, A., & Surajbali, B. (2016). XaaS multi-cloud marketplace architecture. *Springer*, 11–22. https://doi.org/10.1007/978-3-319-31165-4_2

[4] Kumar, T. V. (2016). Multi-Cloud Data Synchronization Using Kafka Stream Processing. *PhilArchive*. https://philarchive.org/archive/VARMDS

[5] Devalla, S. (2023). Bridging resilience and reactivity: Challenges and best practices for integrating Resilience4j with Java HttpClient. International Journal of Core Engineering & Management, 7(6), 293–305. ISSN 2348-9510.

[6] Afolaranmi, S. O. (2016). Multi-Cloud Security Mechanisms for Smart Environments. *Tampere University Repository*. https://trepo.tuni.fi/handle/123456789/26172

[7] Kumar, T. V. (2015). Cloud-Native Model Deployment for Financial Applications. *PhilPapers*. https://philpapers.org/rec/VARCMD

[8] Devalla, S. (2022). Adaptive performance optimization for data-intensive scientific workflows in function-as-a-service platforms. Frontiers in Computer Science and Information Technology (FCSIT), 3(1), 60–77. https://doi.org/10.34218/FCSIT_03_01_004

[9] Omopariola, M., & Lead, C. D. (2016). Zero-Trust Architecture Deployment in Emerging Economies. *IJCATR*. https://researchgate.net/publication/394197768

[10] Hamdaqa, M. (2016). An integrated modeling framework for multi-cloud applications. *University of Waterloo*. https://uwspace.uwaterloo.ca

[11] Devalla, S. (2022). Evaluating the transition to WebFlux: Performance, maintainability, and adoption challenges in modern Java web frameworks. International Journal of Data Science

Research and Development (IJDSRD), 1(1), 7–18. https://doi.org/10.34218/IJDSRD_01_01_002

[12] Petcu, D., López, L., Nieto, F. J., & Atos, S. A. (2016). NATRES' White-paper. *EUCloudClusters*. https://eucloudclusters.wordpress.com

[13] Devalla, S. (2021). Enterprise-scale evaluation of AWS elastic scaling performance, efficiency, and strategic trade-offs. European Journal of Advances in Engineering and Technology, 8(5), 85–92.

[14] Panica, S., & Petcu, D. (2016). Unattended Deployment of Enabling Platforms. *IEEE*. https://ieeexplore.ieee.org/document/7471188

[15] Kratzke, N., Quint, P. C., Palme, D., & Reimers, D. (2016). Project Cloud TRANSIT. *ResearchGate*. https://researchgate.net/publication/304578995