FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 5, May, 2025, pp 80 - 86
DOI: https://doi.org/10.33003/fjs-2025-0905-3207

ADVANCEMENTS IN FEDERATED LEARNING FOR SECURE DATA SHARING IN FINANCIAL SERVICES

[1]Unuigbokhai Nkem Belinda, *[1]Godfrey Perfectson Oise, [1]Babalola Eyitemi Akilo, [2]Nwabuokei Onyemaechi Clement, [1]Joy Akpowehbve Odimayomi, [3]Bakare Sofiat Kehinde and [4]Atake Onoriode Michaele

[1]Department of Computing, Wellspring University, Edo State,
[2]Department of Computer Science, Delta State College of Education, Mosogar,
[3]Department of Computer Science, University of Benin, Edo State
[4]Western Delta University, Oghara, Delta State

*Corresponding authors' email: godfrey.oise@wellspringuniversity.edu.ng
ORCID iD: https://orcid.org/0009-0006-4393-7874

ABSTRACT

This paper explores the application of Federated Learning (FL) in the financial sector, focusing on enhancing security and privacy in key areas such as fraud detection, Anti-Money Laundering (AML) compliance, and biometric authentication systems. FL enables collaborative model training across multiple financial institutions without sharing sensitive transaction data, thereby preserving privacy while improving the accuracy of fraud detection models. In AML compliance, FL facilitates the development of robust models by leveraging diverse datasets, enhancing the ability to detect suspicious activities. Moreover, FL strengthens biometric authentication systems by decentralizing model training, reducing the risks of data breaches, and ensuring compliance with privacy regulations. The paper also evaluates the performance of a loan default prediction model trained using FL, highlighting challenges with class imbalance and model bias toward the majority class. The classification report indicates high recall (98%) but also shows a potential for misclassifying non-default cases, leading to a moderate precision (81%) and an F1-score of 89%. The model's AUC of 0.69 suggests moderate discriminatory power, with room for improvement in its ability to differentiate between default and non-default cases. The model achieves an overall accuracy of 80%. Despite these challenges, it demonstrates good generalization capabilities while maintaining the privacy of client data, presenting a promising approach to secure financial transaction analysis.

Keywords: Anti-Money Laundering (AML), Data Privacy, Differential Privacy (DP), Federated Learning (FL), Homomorphic Encryption (HE), Loan Default Prediction, Secure Multi-Party Computation (SMPC)

INTRODUCTION

With increasing data privacy concerns and stringent financial regulations, traditional centralized machine learning approaches are becoming less viable. Federated Learning (FL) offers a decentralized paradigm, allowing multiple institutions to collaboratively train machine learning models without sharing raw data (L. Li et al., 2020). This paper focuses on FL's role in financial services, specifically targeting secure credit risk analysis using the Lending Club dataset. Federated learning is a privacy-preserving machine learning approach that enables collaborative model training without sharing raw data (G. Oise, 2023). The system works by having participants train models locally and share only model parameters while keeping sensitive data on their own devices or servers (G. P. Oise & Konyeha, 2024). The rapid increase in data generation from everyday activities has created immense opportunities for innovation while raising significant privacy and security concerns (Gray et al., 2024). These concerns have intensified with the enforcement of stringent data protection regulations, such as the EU's General Data Protection Regulation (GDPR) and similar frameworks in the United States and China. (Nevrataki et al., 2023) explores Federated Learning (FL) as a privacy-preserving approach to distributed machine learning that allows multiple parties to train models without sharing raw data. It highlights FL's applications in healthcare, finance, IoT, and the insurance industry, emphasizing its role in enhancing data security and privacy (Khan et al., 2021). Key challenges such as non-IID data and performance limitations are discussed, along with solutions like federated averaging, transfer learning, differential privacy, and secure multi-party computation. The paper concludes by noting FL's growing potential in real-world applications and its importance for future secure and scalable machine learning systems.

Federated Learning (FL) has emerged as a promising solution to these challenges by introducing a decentralized machine learning paradigm in which multiple clients collaboratively train models while keeping their data local (Kairouz et al., 2019). (Zhang et al., 2021) In this framework, a central server coordinates the training process across distributed clients, such as mobile devices or organizations, without accessing their raw data directly (Kairouz et al., 2019). The federated learning workflow typically consists of key stages: client selection, model broadcasting, local computation on client devices, and global aggregation on the central server (Chen et al., 2023; McMahan et al., 2016). This methodology is particularly beneficial in domains where data sharing is restricted due to legal, ethical, or confidentiality concerns, such as healthcare and finance (Huang et al., 2024). A defining advantage of federated learning is its ability to balance artificial intelligence (AI) utility with strong privacy safeguards (Herrera et al., 2024). By ensuring that model training occurs on local devices and only aggregated updates are shared, FL enhances data security while enabling efficient collaboration (Herrera et al., 2024; Li et al., 2021). This approach not only supports compliance with data protection regulations but also mitigates the risk of data breaches during transmission (Huang et al., 2024). Federated Learning emerged as a groundbreaking solution to the growing concerns about data privacy in machine learning applications (Gu et al., 2024) (McMahan et al., 2016) At its core, FL enables multiple participants to collaboratively train machine learning models while keeping their data private and localized (Z. Li et al., 2024) (Yu et al., 2024). The fundamental process of federated learning consists of three main components: local model training, model aggregation, and global model updates. Instead of sharing raw data, participants only exchange model parameters such as weights and gradients (Yu et al., 2024). This approach significantly reduces bandwidth requirements and minimizes the risk of data breaches while still enabling effective collaborative learning(Xu et al., 2019). However, it's important to note that while FL provides an initial layer of privacy protection, there are still potential privacy concerns (Abdulrahman et al., 2021). The exchange of model parameters and the resulting trained model may still inadvertently disclose information about the training data (Mugunthan et al., 2020). To address these residual privacy risks, FL systems commonly incorporate additional privacy-preserving mechanisms, particularly differential privacy and secure multiparty computation (SMC) (Xu et al., 2019). A notable characteristic of federated learning is its ability to handle heterogeneous and massive networks of devices or data centers, such as mobile phones or hospitals(Li et al., 2019). This distributed nature, combined with the need to maintain data privacy, introduces unique challenges that require different approaches compared to traditional centralized machine learning methods (Tan et al., 2021). Federated learning architecture can be categorized into three main types: Horizontal (HFL), Vertical (VFL), and Federated Transfer learning (FTL). These architectures are designed to handle different data distribution scenarios and participant feature sharing. Federated Learning (FL) operates through a distributed architecture where a central server coordinates the training process across multiple client devices or organizations without directly accessing their raw data (Legler et al., 2024; Luan et al., 2023). The training follows a cyclical pattern: the server first broadcasts the current model to selected clients, who then perform local computations on their private data before returning their updates (Shen et al., 2020). FL ensures privacy protection through multiple layers of security. Data decentralization keeps sensitive information on local devices, while encrypted communication protocols safeguard model updates during transmission between clients and the server (Luan et al., 2023). A key component of this framework is the aggregation process, where local model updates are combined in an encrypted state, ensuring that individual clients cannot access each other's models (Shen et al., 2020). Additional privacy enhancements include differential privacy techniques, which can be applied globally or locally. Global differential privacy protects against adversarial aggreFederated Federated Averagingntial privacy safeguards client updates before transmission though it requires a careful balance between noise addition and model utility (Shen et al., 2020). A key advantage of this architecture is its scalability and resilience to individual participant failures (Legler et al., 2024). Moreover, FL enhances energy efficiency by eliminating the need to retrain models from scratch at each location, making it a practical solution for real-world applications (Legler et al., 2024; Liu et al., 2019). Federated Learning (FL) employs multiple privacy and security mechanisms to protect data confidentiality and model integrity. Homomorphic Encryption (HE) enables computations on encrypted data, ensuring secure model aggregation. Secure Multi-Party Computation (SMPC) allows multiple parties to compute jointly without revealing private inputs (Aledhari et al., 2020). Differential Privacy (DP) protects against privacy leakage using clipping techniques and Gaussian mechanisms while balancing model utility (Nguyen et al., 2021). Secure Aggregation Protocols prevent privacy breaches during model updates and mitigate data poisoning attacks. Communication Security ensures encrypted model transmissions, optimizing security and efficiency for scalable FL deployment. In today's digital economy, financial institutions generate and manage vast volumes of sensitive user data, including transactional histories, credit scores, and biometric records. While this data holds great potential for predictive modeling and decision-making, its centralized storage and processing expose it to privacy risks, security breaches, and regulatory violations. Traditional machine learning approaches (G. Oise & Konyeha, 2024), which rely on centralized data aggregation, are increasingly unsuitable for applications in sensitive domains like finance, where confidentiality and compliance with regulations such as GDPR and CCPA are paramount.

To address these challenges, Federated Learning (FL) has emerged as a promising decentralized machine learning paradigm. FL enables multiple institutions to collaboratively train models without transferring raw data, thereby preserving data privacy. Prior research has successfully applied FL in healthcare, IoT, and cybersecurity domains, and more recently, in finance. Studies have demonstrated FL's usefulness in fraud detection, Anti-Money Laundering (AML) compliance, and biometric authentication by leveraging private datasets across distributed environments. However, many existing works overlook critical limitations such as class imbalance, model bias, and privacy-utility trade-offs, which can significantly affect the reliability and generalizability of FL models in real-world financial applications (G. P. Oise et al., 2025). This study aims to address these gaps by developing a privacy-preserving federated learning framework that integrates a Random Forest classifier for loan default prediction using the Lending Club dataset. Unlike previous works, our approach incorporates privacy-enhancing technologies, such as Differential Privacy, Secure Multi-Party Computation (SMPC), and Homomorphic Encryption—to secure model updates during the FL process. Additionally, we simulate a realistic federated setting and evaluate the model using comprehensive metrics, focusing on overcoming class imbalance and improving model robustness. This work contributes a scalable, secure, and interpretable framework for financial risk modeling in privacy-sensitive environments.

Review of Related Works

Federated Learning (FL) has emerged as a decentralized approach to model training that enhances privacy by allowing multiple clients to collaboratively train models without exposing their raw data (Fragulis et al., 2021). This literature review synthesizes key contributions in FL concerning its architectures, security mechanisms, privacy preservation techniques, data heterogeneity handling, model aggregation strategies, and performance evaluation metrics. Federated learning architectures are classified into centralized, decentralized, and hierarchical models. McMahan et al. (2016) introduced the FederatedAveraging (FedAvg) algorithm, which significantly reduces communication overhead while maintaining model performance. Yang et al. (2019) proposed a parameter server architecture, eliminating the need for a third-party coordinator, thereby enhancing privacy. Their work also introduced homomorphic encryption to secure model training and facilitate encrypted transmission of intermediate results, improving communication efficiency. Chen et al. (2023) provided a network topology-based classification of FL systems, analyzing attack scenarios and defense methods. Their study introduced quantization and sparsification techniques to minimize communication overhead in FL. Huang et al. (2024) focused on federated intrusion detection systems (FIDS), demonstrating FL's effectiveness in handling sensitive network security data. Che et al. (2021) explored FL's applications in medical data integration, leveraging FL to preserve privacy in multi-view learning. Stripelis et al. (2022) applied FL in biomedical research consortia, employing sample data anonymity, encrypted transmission, and fully homomorphic encryption (FHE) to secure neuroimaging data. The integration of secure multi-party computation (SMC) and differential privacy (DP), as proposed by Yang et al. (2019), has further improved FL's resilience against privacy threats. Privacy preservation is a core challenge in FL due to data decentralization and adversarial risks. McMahan et al. (2016) ensured data privacy by keeping training data on mobile devices and mitigating non-independent and identically distributed (non-i.i.d) data issues via the FedAvg algorithm. Yang et al. (2019) proposed multi-layered privacy-preserving mechanisms incorporating Homomorphic Encryption (HE), Secure Multi-Party Computation (SMC), and Differential Privacy (DP) to protect sensitive data. Chen et al. (2023) reviewed FL's vulnerabilities but did not specifically address data heterogeneity challenges. Stripelis et al. (2021) developed an FL framework for predicting brain age from MRI scans, leveraging FHE with CKKS encryption to maintain data confidentiality. Korkmaz et al. (2025) advanced FL applications in healthcare by utilizing selective encryption, homomorphic encryption, differential privacy, and bit-wise scrambling for secure medical imaging analysis. Recent research by Cheng et al. (2023) applied a differential privacy approach with adaptive noise addition to safeguard model parameters from inference attacks. Rahulamathavan et al. (2023) further secured FL by implementing a fully homomorphic encryption (FHE) scheme alongside a non-poisoning rate-based weighted aggregation technique to mitigate data poisoning attacks. Model aggregation plays a pivotal role in FL optimization. McMahan et al. (2016) introduced FedAvg, reducing communication rounds while maintaining model accuracy. Yang et al. (2019) integrated secure aggregation and encryption techniques to enhance model update security. Chen et al. (2023) proposed a generalized design framework for FedOpt algorithms to optimize FL convergence. Huang et al. (2024) explored a decentralized FL model with client nodes and an aggregation server, evaluating system performance using accuracy, evaluation loss, and F1-score while ensuring data decentralization. Stripelis et al. (2022) implemented a 3D Convolutional Neural Network (CNN) for Alzheimer's disease prediction, encrypting model parameters to maintain data privacy. Santiago S. Silva et al. (2018) designed a federated learning framework for distributed brain data analysis, employing the Alternating Direction Method of Multipliers (ADMM) algorithm to ensure security and efficiency. Korkmaz et al. (2025) benchmarked FL models, comparing ResNet-50, DenseNet121, EfficientNetB0, and MobileNetV2. Their evaluation metrics included execution time, communication efficiency, and privacy preservation, demonstrating a 90% performance improvement compared to full homomorphic encryption-based models while maintaining security. Encryption is vital in protecting FL models against adversarial threats. Hussien et al. (2023) and Rahulamathavan et al. (2023) leveraged homomorphic encryption to safeguard data transmission, with the latter utilizing CKKS FHE to enhance security. Cheng et al. (2023) combined secure multi-party computation (SMC) and differential privacy to resist inference attacks. Sen et al. (2024) implemented K-anonymity, L-diversity, and pseudonymization for privacy enhancement. Varshney et al. (2023) introduced a Fair Differentially Private Federated Learning Framework to strengthen FL's resistance to privacy attacks. Advancements in architectures, security mechanisms, and privacy-preserving techniques have driven the evolution of Federated Learning (FL). FedAvg, introduced by McMahan et al. (2016), provided a foundation for FL optimization, while later studies by Yang et al. (2019), Chen et al. (2023), and Stripelis et al. (2022) improved privacy through homomorphic encryption, differential privacy, and secure aggregation. These developments have enhanced data security, communication efficiency, and model performance (Zelios et al., 2022). However, challenges remain, including high communication costs, privacy vulnerabilities, data heterogeneity, adversarial threats, and scalability issues. Future research should focus on efficient compression techniques, post-quantum cryptographic methods, adaptive model personalization, robust security mechanisms, and scalable FL architectures. Addressing these challenges will enable broader adoption of FL in privacy-sensitive fields such as healthcare, cybersecurity, and finance, ensuring secure and efficient decentralized learning. Recent advancements in Federated Learning (FL) have focused on enhancing privacy through blockchain integration, improved encryption methods, and novel frameworks for secure data sharing. Key developments include the integration of blockchain for secure and decentralized data access (Chhetri et al., 2023; Lu et al., 2020) and the introduction of the FheFL scheme, which employs multi-key additive homomorphic encryption to secure model aggregation and defend against data poisoning attacks (Rahulamathavan et al., 2023). Additionally, the APPFL framework has strengthened differential privacy implementation in FL (Li et al., 2023), while decentralized storage solutions like the InterPlanetary File System (IPFS) provide secure, distributed storage alternatives (Jaberzadeh et al., 2023). Furthermore, FL is being increasingly applied to Large Language Models (LLMs), leveraging secure aggregation, differential privacy, and parameter-efficient fine-tuning for privacy-preserving collaborative model training (Yan et al., 2024). Future research should focus on optimizing neural network architectures for FL scenarios, addressing data heterogeneity, and improving security mechanisms to enhance FL's applicability across diverse domains (Zacharis et al., 2022). Previous research has applied FL to healthcare, cybersecurity, and mobile computing, but its use in financial services remains underexplored. Studies by (Chen et al., 2023) emphasized optimization techniques and hybrid privacy-preserving strategies. This study builds upon these insights, focusing on model performance and data protection within the financial domain. This paper addresses key research gaps in the application of Federated Learning (FL) for financial analytics, particularly in credit risk assessment and loan default prediction. Existing studies often overlook critical issues such as class imbalance, inadequate privacy safeguards beyond FL's inherent protections, and the lack of realistic federated simulations. Additionally, many do not provide comprehensive performance evaluations that reflect real-world challenges. This study fills these gaps by integrating advanced privacy-preserving techniques. Differential Privacy, Secure Multi-party Computation, and Homomorphic Encryption—into a Random Forest-based FL framework. It also simulates a realistic multi-client FL environment using the Lending Club dataset and evaluates the model with detailed metrics to highlight performance issues, especially on the minority class. This approach enhances both the security and effectiveness of collaborative financial modeling while ensuring compliance with privacy regulations.

MATERIALS AND METHODS

The study explores the integration of Federated Learning (FL) into financial analytics, aiming to ensure data privacy while enabling collaborative machine learning across multiple financial institutions. FL allows each participant to train models locally on private data and share only the model updates—such as weights or gradients—with a central aggregator. This method ensures that sensitive data remains decentralized while still contributing to a robust, shared model. The technique is particularly beneficial for sectors like finance, where privacy and regulatory constraints limit data sharing. A Random Forest classifier is employed to predict loan defaults. This ensemble-based algorithm constructs multiple decision trees and aggregates their predictions, offering robustness and accuracy. It effectively handles high-dimensional data and offers interpretability through feature importance scores, helping to identify critical factors such as income and loan amount in default prediction. Despite these strengths, the model faces challenges with class imbalance, particularly in detecting minority classes like defaulters. To safeguard privacy within the FL framework, the study integrates several advanced security techniques. Differential Privacy adds noise to model updates to prevent inference attacks. Secure Multi-Party Computation allows secure aggregation without exposing individual inputs, while Homomorphic Encryption supports computations on encrypted data, securing model parameters even during transmission. These mechanisms collectively ensure that data confidentiality is maintained throughout the training process. Model performance is evaluated using a suite of metrics. High recall (98%) indicates the model's strong sensitivity to detecting true loan defaults, but a lower precision (81%) suggests it struggles with false positives. The F1-score (89%) reflects a good balance between these metrics, while an AUC-ROC of 0.69 indicates moderate discriminative ability. The confusion matrix further highlights the issue of class imbalance, showing that the model often misclassifies minority-class examples. Comprehensive data preprocessing is conducted, including class filtering, one-hot encoding of categorical variables, and normalization of numerical features. The data is also partitioned across simulated FL clients to mimic a realistic federated environment. Key challenges addressed include class imbalance, bias in model aggregation due to uneven data distributions, and the trade-off between maintaining privacy and preserving model utility. The study effectively demonstrates how Federated Learning, combined with Random Forest and privacy-preserving techniques, can facilitate secure, distributed financial modeling. While the approach preserves data privacy and improves detection of loan defaults, issues such as class imbalance and moderate model accuracy remain areas for future improvement. Enhancements like advanced anomaly detection and hybrid encryption methods are recommended for building more resilient and privacy-aware systems.

The methodology adopted in this paper involves the application of Federated Learning (FL) for secure data sharing and collaborative model training across financial institutions, using the Lending Club dataset.

Dataset: The study utilizes the Lending Club dataset, which is publicly available on Kaggle (Nathan George, 2020). This dataset contains over 2 million loan records with various features like loan amount, interest rate, income, employment, and loan status.

Preprocessing: The data was preprocessed by filtering to include only "Fully Paid" and "Charged Off" loans, encoding categorical variables via one-hot encoding, removing missing and irrelevant data, and normalizing and partitioning the data into simulated federated clients.

Experimental Setup: A Random Forest Classifier was trained independently per client and then aggregated to simulate FL. A standard train-test split (80:20) was applied with stratification to handle class imbalance.

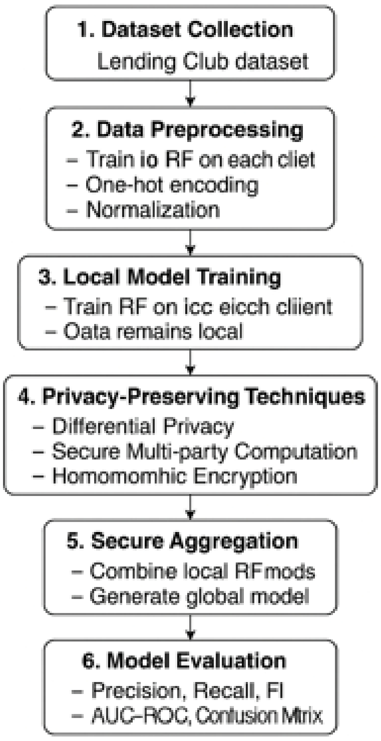

Figure 1: Federated learning Methodology for Secure Financial Prediction

RESULTS AND DISCUSSION

Federated learning plays a critical role in enhancing security and privacy in financial transactions. It enables collaborative fraud detection across multiple financial institutions without sharing raw transaction data, addressing privacy concerns (Rells & Joseph, 2025). Additionally, federated learning improves anti-money laundering (AML) compliance by allowing institutions to train AML models on diverse datasets without exposing sensitive transaction information. It also strengthens biometric authentication systems by enabling decentralized training of biometric models, preventing data breaches while maintaining privacy regulations (Mothukuri et al., 2021). Overall, federated learning enhances fraud detection, AML monitoring, and biometric security in the financial sector (Godfrey Perfectson Oise, 2023). The research discusses the application of Federated Learning (FL) in the financial sector, emphasizing its role in enhancing security and privacy in financial transactions. It highlights several key applications (Lazaridis et al., 2019), including collaborative fraud detection across multiple institutions without sharing raw transaction data and improving privacy preservation (Tsakiris et al., 2022). FL also aids in Anti-Money Laundering (AML) compliance by enabling institutions to train models on diverse datasets while keeping sensitive information secure. Additionally, FL strengthens biometric authentication systems by allowing decentralized training of models, preventing data breaches, and ensuring compliance with privacy regulations. We further examine the performance of a loan default prediction model trained with FL, noting challenges related to class imbalance and model bias toward the majority class (Nevrataki et al., 2023). Despite these issues, the model demonstrates good generalization and the ability to preserve client data privacy, although it shows potential for misclassifying non-default cases.

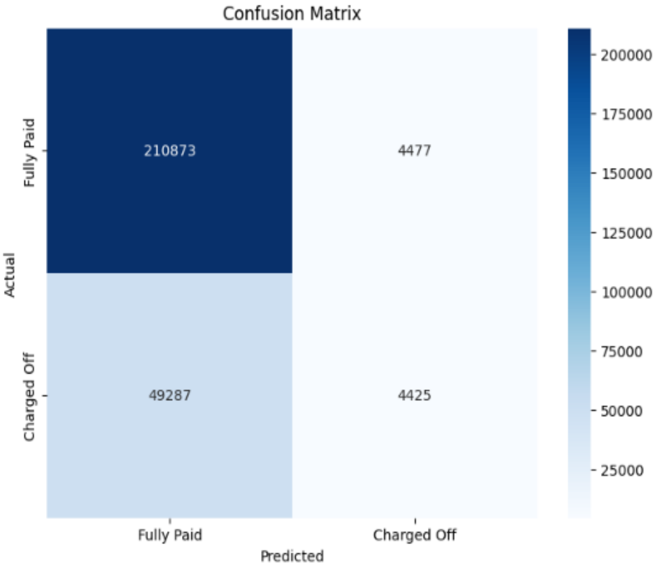

Figure 2: Confusion Matrix of the Model

The confusion matrix reveals significant challenges in the loan default prediction model, particularly due to severe class imbalance. With 210,873 true negatives (correctly predicted "Fully Paid" loans) but only 4,425 true positives (correctly identified defaults), the model demonstrates a strong bias toward the majority class, resulting in a critical 91.8% false negative rate for defaults. This means the model misses nearly 92% of actual high-risk loans, posing substantial financial risks for lenders. While the overall accuracy of 80.8% appears decent, it is misleadingly inflated by the dominance of non-default cases. The precision of 49.7% for defaults indicates that even when the model flags a loan as risky, there's only a 50% chance it's correct.

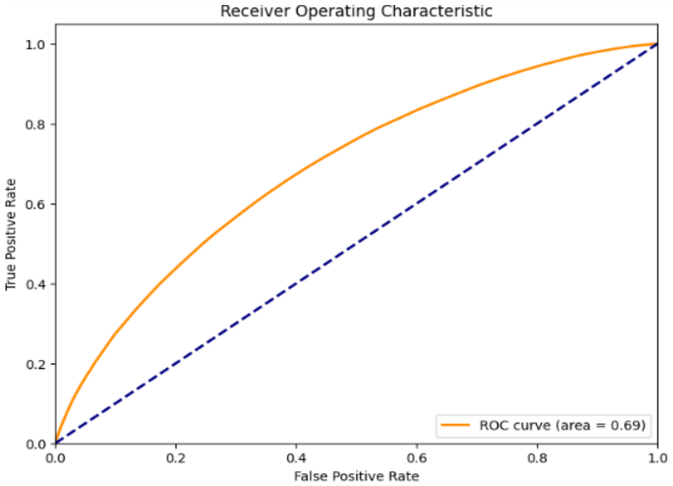

Figure 3: The Receiver Operating Characteristic of the Model

The ROC curve with an AUC of 0.69 indicates moderate discriminatory power for the loan default prediction model, performing better than random guessing (AUC = 0.5) but falling short of the desired strong predictive ability (AUC > 0.8). The curve reveals difficulty in balancing the true positive rate (sensitivity) and false positive rate (1-specificity), particularly at lower false positive rates, where the true positive rate remains low (~0.4), leading to poor recall (8.2%) for defaults. The high AUC and low log loss indicate the model's ability to generalize well while preserving client data privacy (Papatsimouli et al., 2022). These metrics show FL's effectiveness in maintaining predictive power even with decentralized data

Table 1: Evaluation of Metrics

Metrics	Score
Precision	81
Recall	98
F1-Score	89
Accuracy	80

The classification report for the loan default prediction model shows the following performance metrics: Precision of 81%, Recall of 98%, F1-Score of 89%, and Accuracy of 80%. This indicates that the model is highly sensitive to detecting defaults (high recall) (Papatsimouli et al., 2022). The F1-score suggests a good balance between precision and recall, though the model could still be prone to misclassifying some non-default cases as defaults. The accuracy of 80% reflects solid overall performance.

CONCLUSION

This study demonstrates the transformative potential of Federated Learning (FL) in advancing secure and privacy-preserving data sharing within the financial sector. By enabling collaborative model development without the exchange of raw data, FL addresses critical privacy concerns while improving the effectiveness of fraud detection, Anti-Money Laundering (AML) compliance, and biometric authentication systems. The implementation of FL in a loan default prediction use case, using the Lending Club dataset, highlights both the opportunities and limitations of this approach. The model achieved an accuracy of 80%, a high recall of 98%, and an F1-score of 89%, indicating strong performance in identifying default cases. However, the moderate AUC score of 0.69 and precision of 81% suggest room for improvement, particularly in reducing false positives and better capturing minority-class instances. These findings underscore the importance of ongoing work in optimizing model architectures, addressing data imbalance, and refining privacy-preserving techniques within FL frameworks. As financial institutions increasingly adopt decentralized and secure data practices, Federated Learning stands out as a viable and forward-looking solution that aligns with both operational efficiency and regulatory compliance. Future work should explore the integration of advanced techniques such as anomaly detection, hybrid encryption models, and personalized FL to further enhance model robustness and practical deployment in real-world financial ecosystems.

REFERENCES

Abdulrahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2021). A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet of Things Journal*, *8*(7), 5476–5497. https://doi.org/10.1109/JIOT.2020.3030072

Aledhari, M., Razzak, R., Parizi, R. M., & Saeed, F. (2020). Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Access*, *8*, 140699–140725. https://doi.org/10.1109/ACCESS.2020.3013541

Chen, H., Wang, H., Long, Q., Jin, D., & Li, Y. (2023). *Advancements in Federated Learning: Models, Methods, and Privacy* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2302.11466

Fragulis, G. F., Papatsimouli, M., Lazaridis, L., & Skordas, I. A. (2021). An Online Dynamic Examination System (ODES) based on open source software tools. *Software Impacts*, *7*, 100046. https://doi.org/10.1016/j.simpa.2020.100046

Godfrey Perfectson Oise. (2023). A Framework on E-Waste Management and Data Security System. *International Journal on Transdisciplinary Research and Emerging Technologies*, *1*(1).

Gray, M., Fox, N., Gordon, J. E., Brilha, J., Charkraborty, A., Garcia, M. D. G., Hjort, J., Kubalíková, L., Seijmonsbergen, A. C., & Urban, J. (2024). Boundary of ecosystem services: A response to. *Journal of Environmental Management*, *351*, 119666. https://doi.org/10.1016/j.jenvman.2023.119666

Gu, M., Naraparaju, R., & Zhao, D. (2024). *Enhancing Data Provenance and Model Transparency in Federated Learning Systems—A Database Approach* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2403.01451

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., Rouayheb, S. E., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., Zhao, S. (2019). *Advances and Open Problems in Federated Learning* (Version 3). arXiv. https://doi.org/10.48550/ARXIV.1912.04977

Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges. *IEEE Communications Surveys & Tutorials*, *23*(3), 1759–1799. https://doi.org/10.1109/COMST.2021.3090430

Lazaridis, L., Papatsimouli, M., & Fragulis, G. F. (2019). A synchronous-asynchronous tele-education platform. *International Journal of Smart Technology and Learning*, *1*(2), 122. https://doi.org/10.1504/IJSMARTTL.2019.097950

Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*, *149*, 106854. https://doi.org/10.1016/j.cie.2020.106854

Li, Z., He, S., Chaturvedi, P., Kindratenko, V., Huerta, E. A., Kim, K., & Madduri, R. (2024). *Secure Federated Learning Across Heterogeneous Cloud and High-Performance Computing Resources—A Case Study on Federated Fine-tuning of LLaMA 2* (arXiv:2402.12271). arXiv. https://doi.org/10.48550/arXiv.2402.12271

Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, *115*, 619–640. https://doi.org/10.1016/j.future.2020.10.007

Nathan George. (2020). *All Lending Club loan data* [Dataset]. Kaggle online data repository. https://www.kaggle.com/datasets/wordsforthewise/lending-club

Nevrataki, T., Iliadou, A., Ntolkeras, G., Sfakianakis, I., Lazaridis, L., Maraslidis, G., Asimopoulos, N., & Fragulis, G. F. (2023). *A survey on federated learning applications in healthcare, finance, and data privacy/data security*. 120015. https://doi.org/10.1063/5.0182160

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Vincent Poor, H. (2021). Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622–1658. https://doi.org/10.1109/COMST.2021.3075439

Oise, G. (2023). A Web Base E-Waste Management and Data Security System. *RADINKA JOURNAL OF SCIENCE AND SYSTEMATIC LITERATURE REVIEW*, *1*(1), 49–55. https://doi.org/10.56778/rjslr.v1i1.113

Oise, G., & Konyeha, S. (2024). E-WASTE MANAGEMENT THROUGH DEEP LEARNING: A SEQUENTIAL NEURAL NETWORK APPROACH. *FUDMA JOURNAL OF SCIENCES*, *8*(3), 17–24. https://doi.org/10.33003/fjs-2024-0804-2579

Oise, G. P., & Konyeha, S. (2024). Deep Learning System for E-Waste Management. *The 3rd International Electronic Conference on Processes*, 66. https://doi.org/10.3390/engproc2024067066

Oise, G. P., Nwabuokei, O. C., Akpowehbve, O. J., Eyitemi, B. A., & Unuigbokhai, N. B. (2025). TOWARDS SMARTER CYBER DEFENSE: LEVERAGING DEEP LEARNING FOR THREAT IDENTIFICATION AND PREVENTION. *FUDMA JOURNAL OF SCIENCES*, *9*(3), 122–128. https://doi.org/10.33003/fjs-2025-0903-3264

Papatsimouli, M., Lazaridis, L., Ziouzios, D., Dasygenis, M., & Fragulis, G. (2022). Internet Of Things (IoT) awareness in Greece. *SHS Web of Conferences*, *139*, 03013. https://doi.org/10.1051/shsconf/202213903013

Rells, J., & Joseph, W. (2025). *Federated Learning for Secure Financial Transactions*. https://www.researchgate.net/publication/389389123

Tsakiris, G., Papadopoulos, C., Patrikalos, G., Kollias, K.-F., Asimopoulos, N., & Fragulis, G. F. (2022). The development of a chatbot using Convolutional Neural Networks. *SHS Web of Conferences*, *139*, 03009. https://doi.org/10.1051/shsconf/202213903009

Yu, S., Muñoz, J. P., & Jannesari, A. (2024). *Federated Foundation Models: Privacy-Preserving and Collaborative Learning for Large Models* (arXiv:2305.11414). arXiv. https://doi.org/10.48550/arXiv.2305.11414

Zacharis, G., Gadounas, G., Tsirtsakis, P., Maraslidis, G., Assimopoulos, N., & Fragulis, G. (2022). Implementation and Optimization of Image Processing Algorithm using Machine Learning and Image Compression. *SHS Web of Conferences*, *139*, 03014. https://doi.org/10.1051/shsconf/202213903014

Zelios, A., Grammenos, A., Papatsimouli, M., Asimopoulos, N., & Fragulis, G. (2022). Recursive neural networks: Recent results and applications. *SHS Web of Conferences*, *139*, 03007. https://doi.org/10.1051/shsconf/202213903007

Zhang, Y., Bai, G., Li, X., Nepal, S., & Ko, R. K. L. (2021). *Confined Gradient Descent: Privacy-preserving Optimization for Federated Learning* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2104.13050

©2025 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.