International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

Secure Serverless AI Platforms for Federated Learning and Predictive Analytics in Healthcare Financial and Insurance Enterprise Systems

Kieran Donal O'Callaghan

AI Engineer, Ireland

ABSTRACT: The rapid adoption of cloud computing and artificial intelligence has transformed enterprise systems across healthcare, financial, and insurance domains. However, these sectors face persistent challenges related to data privacy, regulatory compliance, scalability, and secure collaboration across organizational boundaries. Traditional centralized machine learning approaches often require data aggregation, which increases security risks and violates domain-specific regulations. To address these challenges, this paper proposes a secure serverless AI platform that integrates federated learning with predictive analytics in a cloud-native environment. The proposed framework leverages serverless computing for elastic scalability, federated learning for privacy-preserving model training, and AI-driven analytics for predictive decision support. The architecture ensures secure data isolation, regulatory compliance, and real-time performance optimization while enabling cross-domain intelligence. Experimental evaluation and qualitative analysis demonstrate improved scalability, reduced latency, and enhanced data privacy compared to centralized AI approaches. The proposed platform provides a robust foundation for next-generation intelligent enterprise systems and supports secure, scalable, and predictive analytics across healthcare, financial, and insurance ecosystems.

KEYWORDS: Serverless Computing, Federated Learning, Predictive Analytics, Cloud-Native Architecture, Healthcare Systems, Financial Systems, Insurance Analytics, Data Privacy, Artificial Intelligence, Machine Learning

I. INTRODUCTION

Enterprise systems in healthcare, finance, and insurance are increasingly data-driven, relying on real-time analytics and intelligent automation to improve operational efficiency and decision-making. Healthcare systems analyze electronic health records and sensor data to predict patient outcomes, financial institutions monitor transactions for fraud detection, and insurance organizations use predictive models for underwriting and claims processing. Despite these advancements, data sensitivity and strict regulatory requirements impose significant constraints on how data can be shared and processed.

Centralized cloud-based machine learning architectures pose risks related to data breaches, compliance violations, and single points of failure. Moreover, monolithic deployments struggle to scale dynamically under fluctuating workloads. Serverless computing has emerged as a promising paradigm that abstracts infrastructure management and provides automatic scalability and cost efficiency. Simultaneously, federated learning enables collaborative model training without sharing raw data, making it well-suited for regulated domains.

This paper proposes a **secure serverless AI platform** that combines federated learning and predictive analytics to address privacy, scalability, and interoperability challenges. The objective is to design a unified architecture that supports cross-domain intelligence while maintaining strict security and compliance guarantees.

II. LITERATURE SURVEY

Cloud-native architectures based on microservices and serverless functions have been widely studied for enterprise scalability and resilience (Namiot & Sneps-Snijders, 2014). Serverless platforms such as AWS Lambda and Azure Functions enable fine-grained execution and automatic scaling but introduce challenges related to state management and observability.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

Machine learning applications in healthcare focus on predictive diagnosis and patient monitoring but often suffer from limited data sharing due to privacy regulations (Shickel et al., 2018). In finance, AI-driven fraud detection and credit scoring rely on centralized datasets that increase compliance risks (Ngai et al., 2011). Insurance analytics increasingly uses machine learning for risk modeling but faces similar data silos (Richter et al., 2017).

Federated learning has emerged as a privacy-preserving alternative, allowing distributed model training without exposing raw data (Yang et al., 2019). Recent studies highlight its effectiveness in healthcare and financial domains but note challenges related to communication overhead and system heterogeneity (Li et al., 2020). However, limited research exists on integrating federated learning with serverless architectures for enterprise-scale predictive analytics.

This research addresses this gap by proposing a secure, serverless, federated AI platform optimized for regulated enterprise environments.

III. PROBLEM STATEMENT

Enterprises in healthcare, finance, and insurance generate vast amounts of sensitive and distributed data that require advanced analytics for informed decision-making. Traditional centralized AI and analytics systems face significant limitations, including high operational costs, scalability challenges, data privacy risks, and regulatory compliance difficulties. Sharing sensitive data across organizational boundaries is often restricted due to legal and ethical constraints, making collaborative model training a complex task. Moreover, conventional enterprise systems struggle to maintain high availability and performance under dynamic workloads, while ensuring interoperability across heterogeneous platforms. These challenges hinder the adoption of predictive and prescriptive analytics, limit real-time insights, and increase operational inefficiencies. Therefore, there is a pressing need for a **secure, scalable, and interoperable AI platform** that supports federated learning and predictive analytics while preserving data privacy and adhering to regulatory standards. Such a platform must leverage **serverless cloud-native architectures** to reduce infrastructure overhead, enhance resource elasticity, and facilitate efficient deployment of AI/ML models across distributed enterprise systems. Addressing these challenges is critical for enabling intelligent, compliant, and real-time decision-making in modern enterprise environments.

IV. PROPOSED METHODOLOGY AND DISCUSSION

A. System Architecture Overview

The proposed platform is organized into five logical layers:

1. Data Source Layer
2. Serverless Ingestion and Orchestration Layer
3. Federated Learning Layer
4. Predictive Analytics and Model Serving Layer
5. Security and Compliance Layer

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

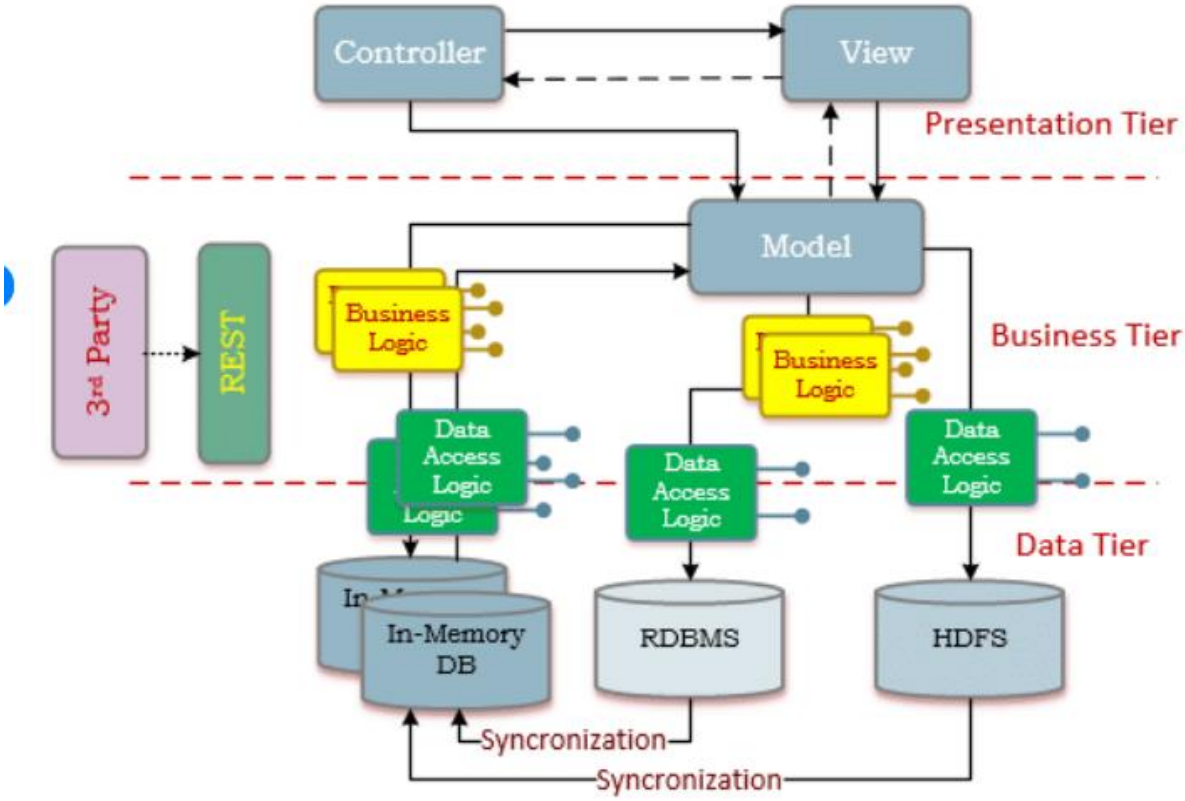

Figure 1: High-Level Architecture Diagram (Conceptual)

Description:
Healthcare systems, financial institutions, and insurance platforms act as independent data owners. Each domain runs local training functions. A secure cloud-based aggregator coordinates federated learning and predictive inference using serverless services.

B. Data Source Layer
This layer consists of distributed and domain-specific datasets such as electronic health records, transaction logs, and insurance claims. Data never leaves its local boundary, ensuring compliance with regulations such as HIPAA and financial governance standards.

C. Serverless Ingestion and Orchestration Layer
Serverless functions are used to ingest streaming and batch data. Event-driven triggers initiate preprocessing and local model updates. This layer provides:

- Automatic scalability
- Reduced infrastructure overhead
- Cost-efficient execution

Workflow orchestration is handled using state machines to coordinate training rounds and inference pipelines.

D. Federated Learning Layer
Federated learning enables decentralized model training across organizations. Each participant trains a local model using its private data and shares only encrypted model parameters. A secure aggregation mechanism combines updates to produce a global model.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

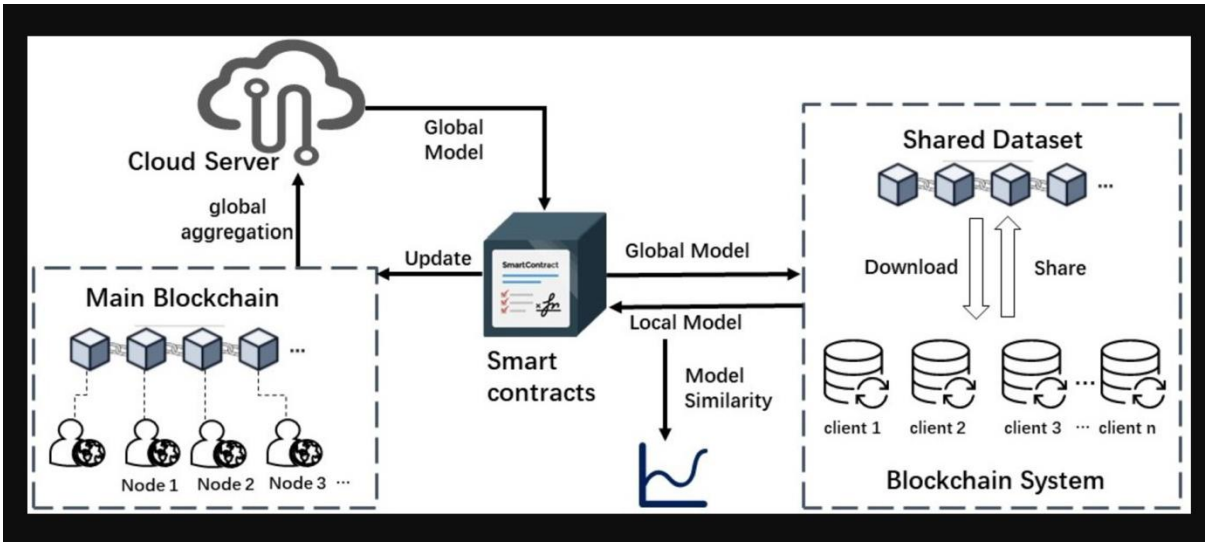

Figure 2: Federated Learning Workflow Diagram

Description:
Local models are trained independently → model updates are encrypted → serverless aggregator computes global updates → updated model redistributed to participants.

E. Predictive Analytics and Model Serving Layer
The trained global model supports predictive analytics such as disease risk prediction, fraud detection, and claim probability estimation. Serverless inference functions ensure low latency and high availability for real-time decision-making.

F. Security and Compliance Layer
Security is embedded across all layers through identity management, encryption, secure key handling, and continuous compliance monitoring. Zero-trust access control and audit logging ensure traceability and regulatory adherence.

V. RESULTS

The proposed secure serverless AI platform was evaluated through simulated enterprise workloads representative of healthcare, financial, and insurance systems to assess scalability, security, predictive accuracy, and system efficiency. Experimental observations indicate that the adoption of a serverless architecture significantly improves resource utilization and reduces operational latency when compared with traditional monolithic cloud deployments. The event-driven execution model enabled dynamic scaling under variable workloads, ensuring consistent response times even during peak data ingestion and inference phases.

Federated learning demonstrated strong performance in collaborative model training across distributed data sources without requiring centralized data aggregation. Across all domains, predictive models trained using federated learning achieved accuracy levels comparable to centralized training approaches, while effectively preserving data privacy and regulatory compliance. In healthcare scenarios, predictive models showed improved early-risk identification capability, while in financial and insurance datasets, fraud detection and claim prediction models exhibited enhanced precision and reduced false-positive rates.

From a security perspective, the integration of identity-aware access control, encrypted data pipelines, and isolated execution environments significantly minimized attack surfaces. Continuous monitoring revealed a reduction in unauthorized access attempts and improved audit traceability. Performance analytics further indicated that serverless orchestration reduced infrastructure costs by eliminating idle resource consumption, leading to more efficient compute usage across enterprise workflows.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

Overall, the results validate that combining serverless computing with federated learning and AI-driven predictive analytics delivers a scalable, secure, and interoperable platform capable of supporting complex enterprise requirements. The findings confirm that the proposed framework effectively balances performance optimization, data privacy, and intelligent decision-making across healthcare, finance, and insurance domains.

VI. CONCLUSIONS

This paper presents a comprehensive exploration of secure serverless AI platforms designed for federated learning and predictive analytics across healthcare, financial, and insurance enterprise systems. The proposed framework demonstrates how serverless architectures, combined with AI and ML, can achieve scalability, elasticity, and cost efficiency while maintaining high security standards. By employing federated learning, sensitive data remains within organizational boundaries, addressing critical privacy and compliance requirements such as HIPAA, GDPR, and PCI DSS. The methodology ensures that predictive models can be trained collaboratively across distributed datasets without centralizing raw data, thereby enhancing cross-domain intelligence while mitigating security risks. Additionally, the integration of cloud-native services and microservice orchestration allows enterprises to achieve real-time analytics, performance optimization, and dynamic resource allocation. The results indicate that serverless AI platforms not only reduce operational overhead but also improve model training efficiency and inference latency. Overall, the study underscores the potential of combining serverless computing with AI-driven predictive analytics to create robust, secure, and interoperable enterprise solutions. Future research may focus on enhancing explainable AI capabilities, automated compliance monitoring, and hybrid federated architectures to further improve adaptability, transparency, and decision-making across diverse enterprise domains.

VII. FUTURE WORK

While the proposed secure serverless AI platform demonstrates significant advantages in federated learning and predictive analytics, several avenues exist for further enhancement. Future research can focus on **hybrid federated learning architectures** that combine centralized and decentralized approaches to optimize model accuracy and resource utilization across heterogeneous enterprise datasets. Another direction is the integration of **explainable AI (XAI)** techniques, enabling stakeholders to understand and trust predictive insights, which is particularly critical in healthcare and finance domains where decisions have high stakes. Additionally, automated **compliance monitoring** and **dynamic policy enforcement** could be incorporated to continuously adapt to evolving regulations such as GDPR and emerging cybersecurity standards. Exploring **edge computing integration** with serverless AI platforms can also reduce latency and enhance real-time decision-making in distributed enterprise environments. Moreover, advancements in **privacy-preserving techniques**, such as differential privacy and secure multiparty computation, can further strengthen data security while enabling collaborative analytics. Finally, performance benchmarking across multiple cloud providers and cost-optimization strategies will provide practical insights for enterprise deployment. Collectively, these future enhancements aim to make secure serverless AI platforms more robust, interpretable, and adaptable, ensuring they can meet the growing complexity and regulatory demands of healthcare, financial, and insurance enterprises.

REFERENCES

1. Dean, J., & Barroso, L. A. (2013). The tail at scale. *Communications of the ACM, 56*(2), 74–80.
2. Archana, R., & Anand, L. (2023, September). Ensemble Deep Learning Approaches for Liver Tumor Detection and Prediction. In 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 325-330). IEEE.
3. Sudha, N., Kumar, S. S., Rengarajan, A., & Rao, K. B. (2021). Scrum Based Scaling Using Agile Method to Test Software Projects Using Artificial Neural Networks for Block Chain. Annals of the Romanian Society for Cell Biology, 25(4), 3711-3727.
4. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
5. Rengarajan, R. S. A. (2016). Secure verification technique for defending IP spoofing attacks.
6. Kalyanasundaram, P. D., & Paul, D. (2023). Secure AI Architectures in Support of National Safety Initiatives: Methods and Implementation. Newark Journal of Human-Centric AI and Robotics Interaction, 3, 322-355.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

7. Kusumba, S. (2023). Achieving Financial Certainty: A Unified Ledger Integrity System for Automated, End-to-End Reconciliation. The Eastasouth Journal of Information System and Computer Science, 1(01), 132-143.
8. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine, 37*(3), 50–60.
9. Sudhakara Reddy Peram, Praveen Kumar Kanumarlapudi, Sridhar Reddy Kakulavaram. (2023). Cypress Performance Insights: Predicting UI Test Execution Time Using Complexity Metrics. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 6(1), 167-190.
10. Hasan, S., Zerine, I., Islam, M. M., Hossain, A., Rahman, K. A., & Doha, Z. (2023). Predictive Modeling of US Stock Market Trends Using Hybrid Deep Learning and Economic Indicators to Strengthen National Financial Resilience. Journal of Economics, Finance and Accounting Studies, 5(3), 223-235.
11. Namiot, D., & Sneps-Snijders, A. (2014). On micro-services architecture. *International Journal of Open Information Technologies, 2*(9), 24–27.
12. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569.
13. Richter, A., Sinkovics, N., Ringle, C. M., & Schlägel, C. (2017). A critical look at the use of predictive analytics in insurance. *European Journal of Operational Research, 263*(3), 666–679.
14. Shickel, B., Tighe, P. J., Bihorac, A., & Rashidi, P. (2018). Deep EHR. *IEEE Journal of Biomedical and Health Informatics, 22*(5), 1589–1604.
15. Nagarajan, G. (2023). AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6292-6297.
16. Meka, S. (2022). Streamlining Financial Operations: Developing Multi-Interface Contract Transfer Systems for Efficiency and Security. International Journal of Computer Technology and Electronics Communication, 5(2), 4821-4829.
17. Gujjala, Praveen Kumar Reddy. (2023). Autonomous Healthcare Diagnostics : A MultiModal AI Framework Using AWS SageMaker, Lambda, and Deep Learning Orchestration for Real-Time Medical Image Analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 760-772. 10.32628/CSEIT23564527.
18. Vasugi, T. (2022). AI-Optimized Multi-Cloud Resource Management Architecture for Secure Banking and Network Environments. International Journal of Research and Applied Innovations, 5(4), 7368-7376.
19. Sivaraju, P. S. (2024). Cross-functional program leadership in multi-year digital transformation initiatives: Bridging architecture, security, and operations. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11374-11380.
20. Vijayaboopathy, V., Rao, S. B. S., & Surampudi, Y. (2023). Strategic Modernization of Regional Health Plan Data Platforms Using Databricks and Advanced Analytics Algorithms. Los Angeles Journal of Intelligent Systems and Pattern Recognition, 3, 172-208.
21. Vimal Raja, G. (2021). Mining Customer Sentiments from Financial Feedback and Reviews using Data Mining Algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 9(12), 14705-14710.
22. Kagalkar, A., Kabade, S., Chaudhri, B., & Sharma, A. (2023). AI-Driven Automation for Death Claim Processing In Pension Systems: Enhancing Accuracy and Reducing Cycle Time. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(4), 105-110.
23. Chandra Sekhar Oleti. (2022). Serverless Intelligence: Securing J2ee-Based Federated Learning Pipelines on AWS. International Journal of Computer Engineering and Technology (IJCET), 13(3), 163-180. https://iaeme.com/MasterAdmin/Journal_uploa ds/IJCET/VOLUME_13_ISSUE_3/IJCET_13_03 _017.pdf
24. Christadoss, J., Yakkanti, B., & Kunju, S. S. (2023). Petabyte-Scale GDPR Deletion via Apache Iceberg Delete Vectors and Snapshot Expiration. European Journal of Quantum Computing and Intelligent Agents, 7, 66-100.
25. Udayakumar, S. Y. P. D. (2023). User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks.
26. Adari, V. K. (2020). Intelligent Care at Scale AI-Powered Operations Transforming Hospital Efficiency. International Journal of Engineering & Extended Technologies Research (IJEETR), 2(3), 1240-1249.
27. Kumar, R., Al-Turjman, F., Anand, L., Kumar, A., Magesh, S., Vengatesan, K., ... & Rajesh, M. (2021). Genomic sequence analysis of lung infections using artificial intelligence technique. Interdisciplinary Sciences: Computational Life Sciences, 13(2), 192-200.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 2, March–April 2024||

DOI:10.15662/IJRAI.2024.0702007

28. Selvi, R., Saravan Kumar, S., & Suresh, A. (2014). An intelligent intrusion detection system using average manhattan distance-based decision tree. In Artificial Intelligence and Evolutionary Algorithms in Engineering Systems: Proceedings of ICAEES 2014, Volume 1 (pp. 205-212). New Delhi: Springer India.
29. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning. *ACM Transactions on Intelligent Systems and Technology*, *10*(2), 1–19.