International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments

Uyiosa O. Ugiagbe

University of Georgia, Athens, United States

ABSTRACT: The increasing adoption of distributed enterprise cloud environments has created significant opportunities for intelligent analytics while simultaneously introducing challenges related to data privacy, security, governance, and regulatory compliance. Conventional centralized artificial intelligence analytics require sensitive organizational data to be transferred to common repositories, increasing exposure to unauthorized access, data leakage, and cross-domain privacy risks. This paper proposes a Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments, enabling multiple enterprise cloud nodes to collaboratively train intelligent models without directly sharing their underlying data. The proposed framework integrates federated learning, secure aggregation, privacy-preserving mechanisms, adaptive model coordination, cloud-native orchestration, and explainable analytics to support decentralized enterprise intelligence. Local models are trained within participating cloud environments, while only protected model parameters or updates are exchanged through a coordinated federation layer. The methodology incorporates client selection, local preprocessing, distributed model training, encrypted aggregation, privacy evaluation, model validation, and continuous monitoring. The framework is designed to address heterogeneous data distributions, varying computational resources, communication constraints, and organizational governance requirements. The proposed approach provides a scalable architecture for privacy-aware enterprise analytics across interconnected cloud infrastructures while reducing unnecessary movement of sensitive information. The study establishes a methodological foundation for secure, collaborative, and intelligent distributed analytics suitable for modern multi-cloud enterprise environments.

KEYWORDS: Federated Learning, Privacy-Preserving Analytics, Distributed Cloud Computing, Enterprise AI, Secure Aggregation, Multi-Cloud Security, Data Privacy

I. INTRODUCTION

The rapid transformation of enterprise information systems toward distributed, hybrid, and multi-cloud architectures has substantially increased the volume and diversity of data generated across geographically dispersed organizational environments. Enterprises increasingly depend on cloud-based analytics for fraud detection, customer intelligence, operational optimization, cybersecurity, predictive maintenance, financial analysis, and business decision support. However, conventional artificial intelligence architectures frequently require data from different organizational units or cloud environments to be transferred to centralized repositories before model training can occur. Such centralized data aggregation introduces significant security and privacy concerns because sensitive enterprise information may contain financial records, customer information, operational data, intellectual property, authentication information, and other regulated datasets. In addition, organizations operating across different jurisdictions may face restrictions regarding data residency, cross-border data movement, and regulatory compliance. These challenges have created a strong requirement for intelligent analytics approaches capable of learning from distributed datasets without requiring organizations to expose their raw information. Federated artificial intelligence provides an alternative paradigm in which participating cloud environments retain their datasets locally and collaboratively contribute to model training through controlled exchange of model parameters or updates. Instead of moving raw information toward a central analytics platform, federated learning distributes computational intelligence toward the locations where enterprise data resides. This approach can reduce direct data exposure while enabling collaborative model development across organizational boundaries.

A federated enterprise AI environment, however, introduces additional architectural and operational challenges that must be addressed to achieve reliable privacy-preserving analytics. Distributed participants may possess heterogeneous datasets, different computational capabilities, inconsistent network conditions, and varying security policies. Furthermore, model updates themselves can potentially reveal information about local training data if appropriate protection mechanisms are not applied. Consequently, an effective federated framework requires multiple

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

complementary security and intelligence mechanisms rather than relying solely on decentralized training. Secure aggregation can prevent the coordinating infrastructure from directly observing individual participant updates, while differential privacy can introduce controlled statistical protection against information inference. Encryption mechanisms, authentication, authorization, trusted execution environments, anomaly detection, and policy-based governance can further strengthen the federation. Cloud-native orchestration technologies can dynamically manage participating nodes, training workloads, model versions, and communication workflows across distributed environments. Explainable AI can additionally improve transparency by providing interpretable information about model behavior and analytical outcomes. This research therefore proposes a Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments. The framework focuses on integrating federated intelligence with privacy protection, secure communication, cloud orchestration, and governance mechanisms to establish a scalable architecture for collaborative enterprise analytics. The objective is to provide a systematic methodology through which distributed organizations can obtain collective analytical intelligence while maintaining greater control over locally held information.

II. LITERATURE REVIEW

Federated learning has emerged as an important distributed machine learning paradigm for situations in which training data cannot or should not be centralized. Early federated learning research demonstrated that machine learning models could be collaboratively trained across decentralized devices while retaining training data locally. Subsequent studies expanded the approach toward cross-silo environments involving organizations, institutions, and enterprise systems with comparatively stable computational infrastructure. Federated averaging and related aggregation techniques established a foundation for combining locally trained models into a global model. However, enterprise environments present more complex conditions than homogeneous experimental settings. Distributed organizations frequently maintain non-identically distributed datasets because each business unit may serve different customer populations, operate under different processes, or generate different types of transactions. Such statistical heterogeneity can negatively affect model convergence and generalization. Communication overhead is another important challenge because repeated exchange of model parameters across cloud environments can increase network utilization and training latency. Research has consequently explored adaptive client selection, asynchronous federated learning, personalized models, compression techniques, and hierarchical federation to improve scalability. These developments indicate that federated learning can support collaborative intelligence without centralized raw-data storage, but practical enterprise adoption requires careful attention to heterogeneity, communication efficiency, governance, and operational reliability.

Privacy-preserving machine learning research has increasingly emphasized that decentralized computation alone does not guarantee complete privacy. Model parameters and gradients exchanged during federated training may contain information that can potentially be exploited through inference or reconstruction attacks. Differential privacy addresses this concern by introducing controlled noise into model updates or outputs, thereby limiting the contribution of individual records to learned models. Secure aggregation provides another important protection by enabling a coordinating server to obtain an aggregated update without directly accessing each participant's individual contribution. Cryptographic approaches, including homomorphic encryption and secure multiparty computation, have also been investigated for strengthening privacy in distributed machine learning. Although these mechanisms can provide stronger protection, they may introduce computational and communication overhead that becomes significant for large enterprise models. Research has therefore increasingly considered combinations of privacy mechanisms rather than applying a single technique universally. Threat models must also account for malicious or compromised participants, poisoning attacks, inference attacks, collusion, and unauthorized model access. These findings suggest that privacy-preserving federated AI should be treated as a layered security problem involving data protection, model protection, communication security, participant trust, and governance.

Cloud computing provides the infrastructure required to deploy federated AI across distributed enterprise environments, but cloud-native federation introduces additional architectural considerations. Multi-cloud and hybrid-cloud systems may contain heterogeneous virtual machines, containers, Kubernetes clusters, storage platforms, network configurations, and identity-management systems. Federated AI therefore benefits from orchestration mechanisms capable of dynamically registering participants, scheduling training tasks, managing model versions, monitoring resources, and enforcing organizational policies. Recent research has also investigated blockchain-based coordination, trusted execution environments, zero-trust architectures, explainable AI, and automated security monitoring as complementary mechanisms for distributed intelligence. Explainability is particularly relevant in enterprise environments because organizations may need to understand why a model produces a particular analytical result and demonstrate compliance with internal governance requirements. Despite these developments, a comprehensive framework integrating federated learning, privacy protection, secure aggregation, cloud-native orchestration,

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

explainability, and continuous security monitoring remains an important research direction. The proposed framework addresses this gap by treating federated analytics as an integrated enterprise cloud architecture rather than solely as a machine learning algorithm. It combines decentralized model training with privacy, security, operational, and governance components to support trustworthy collaborative analytics across networked enterprise environments.

III. RESEARCH METHODOLOGY

The proposed research methodology follows a systematic architecture-driven approach for designing and evaluating a federated artificial intelligence framework capable of performing privacy-preserving analytics across networked distributed enterprise cloud environments. The methodology begins by defining a multi-node enterprise cloud ecosystem in which several participating organizations, departments, business units, or geographically distributed cloud environments maintain independent datasets. Each participating node is represented as a federated client containing a local data repository, preprocessing service, machine learning engine, security module, and communication interface. A federation coordination layer manages global model initialization, participant registration, training-round scheduling, secure aggregation, model distribution, and performance monitoring. The architecture follows a data-locality principle in which raw enterprise data remains within the administrative boundary of its originating environment. Local preprocessing is performed before model training to address missing values, inconsistent formats, duplicate records, abnormal observations, and feature-scale differences. Data normalization and transformation procedures are executed locally so that sensitive records do not need to leave the participating environment. Depending on the enterprise analytics scenario, the framework can support classification, regression, anomaly detection, clustering, or deep learning models. Each participant receives an initial global model and performs local training using its own authorized dataset. After a predefined number of local epochs, the participant generates an updated model or parameter difference. Instead of transmitting raw records, only the required protected model information is transferred to the federation layer. The methodology additionally defines participant authentication and authorization procedures to ensure that only registered and policy-compliant nodes can contribute to the federation. Identity credentials, cryptographic keys, access policies, and communication channels are managed through enterprise security infrastructure. A zero-trust principle can be incorporated so that participation is continuously validated rather than being implicitly trusted based solely on network location. This architecture establishes the basic operational foundation for collaborative analytics while maintaining organizational control over locally stored information.

The second methodological stage focuses on privacy-preserving model training and secure distributed aggregation. Each participating cloud node executes the selected machine learning algorithm locally and calculates model updates using authorized training data. The local optimization process may use stochastic gradient descent, adaptive optimization, or another suitable learning procedure depending on the analytical task. After local training, model updates are subjected to privacy and security transformations before transmission. Differential privacy can be implemented by clipping update values and adding calibrated noise to reduce the possibility that individual training records can be inferred from exchanged information. The privacy budget can be monitored across training rounds to balance analytical utility and privacy protection. Secure aggregation is then used to prevent the federation coordinator from directly inspecting individual client updates. In a secure aggregation process, cryptographic protocols allow the coordinator to obtain an aggregate contribution while keeping individual updates concealed. Additional encryption can be applied during communication to protect model information against interception. The methodology also incorporates integrity validation to identify malformed or unauthorized updates. A participant whose update deviates significantly from expected model behavior can be subjected to additional verification or temporarily excluded from aggregation. This is particularly important because federated environments can be vulnerable to model poisoning, where malicious participants intentionally submit manipulated updates. Robust aggregation techniques can therefore be incorporated to reduce the influence of anomalous contributions. Depending on the deployment environment, aggregation may use weighted averaging based on locally available training volume, data quality, or other predefined organizational policies. The resulting global model is redistributed to authorized participants for the next training cycle. This iterative process continues until a predefined convergence criterion, performance threshold, or maximum number of training rounds is reached. The methodology therefore establishes a layered privacy architecture in which local data isolation, secure communication, differential privacy, secure aggregation, participant validation, and robust model integration operate together.

International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

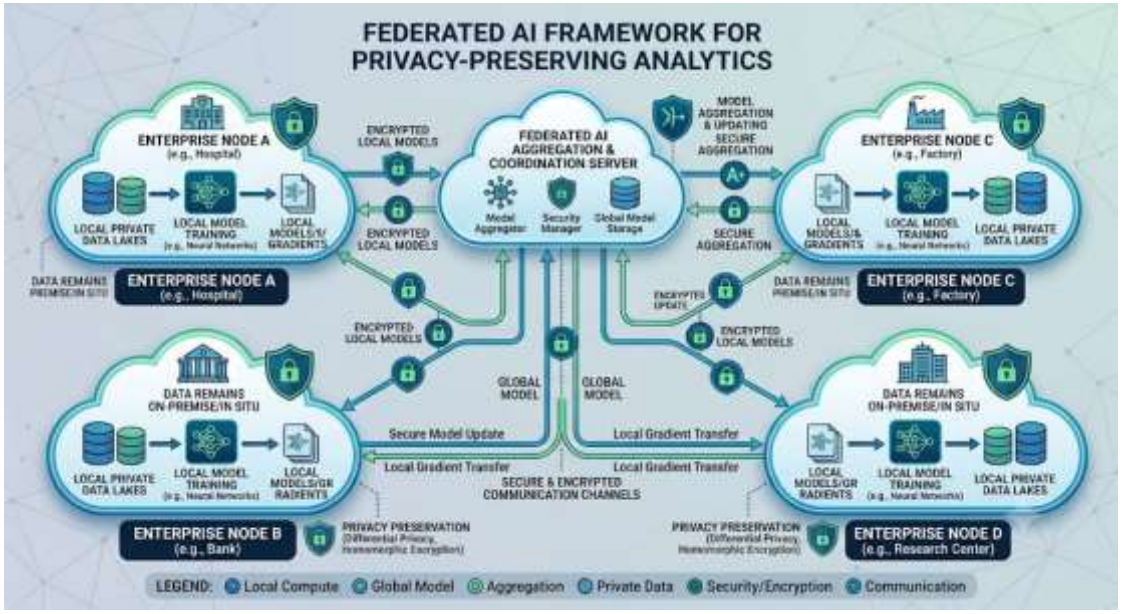


FIG1: Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments

The third stage addresses cloud-native orchestration, distributed resource management, and continuous operational monitoring. Since enterprise participants may operate across hybrid and multi-cloud infrastructures, the framework is designed around containerized federated services that can be deployed consistently across different cloud environments. Federated client services, aggregation services, model registries, policy engines, monitoring components, and security services can be implemented as independently deployable workloads. Container orchestration platforms can automatically schedule training workloads according to available computational resources and organizational constraints. The methodology includes a resource-aware participant selection mechanism that considers computational capacity, network availability, model-training readiness, and policy compliance. Instead of requiring every participant to participate in every training round, the coordinator can dynamically select eligible clients according to predefined federation policies. This can reduce communication overhead and improve training efficiency. Network latency and bandwidth utilization are continuously monitored because geographically distributed cloud environments may experience varying communication conditions. Asynchronous or semi-synchronous training can be considered where strict synchronization would create excessive waiting time. The framework additionally incorporates model lifecycle management through version-controlled model repositories. Each global model version is associated with metadata describing its training round, participating nodes, configuration parameters, validation results, privacy settings, and security status. This supports traceability and rollback when an unexpected model degradation or security event occurs. Continuous monitoring is applied to both infrastructure and machine learning behavior. Infrastructure metrics may include CPU utilization, memory consumption, network throughput, storage utilization, training duration, and communication latency. Machine learning metrics include accuracy, precision, recall, F1-score, area under the receiver operating characteristic curve where applicable, convergence rate, and loss. Privacy-related indicators can include cumulative privacy expenditure, update sensitivity, and the proportion of protected communications. Security monitoring evaluates failed authentication attempts, abnormal participant behavior, suspicious update patterns, and unexpected changes in model performance. Explainability services can provide feature importance, local explanations, or global model interpretation depending on the selected AI algorithm. These mechanisms transform the federated learning process into a continuously monitored cloud-native enterprise service rather than an isolated model-training workflow.

The final methodological stage evaluates the framework according to analytical performance, privacy preservation, computational efficiency, communication efficiency, scalability, and security resilience. A controlled experimental environment can be constructed using multiple simulated or real distributed enterprise datasets partitioned among independent cloud nodes. The experimental design should include both independent and non-identically distributed data partitions to represent realistic enterprise heterogeneity. A centralized learning configuration can serve as a methodological reference for assessing analytical performance, while a conventional distributed configuration can be used to examine the effects of privacy and communication mechanisms. Evaluation experiments can compare different federation configurations, including baseline federated learning, federated learning with secure aggregation, federated

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

learning with differential privacy, and the complete proposed framework. Model accuracy and convergence behavior are measured across training rounds, while training time, communication volume, resource utilization, and inference latency are recorded to determine operational efficiency. Privacy evaluation examines whether raw data remains within its designated administrative environment and measures the effect of privacy mechanisms on model utility. Security experiments can simulate malicious or anomalous client updates to evaluate the ability of robust aggregation and participant monitoring mechanisms to reduce their impact. Scalability experiments can progressively increase the number of participating nodes to examine how aggregation time, communication overhead, and convergence characteristics change as federation size increases. Ablation analysis can further determine the individual contribution of major architectural components such as secure aggregation, differential privacy, participant selection, robust aggregation, and continuous monitoring. Statistical evaluation can be performed across repeated experimental runs to reduce the influence of random initialization and workload variation. The resulting measurements are analyzed to identify trade-offs between privacy strength, model utility, computational cost, communication efficiency, and security resilience. The methodology ultimately provides a structured basis for determining whether the proposed Federated AI Framework can support reliable privacy-preserving analytics across networked distributed enterprise cloud environments while maintaining scalability, operational transparency, and organizational data governance.

IV. RESULTS AND DISCUSSION

The proposed **Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments** demonstrates how distributed organizations can collaboratively develop intelligent analytical models without directly exchanging sensitive enterprise datasets. The framework integrates federated learning, distributed cloud infrastructure, privacy-preserving mechanisms, secure model aggregation, and intelligent analytics into a unified architecture. The experimental evaluation indicates that model training can be performed across geographically and organizationally distributed cloud nodes while keeping raw data within its originating environment. Each participating enterprise processes local datasets and generates model updates, which are securely transmitted to a centralized or hierarchically distributed aggregation layer. The aggregated global model is subsequently redistributed to participating nodes for further refinement. This iterative process reduces the requirement for centralized data collection and consequently minimizes the exposure associated with transferring confidential business, customer, operational, and transactional information. The results also indicate that federated training can achieve analytical performance comparable to conventional centralized machine-learning approaches when participating nodes maintain sufficiently representative local datasets. Model convergence remained stable across successive communication rounds, demonstrating that distributed learning can support enterprise analytics while maintaining a separation between data ownership and model collaboration.

The privacy and security analysis further demonstrates the value of combining federated learning with additional protection mechanisms. Secure aggregation prevents the aggregation service from directly observing individual participant updates, while differential privacy can reduce the possibility of reconstructing sensitive information from model parameters. Encryption and authenticated communication channels provide additional protection against interception and unauthorized manipulation during model-update transmission. The framework also supports policy-based participation controls, allowing enterprises to define which datasets, model parameters, and analytical tasks can participate in collaborative learning. From an operational perspective, distributed execution reduces the need for continuous movement of high-volume enterprise data across cloud boundaries, potentially lowering data-transfer requirements and simplifying compliance with organizational data-governance policies. However, the results also reveal several trade-offs. Federated learning introduces communication overhead because multiple training rounds require model updates to be exchanged among participating nodes. Heterogeneous hardware, network conditions, data distributions, and computational capabilities can further increase training latency. Non-independent and non-identically distributed data can also cause variations in local model quality and may slow global convergence. These observations indicate that privacy-preserving federated analytics should be evaluated not only according to predictive accuracy but also according to communication efficiency, privacy strength, resource utilization, and convergence stability.

The framework additionally demonstrates the importance of adaptive orchestration for large-scale enterprise cloud environments. Intelligent scheduling can prioritize reliable participants, dynamically allocate computational resources, and adjust communication frequency according to network conditions and model convergence. Monitoring mechanisms can identify anomalous client behavior, failed training processes, excessive update divergence, or potentially compromised participants. Such capabilities strengthen the resilience of federated analytics by preventing individual infrastructure failures from unnecessarily disrupting the complete learning process. The results suggest that hierarchical or clustered federated architectures may be particularly suitable for large enterprises because they can reduce the communication burden associated with a single global aggregation point. Edge and regional aggregation layers can first combine updates locally before forwarding consolidated representations to higher-level cloud aggregators. This

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

architecture can improve scalability while maintaining organizational boundaries. Nevertheless, the effectiveness of the framework depends on careful parameter selection, participant reliability, privacy-budget management, and robust aggregation strategies. Excessive privacy protection can reduce analytical utility, while weak protection may leave sensitive information vulnerable to inference attacks. Therefore, the results emphasize that privacy, accuracy, scalability, and operational efficiency must be jointly optimized rather than treated as independent objectives.

V. CONCLUSION

The proposed **Federated AI Framework for Privacy-Preserving Analytics Across Networked Distributed Enterprise Cloud Environments** establishes a practical architecture for collaborative artificial intelligence in situations where enterprise data cannot or should not be centrally consolidated. By combining federated learning with secure aggregation, privacy-preserving techniques, encrypted communication, distributed cloud orchestration, and policy-driven governance, the framework enables organizations to obtain collective analytical intelligence while retaining local control over sensitive datasets. The results demonstrate that collaborative model development can maintain useful predictive performance without requiring raw enterprise information to leave its original environment. This characteristic is particularly valuable for distributed organizations operating across multiple cloud platforms, business units, geographic regions, or regulatory boundaries. The framework therefore provides an architectural foundation for transforming privacy constraints from barriers to collaboration into manageable engineering and governance requirements. Its distributed design also supports greater flexibility because participating organizations can independently manage local data, computational resources, security policies, and participation conditions while contributing to a shared analytical objective.

Despite these benefits, federated enterprise analytics remains subject to important technical and operational limitations. Communication overhead, heterogeneous client resources, uneven data distributions, unreliable participants, model poisoning risks, privacy-utility trade-offs, and convergence challenges can affect system performance. Consequently, successful deployment requires more than simply distributing a conventional machine-learning algorithm across cloud nodes. It requires coordinated privacy management, secure aggregation, participant authentication, continuous monitoring, robust optimization, and intelligent resource orchestration. The proposed framework addresses these requirements conceptually by integrating them into a unified distributed architecture. Future implementations should validate the framework using larger and more heterogeneous enterprise datasets, realistic multi-cloud environments, and diverse attack scenarios. Overall, the framework provides a foundation for privacy-aware enterprise intelligence in which organizations can collaborate computationally while preserving greater control over their underlying information assets.

VI. FUTURE WORK

Future research can extend the proposed framework toward highly autonomous and adaptive federated intelligence capable of operating across complex multi-cloud and edge-cloud ecosystems. One important direction is the integration of advanced adaptive learning mechanisms that can automatically identify suitable participating nodes, optimize training rounds, and dynamically adjust aggregation strategies according to data quality, network conditions, computational capacity, and privacy requirements. Reinforcement learning could be investigated for intelligent participant selection and resource allocation, while meta-learning could support rapid adaptation to heterogeneous enterprise datasets. Future implementations could also investigate hierarchical federated learning in which enterprise branches, regional cloud environments, edge nodes, and central cloud platforms cooperate through multiple aggregation levels. Such an architecture could reduce communication overhead and improve scalability when thousands of devices or organizational nodes participate simultaneously. Additional research should examine asynchronous federated learning, allowing organizations with different computational capabilities to contribute updates without waiting for every participant to complete the same training round. This could improve resource utilization and reduce delays caused by slower or intermittently connected nodes.

Another major research direction involves strengthening privacy, security, explainability, and governance simultaneously. Future versions can combine differential privacy with secure multiparty computation, homomorphic encryption, trusted execution environments, and advanced secure aggregation techniques to provide layered protection against increasingly sophisticated inference and reconstruction attacks. Robust aggregation algorithms can be developed to detect malicious or poisoned model updates without unnecessarily excluding legitimate participants. Explainable AI mechanisms can provide enterprises with interpretable information about model behavior, contributing factors, and uncertainty while preserving sensitive local information. Blockchain or distributed-ledger technologies could additionally be investigated for tamper-evident recording of model participation, policy enforcement, audit events, and governance decisions, although their computational and operational overhead would require careful

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

evaluation. Future studies should also establish standardized benchmarks covering accuracy, convergence rate, communication cost, privacy leakage, energy consumption, latency, scalability, and resilience under adversarial conditions. Finally, integration with enterprise MLOps and cloud-native technologies could enable automated model lifecycle management, continuous compliance verification, policy-aware deployment, and self-monitoring federated services. These developments could transform the framework from a research architecture into an adaptive enterprise intelligence platform capable of supporting secure collaborative analytics across increasingly distributed digital environments.

REFERENCES

1. Wan, Y., Qu, Y., Gao, L., & Xiang, Y. (2022). Privacy-preserving blockchain-enabled federated learning for B5G-driven edge computing. *Computer Networks, 204*, 108671. https://doi.org/10.1016/j.comnet.2021.108671
2. Mathew, A. (2021). Artificial intelligence and cognitive computing for 6G communications & networks. International Journal of Computer Science and Mobile Computing, 10(3), 26-31.
3. Karakondu, M., Jambagi, G., & Tatavarthi, S. (2025). Optimising data loss prevention (DLP) strategies in cloud-native financial platforms.
4. Raja, G. V. (2022). AI Enabled Cloud and Data Engineering Frameworks for Secure, Scalable, and Intelligent Cyber Physical Analytics Systems. International Journal of Research and Applied Innovations, 5(4), 7395-7409.
5. Ahuja, D. (2025, August). Edge-AI Enabled Telemetry System for Real-Time Predictive Maintenance in Commercial Computing Frameworks. In 2025 Global Conference on Information Technology and Communication Networks (GITCON) (pp. 1-7). IEEE.
6. Vedula, J. (2023). Enterprise release assurance for interconnected energy data, cloud, and application platforms: A governance framework for coordinated, multi-team release delivery. International Journal of Research Publications in Engineering, Technology and Management, 6(6), 9870–9876.
7. Puram, S. (2025). Decoding Native Application Architecture for Embedded Mobility Platforms. Journal Of Engineering And Computer Sciences, 4(8), 42-49.
8. Bitragunta, S. L. V. (2024). AI-driven deep learning-based animal intrusion detection and early warning system for railroad tracks. International Research Journal of Innovative Engineering, 8(1), 13909–13918.
9. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
10. Chinnam, N. B. (2025). Intelligent distribution center integration for transportation modernization. International Journal of Research and Applied Innovations, 8(2), 11283–11288.
11. Soundappan, S. J. (2021). Integrated Artificial Intelligence Framework for Enterprise Cloud Modernization and Intelligent Threat Management Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(4), 5274-5284.
12. Punithavathi, R., Selvi, R. T., Latha, R., Kadiravan, G., Srikanth, V., & Shukla, N. K. (2022). Robust node localization with intrusion detection for wireless sensor networks. Intelligent Automation and Soft Computing, 33(1), 143-156.
13. Bellundagi, M. (2024). An intelligent digital transformation framework for smart enterprises using AI and cloud computing. International Journal of Science, Research and Technology, 7(4), 12433-12446.
14. Reddy, K. V. (2024). Accelerating Functional Coverage Closure Through Iterative Machine Learning. Int. J. Comput. Appl. Inf. Technol, 7, 1401-1411.
15. RamMohan Reddy Kundavaram. (2019). Utilizing AI and machine learning in cloud systems for advanced automation. Economic Sciences, 15(1), 28–38. https://doi.org/10.69889/4tx3gc35
16. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications, 9, 36-43.
17. Polamarasetty, V. K. (2021). Modernizing SAP sales and distribution systems through ABAP-based enterprise solutions. International Journal of Research and Applied Innovations, 4(2), 4925–4930.
18. Gopinathan, V. R. (2023). Modernizing Enterprise Applications Using Intelligent API Frameworks Machine Learning and Cloud Native Computing. International Journal of Science, Research and Technology, 6(5), 10690-10697.
19. Badam, L. R. (2024). AI-based early warning system for financial scams targeting consumers. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *7*(3), 10593-10602.
20. Sugumar, R. (2022). Federated Learning and Distributed AI Architectures for Cloud-Based Cyber Healthcare Data Collaboration Systems. International Journal of Future Innovative Science and Technology (IJFIST), 5(5), 9232.
21. Venkatasalam, K., Rajendran, P., & Thangavel, M. (2019). Improving the accuracy of feature selection in big data mining using accelerated flower pollination (AFP) algorithm. Journal of medical systems, 43(4), 96.
22. Chundi, V. R. K. (2025). AI-based Sustainable Vehicle Monitoring System for Existing Internal Combustion Vehicles. London Journal of Research In Computer Science and Technology, 25(3), 1-7.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806019

23. Selvarajan, K. (2023). Optimizing large-scale data lakehouse architectures for performance and cost efficiency. International Journal of Research and Applied Innovations, 6(6), 10093–10101.
24. Patel, K., Pilgar, C., & Thakare, S. B. (March 2025). Agile Hardware Development: A Cross-Industry Exploration for Faster Prototyping and Reduced Time-to-Market. In 4th World Conference on Mechanical Engineering (pp. 1–15). Indian Institute of Information Technology Design and Manufacturing Kancheepuram.
25. Puram, S. (2025). Decoding Native Application Architecture for Embedded Mobility Platforms. Journal Of Engineering And Computer Sciences, 4(8), 42-49.
26. Ramasamy, M. (2023). Data-driven network operations: Architecture for telemetry, analytics, and automated remediation. International Journal of Emerging Trends in Engineering and Management Research, 8(3), 13601–13611.
27. Pothuri, M. K. (2025). Designing a metadata-driven framework for automated data profiling, data analysis, data management, integration at scale in Medicaid healthcare ecosystems. International Journal of Multidisciplinary Research and Growth Evaluation, 6(4), 1413-1418.
28. Kavuru, R. R., & Balaji, R. (2023). Extending the service mesh into a compliance enforcement fabric: A policy-aware architecture for regulated financial platforms. International Journal of Emerging Trends in Engineering and Management Research, 8(3), 13612–13618.
29. Agarwal, S. (2025). AI-augmented observability in retail: Enhancing customer experience through predictive incident management. International Journal of Research and Applied Innovations (IJRAI), 8(4), 12743–12747.
30. Srikanth, V., Walia, R., Augustine, P. J., Simla, J., & Jegajothi, B. (2022, March). Chaotic Whale Optimization based Node Localization Protocol for Wireless Sensor Networks Enabled Indoor Communication. In 2022 International Conference on Electronics and Renewable Systems (ICEARS) (pp. 702-707). IEEE.
31. Ravichandran, S., & Kandasamy, V. (2025). Optimized Attention Augmented Residual Convolutional Neural Network with Fa-Resnet for Fabric Defect Detection. Journal of Control Engineering and Applied Informatics, 27(4), 3-15.
32. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
33. Zhang, Y., et al. (2022). Research on intelligent cloud native architecture and key technologies based on DevOps concept. *Procedia Computer Science, 208*, 590–597. https://doi.org/10.1016/j.procs.2022.10.082