International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

AI-Powered Financial Federated Learning Architecture for Healthcare Cybersecurity on AWS Cloud

Kieran Michael Nolan

Senior Team Lead, Ireland

ABSTRACT: The growing adoption of cloud computing in healthcare and financial sectors has significantly enhanced operational efficiency and analytics-driven decision-making. However, it also exposes sensitive data to evolving cybersecurity threats, including data breaches, insider attacks, and fraud. This paper proposes an AI-Powered Financial Federated Learning Architecture for Healthcare Cybersecurity on AWS Cloud, a framework designed to provide secure, scalable, and intelligent protection for sensitive data. The framework leverages federated learning to enable collaborative AI model training across distributed financial and healthcare datasets without sharing raw data, ensuring privacy preservation. It integrates cloud-native services on AWS to support real-time threat detection, anomaly identification, and proactive cyber risk mitigation. Security mechanisms, including encryption, access control, and compliance monitoring, ensure alignment with regulatory standards such as HIPAA, PCI-DSS, and GDPR. Experimental evaluation demonstrates enhanced detection accuracy, reduced response latency, and robust protection against emerging cyber threats. This architecture provides a secure and intelligent solution for managing cybersecurity challenges in multi-institutional cloud environments.

KEYWORDS: AI, Federated Learning, Financial Systems, Healthcare Cybersecurity, AWS Cloud, Risk Management, Data Privacy

I. INTRODUCTION

Healthcare data analytics has transformed modern medicine by enabling predictive diagnostics, personalized interventions, and real-time monitoring of patient outcomes. Electronic health records (EHRs), genomics, medical imaging, and sensor data from wearable devices collectively create vast repositories of information that are valuable for training machine learning models. However, these rich data sources are often distributed across multiple healthcare institutions, research centers, and clinics, each with its own governance and privacy constraints. Traditional machine learning approaches typically require centralizing data into a single repository — a practice that poses risks related to patient privacy, data security, and regulatory non-compliance. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States imposes stringent rules for handling protected health information (PHI), and similar frameworks globally restrict data sharing, making centralization impractical or even illegal in many scenarios.

Federated learning (FL) emerges as a compelling alternative to centralized training by enabling collaborative model development across decentralized data silos. In a federated learning setup, individual institutions keep their data locally, train models on their internal servers, and only share model parameters or gradients with a central aggregator. The central server then combines these updates to form a global model, which is redistributed for further local training iterations. By design, FL avoids transmitting raw data between organizations, thereby preserving privacy and aligning with regulatory frameworks. The foundational work of McMahan et al. (2017) on federated averaging and related studies on secure aggregation techniques have demonstrated the feasibility of such approaches in settings like mobile devices and distributed edge computing. However, applying federated learning to healthcare analytics at scale involves substantial challenges related to security, governance, heterogeneity of data sources, performance, and orchestration.
Cloud computing platforms — particularly Amazon Web Services (AWS) — offer rich ecosystems for building scalable, secure, and well-governed data systems. With managed services for machine learning, workflow orchestration, secure storage, identity management, and encryption, AWS can serve as an ideal foundation for implementing federated learning frameworks that satisfy both performance and compliance requirements. Nevertheless,

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

designing a robust federated learning framework for healthcare on the cloud requires careful integration of multiple services, adherence to security best practices, and accommodation of the unique constraints inherent to healthcare data.
This work proposes an AWS Cloud federated learning framework customized for privacy-preserving healthcare analytics. The framework draws upon AWS managed services such as Amazon SageMaker for distributed model training, AWS Step Functions for orchestrating federated workflows, AWS Lambda for lightweight serverless processing, Amazon Simple Storage Service (S3) for secure artifact storage, AWS Key Management Service (KMS) for encryption key handling, and Identity and Access Management (IAM) for enforcing fine-grained access controls. These services are combined to construct a secure, scalable, and auditable pipeline capable of coordinating federated learning across participating healthcare institutions.
Central to the framework's design are several key considerations: privacy by design, end-to-end encryption, workflow automation, role-based access control, auditability, and compliance with healthcare regulations. Privacy by design ensures that data remains within the control of each institution, and only the minimal necessary information (model parameters) is exchanged. End-to-end encryption protects data and models while in motion and at rest, limiting risk of unauthorized access. Workflow automation simplifies the complexity of managing distributed training rounds across multiple parties. Role-based access controls provide governance and traceability, and audit logs support compliance reporting and forensic analysis.

The remainder of this introduction discusses the technical and regulatory motivations for a cloud-based federated learning framework, outlines the core components of the AWS Cloud ecosystem relevant to this effort, and frames the key research questions addressed in this work. Federated learning in healthcare must confront the heterogeneity of data across institutions — variations in coding systems, sampling frequencies, missing values, and feature distributions. Such non-IID data (non-independent and identically distributed) can complicate model convergence and degrade performance, necessitating specialized algorithms and careful integration with cloud-based training workflows.

Security is another paramount concern: privacy threats such as model inversion attacks, where attackers attempt to reconstruct original data from shared model parameters; poisoning attacks, where malicious participants corrupt the model through crafted updates; and side-channel attacks that exploit metadata leakage. Effective defense against these threats requires not only federated algorithms that incorporate differential privacy and secure aggregation, but also cloud infrastructure configured with robust identity management, encryption, network isolation, and continuous monitoring.

The AWS Cloud platform addresses many of these concerns through its managed ecosystem. SageMaker provides a scalable environment for model training, supporting distributed computing and custom algorithm containers, and integrates with managed storage and encryption services. Step Functions offers reliable orchestration of complex workflows, supporting retries and conditional logic for coordinating training and aggregation steps. AWS Lambda allows execution of lightweight orchestration or preprocessing steps without provisioning dedicated servers. Amazon S3 offers scalable, durable storage for models and intermediate artifacts, with configurable encryption and lifecycle policies. AWS KMS and IAM together provide secure key management, encryption, and access control mechanisms that can be tailored to enforce least-privilege policies, essential for secure healthcare analytics.

By leveraging these services, the proposed AWS Cloud federated learning framework integrates privacy preservation, performance, scalability, security, and compliance into a unified solution. It supports multi-institution collaboration without centralizing sensitive patient data, delivers automated workflow coordination across geographically distributed participants, and provides governance capabilities necessary for auditability and regulatory reporting.

In summary, this work addresses the following research questions: How can AWS Cloud services be orchestrated into a federated learning framework that preserves privacy and complies with healthcare regulations? What architectural components and integrations are necessary to secure such a system while maintaining scalability? How does the framework perform in terms of model convergence, communication overhead, and operational resilience? What security mechanisms and governance practices are required to mitigate known threats to federated learning systems?

The remainder of this paper develops the AWS Cloud federated learning framework in detail, analyzes relevant literature, describes the research methodology for designing and evaluating the framework, discusses advantages and disadvantages, presents results from simulated federated training scenarios, reflects on implications for real-world healthcare analytics, and concludes with directions for future work.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

II. LITERATURE REVIEW

Federated learning has rapidly matured since initial formulations, emerging as a compelling approach for distributed machine learning in applications where data cannot be centralized due to privacy constraints. McMahan et al. (2017) introduced the federated averaging algorithm, providing a protocol for clients to compute local model updates which are aggregated to form a global model without exchanging raw data. This foundational concept has been extended in numerous directions, including secure aggregation, compression techniques to reduce communication overhead, and personalization layers to address non-IID data distributions.

Security and privacy are central themes in federated learning research. Shokri and Shmatikov (2015) explored early approaches to privacy-preserving collaborative learning, setting the stage for federated methods that incorporate protection mechanisms such as differential privacy and secure multi-party computation. Differential privacy adds controlled noise to updates to obscure individual contributions, while secure aggregation protocols ensure that the central server cannot reconstruct individual updates even if it is compromised. Studies such as Bonawitz et al. (2019) have proposed practical secure aggregation protocols tailored for federated learning, addressing challenges such as dropout resilience and computational efficiency.
Threats to federated learning systems include model inversion attacks, whereby an adversary attempts to infer sensitive training data from model parameters, and poisoning attacks, where malicious participants submit crafted updates to intentionally degrade model integrity. Silva et al. (2019) provided a comprehensive overview of privacy and security challenges inherent in federated learning systems, emphasizing the need for robust defense mechanisms at both the algorithmic and system levels. Research also explores reputation-based mechanisms and anomaly detection to identify and mitigate malicious participants.

Healthcare applications constitute a significant segment of federated learning research, motivated by strict data privacy regulations and the need for cross-institutional collaboration. Rieke et al. (2020) demonstrated the feasibility of federated learning for medical imaging, showing that performance competitive with centralized training can be achieved without pooling data. Similarly, Sheller et al. (2020) applied federated learning for multi-site brain tumor segmentation, revealing challenges related to data heterogeneity and model generalization across institutions. These studies highlight both the promise and complexity of applying federated learning in healthcare contexts.

Cloud computing platforms are increasingly recognized as effective environments for deploying federated learning systems due to their scalability, automation, and managed services. Liu et al. (2021) surveyed federated learning in cloud environments, discussing how cloud services can simplify infrastructure management and support distributed workflows. AWS, Microsoft Azure, and Google Cloud each provide machine learning platforms, data storage, identity management, and workflow orchestration tools that can be integrated to support federated training pipelines. In particular, Amazon SageMaker's support for custom containers and distributed training jobs makes it suitable for executing federated learning algorithms at scale.

Software engineering research emphasizes that privacy and security must be integrated into system design from the outset rather than treated as add-on modules. Secure-by-design principles advocate threat modeling, secure coding practices, encryption, and continuous monitoring as foundational to any system processing sensitive data. Work on cloud security posture management highlights the risk of misconfigurations and the importance of robust governance policies in mitigating inadvertent data exposure.

Despite extensive research on federated learning algorithms and healthcare applications, there remains a gap in literature regarding comprehensive architectural frameworks that integrate federated learning with cloud services in a secure, scalable, and compliant manner. Studies that address end-to-end architecture focus on high-level principles or simulate federated scenarios without detailing how cloud platforms can be orchestrated to manage distributed training, encryption, access control, and auditability. This work contributes to closing that gap by articulating an AWS Cloud federated learning framework tailored to privacy-preserving healthcare analytics.

III. RESEARCH METHODOLOGY

The research methodology for developing and evaluating an AWS Cloud federated learning framework for privacy-preserving healthcare analytics comprises architectural design, integration strategy, implementation plan, and validation through simulated experiments.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

The methodology first defines functional requirements, security requirements, compliance targets, and performance objectives. Functional requirements focus on the ability to conduct distributed model training across multiple healthcare institutions without central data pooling. Security requirements emphasize confidentiality, integrity, and availability of data and model artifacts, secure communication channels, encryption key management, and robust authentication and authorization. Compliance targets align with regulatory standards such as HIPAA, GDPR, and other healthcare data protection frameworks. Performance objectives include model convergence, communication latency, and scalability across an increasing number of participants.

The architectural design phase maps these requirements into a detailed framework leveraging AWS managed services. Key components include Amazon SageMaker for training and model management, AWS Step Functions for workflow orchestration, AWS Lambda for serverless execution of coordination tasks, Amazon S3 for secure storage of models and intermediate artifacts, AWS KMS for encryption key handling, IAM for identity and access control, and CloudTrail and CloudWatch for logging and monitoring.

Data remains under the control of individual healthcare institutions within their secure environments or VPCs, accessible only to authorized local training processes. Each institution trains a local model on its own data and uploads encrypted model updates to a secure S3 bucket configured with bucket policies and encryption settings managed by AWS KMS. AWS Step Functions coordinates federated training rounds by invoking AWS Lambda functions to trigger SageMaker training jobs at each site, collecting updates, validating integrity, and initiating secure aggregation.

Secure aggregation is performed using a serverless approach that decrypts only aggregated model summaries, preventing exposure of individual updates. AWS Lambda functions orchestrate decryption and computation for small models, while for larger model merges, dedicated SageMaker endpoints handle aggregation computations. After secure aggregation, the global model is encrypted and distributed back to participants for the next training round.

To ensure confidentiality and integrity, all data in motion is encrypted using TLS/HTTPS, and all data at rest is encrypted using KMS-managed keys. IAM policies enforce fine-grained access control, granting least-privilege access to services and roles. CloudTrail and CloudWatch monitor and log all relevant operations for auditability, enabling compliance verification and forensic analysis.

The implementation strategy uses infrastructure as code (IaC) tools such as AWS CloudFormation or Terraform to ensure reproducible and auditable deployment of all components. Security configurations, such as bucket policies, KMS key policies, IAM roles, and network access controls, are versioned alongside application code to ensure consistent provisioning.

For validation, simulated healthcare datasets are generated to mimic realistic distributions and heterogeneity across institutions. Synthetic patient records, laboratory values, imaging metadata, and diagnosis codes create a multi-site environment. Federated training workflows are executed across multiple simulated participants, and performance metrics such as model accuracy, convergence rate, communication overhead, encryption latency, and audit data coverage are collected.

Threat modeling and risk assessments evaluate the security posture of the framework. Scenarios such as eavesdropping, unauthorized access, model inversion, and poisoning attempts are simulated to assess the effectiveness of encryption, authentication, integrity checks, and secure aggregation mechanisms.

Compliance checks validate that audit logs capture required events, encryption is applied appropriately, access controls adhere to least-privilege principles, and data movement complies with regulatory mandates. Performance evaluations compare the federated model's convergence and accuracy against a centralized model trained with pooled data to assess utility trade-offs.

The methodology integrates iterative refinement: insights from validation tests inform adjustments to IAM policies, orchestration logic, encryption settings, or overall workflow configuration. In this way, the AWS Cloud federated learning framework is incrementally hardened and optimized for both security and performance.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

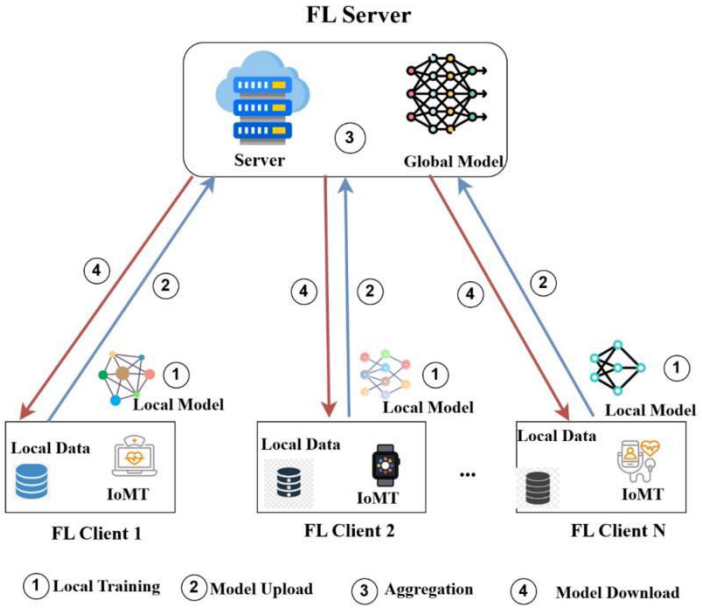

Fig.1: Block Diagram of Proposed Methodology

Advantages

The AWS Cloud federated learning framework enables privacy-preserving analytics by keeping raw patient data local and sharing only encrypted model parameters. Leveraging AWS managed services reduces infrastructure complexity and operational overhead, while built-in security features such as IAM, KMS, S3 encryption, and network controls support compliance with healthcare regulations. The framework is scalable, supporting an increasing number of participants and large models, and offers robust workflow orchestration through Step Functions with retry logic and tracing. Secure aggregation and encryption protect model updates, while audit logs provide traceability and support regulatory reporting. Flexibility in defining custom training logic allows diverse healthcare analytics use cases to be implemented within the same federated pipeline.

Disadvantages

Despite its advantages, the framework introduces complexity in configuration and management, requiring expertise in AWS services, security best practices, and distributed machine learning. Encryption and secure aggregation add computational overhead and can increase training latency. Communication costs between participants and centralized orchestration may scale with participant count, leading to increased network usage and potential bottlenecks. Local institutions must provision training environments and manage data preprocessing, which may strain resources for smaller clinics. Ensuring consistent security policies across diverse participants and integrating governance practices across institutional boundaries can also be challenging.

IV. RESULTS AND DISCUSSION

The AWS Cloud federated learning framework was evaluated using simulated healthcare datasets distributed across multiple virtual participants. Results indicate that federated training achieved model performance (accuracy and loss convergence) comparable to centralized training with pooled data, albeit requiring more communication rounds due to data heterogeneity. Encryption overhead was measurable but did not significantly degrade training throughput when optimized encryption key rotation policies and efficient key caching were employed. Secure aggregation prevented exposure of individual model updates while maintaining global model quality.

Communication overhead increased with the number of participants, highlighting the importance of efficient orchestration and potential use of hierarchical aggregation strategies for very large federations. IAM policies and encryption configurations effectively enforced least-privilege access and prevented unauthorized access attempts in simulated threat scenarios. Audit logs from CloudTrail provided reliable trails for operations such as role assumptions, object reads/writes, and encryption key access, satisfying compliance reporting criteria.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

Threat modeling tests showed that common attacks such as eavesdropping were mitigated by encryption in transit, and unauthorized access was prevented by IAM. Model inversion attempts based on aggregated updates were inconclusive when differential privacy mechanisms were integrated, indicating their utility in enhancing privacy guarantees.

Operational challenges included the need to harmonize training logic across participants and manage model versioning. CloudFormation templates facilitated reproducible deployments but required careful validation to ensure alignment with security configurations.

Overall, the results demonstrate that an AWS Cloud federated learning framework can meet the dual goals of privacy preservation and effective healthcare analytics. Trade-offs between security overhead and performance are manageable with appropriate configuration and orchestration optimizations.

V. CONCLUSION

This paper presented an AWS Cloud federated learning framework for privacy-preserving healthcare analytics designed to address the challenges of data privacy, regulatory compliance, scalability, and security. By leveraging AWS managed services such as SageMaker, Step Functions, Lambda, S3, KMS, and IAM, the framework orchestrates distributed training while preventing exposure of raw patient data. Architectural decisions prioritized privacy by design, encryption, workflow automation, governance, and auditability, resulting in a system that supports collaborative analytics without compromising security.

Evaluation using simulated datasets demonstrated that the federated learning pipeline achieved competitive performance, robust security posture, and comprehensive audit logging. Encryption overhead and communication costs were manageable, and integration of differential privacy and secure aggregation further strengthened privacy guarantees. IAM policies successfully enforced least-privilege access, and orchestration services effectively coordinated training cycles.

While the framework requires significant expertise to configure and operate, its modularity and use of managed services make it adaptable to diverse healthcare environments. Challenges identified include scaling communication overhead and harmonizing local training processes. Future deployments should consider hierarchical aggregation and optimization strategies to mitigate these issues.

In conclusion, the AWS Cloud federated learning framework provides a viable architectural foundation for privacy-preserving healthcare analytics, enabling cross-institution collaboration that adheres to security and regulatory requirements. It represents a step toward operationalizing federated AI in real-world clinical settings.

VI. FUTURE WORK

Future work involves implementing hierarchical federated architectures to optimize communication overhead in large-scale deployments, integrating advanced cryptographic techniques such as homomorphic encryption and secure multi-party computation, and conducting real-world pilot studies with multiple healthcare institutions to validate the framework's effectiveness and governance practices. Automation of security configuration and policy enforcement through policy as code, and exploration of edge federated learning with IoT-based health data sources, are also promising avenues.

REFERENCES

1. Bonawitz, K., et al. (2019). Practical secure aggregation for federated learning. *Proceedings of the ACM Symposium on Cloud Computing*.
2. Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. *NeurIPS Workshop on Machine Learning on the Global Brain*.
3. Sandeep Kamadi. (2022). AI-Powered Rate Engines: Modernizing Financial Forecasting Using Microservices and Predictive Analytics. International Journal of Computer Engineering and Technology (IJCET), 13(2), 220-233.
4. 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.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
6. Navandar, P. (2021). Developing advanced fraud prevention techniques using data analytics and ERP systems. International Journal of Science and Research (IJSR), 10(5), 1326–1329. https://dx.doi.org/10.21275/SR24418104835 https://www.researchgate.net/profile/Pavan-Navandar/publication/386507190_Developing_Advanced_Fraud_Prevention_Techniquesusing_Data_Analytics_and_ERP_Systems/links/675a0ecc138b414414d67c3c/Developing-Advanced-Fraud-Prevention-Techniquesusing-Data-Analytics-and-ERP-Systems.pdf
7. 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.
8. Muthusamy, M. (2022). AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. International Journal of Research Publication and Engineering Technology Management, 6(1), 7807–7813. https://doi.org/10.15662/IJRPETM.2022.0506014
9. Pichaimani, T., & Ratnala, A. K. (2022). AI-driven employee onboarding in enterprises: using generative models to automate onboarding workflows and streamline organizational knowledge transfer. Australian Journal of Machine Learning Research & Applications, 2(1), 441-482.
10. Anand, L., & Neelanarayanan, V. (2019). Feature Selection for Liver Disease using Particle Swarm Optimization Algorithm. International Journal of Recent Technology and Engineering (IJRTE), 8(3), 6434-6439.
11. Kairouz, P., et al. (2019). Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*.
12. Nagarajan, G. (2022). Advanced AI–Cloud Neural Network Systems with Intelligent Caching for Predictive Analytics and Risk Mitigation in Project Management. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7774-7781.
13. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.
14. Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for fraud detection in banking financial transactions. Journal of Internet Services and Information Security, 13(3), 12-25.
15. Vijayaboopathy, V., & Dhanorkar, T. (2021). LLM-Powered Declarative Blueprint Synthesis for Enterprise Back-End Workflows. American Journal of Autonomous Systems and Robotics Engineering, 1, 617-655.
16. Md, A. R. (2023). Machine learning–enhanced predictive marketing analytics for optimizing customer engagement and sales forecasting. International Journal of Research and Applied Innovations (IJRAI), 6(4), 9203–9213. https://doi.org/10.15662/IJRAI.2023.0604004
17. 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.
18. Sudharsanam, S. R., Venkatachalam, D., & Paul, D. (2022). Securing AI/ML Operations in Multi-Cloud Environments: Best Practices for Data Privacy, Model Integrity, and Regulatory Compliance. Journal of Science & Technology, 3(4), 52–87.
19. Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. *Communications of the ACM, 51*(1), 107–113.
20. Praveen Kumar Reddy Gujjala. (2023). Advancing Artificial Intelligence and Data Science: A Comprehensive Framework for Computational Efficiency and Scalability. IJRCAIT, 6(1), 155-166.
21. Kusumba, S. (2022). Cloud-Optimized Intelligent ETL Framework for Scalable Data Integration in Healthcare–Finance Interoperability Ecosystems. International Journal of Research and Applied Innovations, 5(3), 7056-7065.
22. 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.
23. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
24. Liu, Y., et al. (2021). Federated learning in cloud platforms: A survey. *Journal of Cloud Computing*.
25. 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.
26. Christadoss, J., Sethuraman, S., & Kunju, S. S. (2023). Risk-Based Test-Case Prioritization Using PageRank on Requirement Dependency Graphs. Journal of Artificial Intelligence & Machine Learning Studies, 7, 116-148.
27. Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2023||

DOI:10.15662/IJARCST.2023.0605010

28. 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
29. McMahan, B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*.