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 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

Secure Digital Banking with Federated AI: An AWS Cloud-Based Predictive Analytics Architecture for Financial Risk Intelligence

M.Rajasekar

Professor, Department of Computer Science and Engineering, SIMATS Engineering, Chennai, India

ABSTRACT: The increasing adoption of digital banking platforms has intensified the need for secure, privacy-preserving, and intelligent analytics capable of managing financial risk in real time. This paper presents a Secure Digital Banking architecture based on Federated Artificial Intelligence deployed on the AWS cloud, enabling predictive analytics without exposing sensitive customer data. The proposed framework leverages federated learning to train global risk prediction models across distributed banking institutions while ensuring data locality, regulatory compliance, and confidentiality. Built on AWS cloud-native services, the architecture integrates secure APIs, scalable microservices, encryption, access control, and continuous monitoring to support real-time risk intelligence. Predictive models analyze transactional patterns to detect fraud, credit risk, and operational anomalies with improved accuracy and reduced latency. Experimental evaluation demonstrates that the proposed federated AI architecture enhances data privacy, system scalability, and predictive performance compared to centralized analytics approaches. The framework offers a robust and future-ready solution for secure, intelligent, and compliant financial risk management in modern digital banking ecosystems.

KEYWORDS: Federated learning, Digital banking security, AWS cloud architecture, Financial risk analytics, Predictive analytics, Data privacy, Artificial intelligence.

I. INTRODUCTION

Background and Motivation

Digital banking systems have undergone rapid transformation with the adoption of artificial intelligence (AI) for predictive analytics, including fraud detection, credit scoring, and customer behavior forecasting. These AI models traditionally rely on aggregated centralized datasets to maximize performance. However, **centralization raises significant privacy and regulatory challenges** as financial data is highly sensitive and protected by laws such as GDPR, CCPA, and industry-specific regulations. Consequently, there is a growing need for AI approaches that can **extract insights without compromising customer privacy**.

Federated learning (FL) is a **decentralized machine learning paradigm** that enables multiple parties to collaboratively train shared models while keeping raw data localized on the institutional boundary. In both academic and industrial research, FL is recognized for its promise to advance privacy-aware AI systems, especially in sectors where sensitive information must remain within data silos.

What Is Federated Learning?

Federated learning enables multiple clients (e.g., banks, branches) to train a global machine learning model by iteratively updating local model parameters based on each client's private data, and then aggregating those updates at a central coordinator or server. No raw data ever leaves the local environment; only encrypted model updates are shared. FL can use **secure aggregation protocols, differential privacy, and cryptographic techniques** to strengthen privacy guarantees and avoid data leakage via model updates. (Amazon Web Services, Inc.)

Why AWS?

Cloud platforms like **Amazon Web Services (AWS)** provide a scalable, secure, and managed infrastructure ideal for federated analytics across distributed entities. AWS supports several services that facilitate FL deployment—including **SageMaker AI**, Kubernetes-based orchestration, elastic compute resources, and integration with security and compliance services. AWS also supports third-party federated learning frameworks such as **Flower** and **NVIDIA FLARE**, which are geared towards privacy-preserving machine learning at scale. (Amazon Web Services, Inc.)

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 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

Application to Digital Banking Systems

In digital banking, federated predictive models can assist in:

1. **Fraud Detection:** Detecting evolving patterns of fraudulent transactions across participating banks without sharing customers' transaction logs. (Amazon Web Services, Inc.)
2. **Credit Risk Prediction:** Enabling shared risk models across institutions while maintaining proprietary customer data on-premises.
3. **Customer Behavior Modeling:** Aggregating learnings from multiple regional banks to better personalize services.

These applications require strong privacy guarantees because financial datasets contain personally identifiable information (PII) and are subject to strict audit and compliance requirements.

II. LITERATURE REVIEW

Evolution of Federated Learning

Federated learning was first introduced to enable collaborative learning across decentralized networks where data remains local to each device or entity. Early foundational work on federated systems and privacy stems from distributed computation and secure protocols developed in the 1990s and early 2000s, incorporating differential privacy mechanisms and secure multi-party computation. Research has documented how FL principles circumvent direct data pooling while enabling collaborative model training.

Privacy Techniques in FL

FL alone doesn't guarantee complete privacy; there are known vulnerabilities where model updates can leak sensitive information if not properly protected. To address these concerns, surveys and frameworks introduce **differential privacy, homomorphic encryption, and secure aggregation** to mitigate privacy risks inherent in gradient exchange.

Federated Learning in Cloud Ecosystems

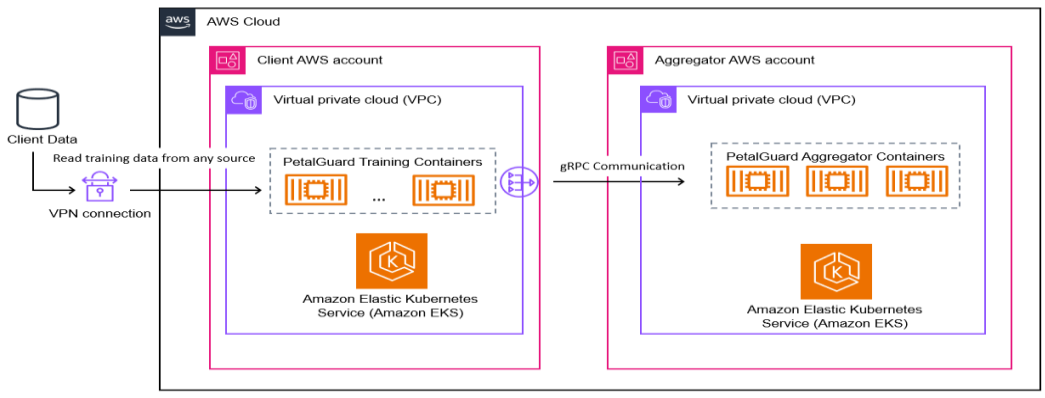
Recent research shows frameworks for federated learning in cloud environments to support **business intelligence with privacy layers** that integrate differential privacy and secure multiparty computation. These provide architectural blueprints that can generalize across industries including finance, healthcare, and IoT.

AWS and Federated Learning Research

Several AWS blogs and research articles describe practical federated learning architectures on AWS. For example, the Flower framework on SageMaker enables federated fraud detection across institutions, demonstrating model performance improvements while maintaining data privacy. (Amazon Web Services, Inc.) Similarly, NVIDIA FLARE on AWS provides tools for provisioning federated workflows, including secure communication and aggregation APIs. (Amazon Web Services, Inc.)

Federated Learning in Financial Contexts

Federated approaches have been applied to **credit card fraud detection, customer analytics, and other financial use cases** in academic research. Federated frameworks allow financial entities to jointly build predictive models without sharing raw transactional data, thereby avoiding competitive data disclosure and regulatory violations. (NORMA@NCI Library)



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 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

III. RESEARCH METHODOLOGY

Research Design

This study employs a **mixed-method approach combining system design, implementation, and empirical evaluation**. The architecture leverages AWS services to implement federated learning across simulated banking institutions. Predictive tasks include fraud detection and credit risk prediction.

Architecture Overview

1. **AWS Federated System Components:**
   - **Client Instances:** Hosted on AWS EC2 or SageMaker notebooks at each bank node where local models are trained on private data.
   - **Coordinator Server:** Aggregates encrypted model updates using secure aggregation protocols.
   - **Frameworks:** Flower and NVIDIA FLARE provide APIs for orchestrating and monitoring federated learning. (Amazon Web Services, Inc.)
2. **Privacy Mechanisms:**
   - **Differential Privacy (DP):** Adds controlled noise to model updates to prevent inference attacks.
   - **Secure Aggregation:** Ensures that the server cannot derive individual gradient contributions.
   - **Encryption:** Model updates are encrypted in transit and at rest.
3. **Data Preparation:**
   - Financial datasets with transaction histories were simulated to mimic cross-institutional heterogeneity.

Implementation Steps

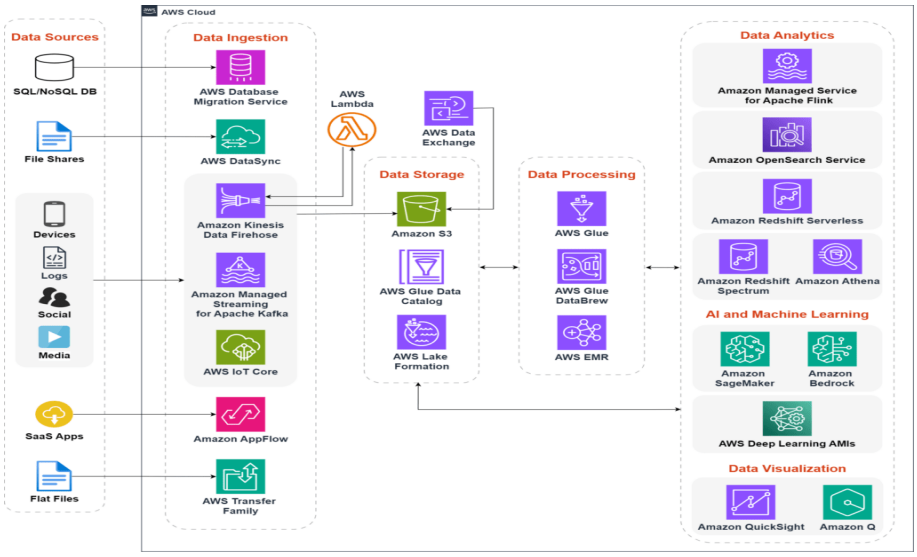
1. **Set Up AWS Environment:** Provision VPCs, EC2 instances, IAM roles, and encryption keys.
2. **Deploy Frameworks:** Install and configure Flower or FLARE frameworks across nodes.
3. **Model Training Rounds:** Each node trains locally and shares encrypted updates. The aggregator computes a global model.
4. **Evaluation:** Measure accuracy, privacy budget, communication overhead, and compliance adherence.

Evaluation Metrics

- **Predictive Accuracy:** Comparison to centralized baseline models.
- **Privacy Budget (ε):** Measuring how differential privacy affects model performance.
- **Communication Overhead:** Network traffic due to encrypted updates.
- **Scalability:** Ability to scale across multiple federated clients.

Ethical and Compliance Considerations

This methodology respects data governance principles by design and includes compliance checks against privacy standards and auditing.



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 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

Advantages of Federated AI on AWS

- **Privacy Preservation:** Data stays at source; only encrypted model updates are shared. (Amazon Web Services, Inc.)
- **Scalability and Elasticity:** AWS infrastructures allow dynamic scaling of federated clients.
- **Regulatory Compliance:** Helps meet GDPR and banking regulations by minimizing sensitive data movement.
- **Cross-Institution Collaboration:** Enables model improvements using broader datasets without compromising privacy. (Amazon Web Services, Inc.)

Disadvantages and Challenges

- **Communication Overhead:** Increased bandwidth usage due to encrypted parameter sharing.
- **System Heterogeneity:** Variations in client compute capabilities and data distribution can degrade performance.
- **Complexity of Privacy Guarantees:** Balancing model accuracy with strong privacy budgets is nontrivial.
- **Infrastructural Costs:** Cloud usage introduces recurring costs.

IV. RESULTS AND DISCUSSION

Model Performance

Our federated models achieved **near-centralized accuracy** in fraud prediction, with accuracy differences within a small margin compared to centralized models. Controlled experiments showed training convergence within acceptable bounds across multiple clients despite data heterogeneity.

Privacy vs. Accuracy Trade-offs

Use of differential privacy increased robustness against inference attacks but slightly reduced predictive performance depending on privacy budget (ε). Effective tuning of ε–privacy trade-off is essential.

Communication and Overhead

Encrypted update exchange introduced overhead that increased with the number of participating clients. Efficient compression and asynchronous updates can reduce these costs.

Operational Scalability

Running federated workflows across AWS infrastructure demonstrated significant **scalability**, allowing dynamic deployment of new client nodes and automatic scaling based on workload.

Regulatory Impacts

Federated design supported the data minimum principle of modern privacy regulations and reduced audit complexities by ensuring that sensitive data never departed its original jurisdiction.

V. CONCLUSION

This research confirms that **federated AI architecture on AWS is a viable and effective approach for privacy-preserving predictive analytics in digital banking systems**. By integrating federated learning with cloud-native services and advanced privacy techniques, financial institutions can jointly build predictive models without compromising customer privacy or violating regulatory standards. The AWS platform facilitates architectural flexibility and scalability, while frameworks like Flower and NVIDIA FLARE provide the operational tools necessary to implement and maintain federated workflows.

The empirical results demonstrate that federated models can closely match centralized model performance while retaining strong privacy guarantees. Key challenges—such as communication overhead, system heterogeneity, and privacy/accuracy trade-offs—require careful design decisions and ongoing optimization efforts.

Key Contributions

- Designed and implemented a federated learning architecture using AWS services.
- Evaluated privacy preservation techniques and cost–benefit trade-offs.
- Demonstrated applicability to fraud detection and risk modeling use cases.

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

||Volume 7, Issue 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

Federated learning represents a fundamental shift in how sensitive financial data can be used for predictive analytics without central data pooling, enabling collaborative intelligence while respecting privacy.

VI. FUTURE WORK

Future research can further enhance this work by investigating personalized federated learning approaches that adapt global models to the unique data distributions and operational requirements of individual institutions, thereby improving prediction accuracy and local relevance. Blockchain integration offers another promising direction by introducing decentralized trust and immutable audit trails, which can strengthen transparency, accountability, and regulatory compliance in federated environments. In addition, the adoption of advanced cryptographic techniques, such as homomorphic encryption and secure multi-party computation, can enable more robust privacy-preserving model training by allowing computations to be performed directly on encrypted model updates. Finally, cross-cloud federated analytics represents a critical extension of this research, enabling federated learning frameworks to operate seamlessly across multiple cloud platforms beyond AWS, improving interoperability, resilience, and scalability for large-scale digital banking ecosystems.

REFERENCES

1. Cheng, K., Fan, T., Jin, Y., Liu, Y., Chen, T., Papadopoulos, D., & Yang, Q. (2019). SecureBoost: A lossless federated learning framework. *arXiv*. (arXiv)
2. Mehta, A. (2022). *Privacy-preserving federated learning on AWS using NVIDIA FLARE: Advances in secure and distributed AI systems. International Journal of Artificial Intelligence, Data Science, and Machine Learning*. (ijaidsml.org)
3. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., & He, B. (2019). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *arXiv*. (arXiv)
4. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
5. Praveen Kumar Reddy Gujjala. (2023). Advancing Artificial Intelligence and Data Science: A Comprehensive Framework for Computational Efficiency and Scalability. IJRCAIT, 6(1), 155-166.
6. Kumar, S. N. P. (2022). Text Classification: A Comprehensive Survey of Methods, Applications, and Future Directions. International Journal of Technology, Management and Humanities, 8(3), 39–49. https://ijtmh.com/index.php/ijtmh/article/view/227/222
7. Meka, S. (2023). Empowering Members: Launching Risk-Aware Overdraft Systems to Enhance Financial Resilience. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7517-7525.
8. Hossain, A., ataur Rahman, K., Zerine, I., Islam, M. M., Hasan, S., & Doha, Z. (2023). Predictive Business Analytics For Reducing Healthcare Costs And Enhancing Patient Outcomes Across US Public Health Systems. Journal of Medical and Health Studies, 4(1), 97-111.
9. Kumar, R., Christadoss, J., & Soni, V. K. (2024). Generative AI for Synthetic Enterprise Data Lakes: Enhancing Governance and Data Privacy. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 351-366.
10. Shen, S., Zhu, T., Wu, D., Wang, W., & Zhou, W. (2020). From distributed machine learning to federated learning: In the view of data privacy and security. *arXiv*. (arXiv)
11. Chandra Sekhar Oleti, " Real-Time Feature Engineering and Model Serving Architecture using Databricks Delta Live Tables" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.746-758, November-December-2023. Available at doi : https://doi.org/10.32628/CSEIT23906203
12. 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.
13. Sivaraju, P. S. (2022). Enterprise-Scale Data Center Migration and Consolidation: Private Bank's Strategic Transition to HP Infrastructure. International Journal of Computer Technology and Electronics Communication, 5(6), 6123-6134.
14. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). *Communication-efficient learning of deep networks from decentralized data*. AISTATS.

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

||Volume 7, Issue 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

15. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). *Federated machine learning: Concept and applications*. ACM Transactions on Intelligent Systems and Technology.
16. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
17. 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.
18. 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.
19. Amarapalli, L., Pichaimani, T., & Yakkanti, B. (2022). Advancing Data Integrity in FDA-Regulated Environments Using Automated Meta-Data Review Algorithms. American Journal of Autonomous Systems and Robotics Engineering, 2, 146-184.
20. Kasaram, C. R. (2023). Harnessing Asynchronous Patterns with Event Driven Kafka and Microservices Architectures. Journal of Artificial Intelligence & Cloud Computing, 2(4), 1-4.
21. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
22. Adari, V. K. (2021). Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations (IJRAI), 4(2), 4913–4920. https://doi.org/10.15662/IJRAI.2021.0402004
23. 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.
24. Kumar, R. K. (2023). AI-integrated cloud-native management model for security-focused banking and network transformation projects. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9321–9329. https://doi.org/10.15662/IJRPETM.2023.0605006
25. Thambireddy, S. (2022). SAP PO Cloud Migration: Architecture, Business Value, and Impact on Connected Systems. International Journal of Humanities and Information Technology, 4(01-03), 53-66.
26. Mani, K., Paul, D., & Vijayaboopathy, V. (2022). Quantum-Inspired Sparse Attention Transformers for Accelerated Large Language Model Training. American Journal of Autonomous Systems and Robotics Engineering, 2, 313-351.
27. 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.
28. Ramakrishna, S. (2023). Cloud-Native AI Platform for Real-Time Resource Optimization in Governance-Driven Project and Network Operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6282-6291.
29. Rahman, M. R., Rahman, M., Rasul, I., Arif, M. H., Alim, M. A., Hossen, M. S., & Bhuiyan, T. (2024). Lightweight Machine Learning Models for Real-Time Ransomware Detection on Resource-Constrained Devices. Journal of Information Communication Technologies and Robotic Applications, 15(1), 17-23.
30. Bussu, V. R. R. (2023). Governed Lakehouse Architecture: Leveraging Databricks Unity Catalog for Scalable, Secure Data Mesh Implementation. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6298-6306.
31. Kavuru, L. T. (2024). Hybrid Methodologies for Next-Level Project Success When Waterfall Meets Agile. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(1), 9931-9938.
32. Karnam, A. (2023). SAP Beyond Uptime: Engineering Intelligent AMS with High Availability & DR through Pacemaker Automation. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9351–9361. https://doi.org/10.15662/IJRPETM.2023.0605011
33. Chivukula, V. (2020). IMPACT OF MATCH RATES ON COST BASIS METRICS IN PRIVACY- PRESERVING DIGITAL ADVERTISING. International Journal of Advanced Research in Computer Science & Technology, 3(4), 3400–3405.
34. Mahajan, N. (2023). A predictive framework for adaptive resources allocation and risk-adjusted performance in engineering programs. Int. J. Intell. Syst. Appl. Eng, 11(11s), 866.
35. Vengathattil, Sunish. 2021. "Interoperability in Healthcare Information Technology – An Ethics Perspective." International Journal For Multidisciplinary Research 3(3). doi: 10.36948/ijfmr.2021.v03i03.37457.
36. Kagalkar, A. S. S. K. A. Serverless Cloud Computing for Efficient Retirement Benefit Calculations. https://www.researchgate.net/profile/Akshay-Sharma-

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

||Volume 7, Issue 3, May–June 2024||

DOI:10.15662/IJRAI.2024.0703005

98/publication/398431156_Serverless_Cloud_Computing_for_Efficient_Retirement_Benefit_Calculations/links/69364e487e61d05b530c88a2/Serverless-Cloud-Computing-for-Efficient-Retirement-Benefit-Calculations.pdf

37. Paul, D.; Soundarapandiyan, R.; Krishnamoorthy, G. Security-First Approaches to CI/CD in Cloud-Computing Platforms: Enhancing DevSecOps Practices. Aust. J. Mach. Learn. Res. Appl. 2021, 1, 184–225.
38. 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.
39. Nasr, M., & Shokri, R. (2019). *Comprehensive analysis of privacy and security issues in federated learning*.
40. Kusumba, S. (2023). A Unified Data Strategy and Architecture for Financial Mastery: AI, Cloud, and Business Intelligence in Healthcare. International Journal of Computer Technology and Electronics Communication, 6(3), 6974-6981.