

 Demak Universal Journal of Islam and Sharia	Demak Universal Journal of Islam and Sharia E-ISSN: 2988-3539 Vol.4, No.01, 2026, pp. 77-92 DOI: https://doi.org/10.61455/deujis.v4i01.616	 WALIDEM INSTITUTE AND PUBLISHING
Received March 08, 2026	Revised July 21, 2026	Accepted August 29, 2026

Federated Learning for Shari‘ah-Compliant Credit Scoring in Islamic Banks: Preserving Data Privacy and Eliminating Riba-Related Features

Maisuna Mustapha Yahya^{1}, Akanbi Bello Muhammed², Alwy Ahmed Mohamed³*

¹Department of Islamic Studies, Faculty of Arts, University of Abuja, Nigeria

²Department of Computer Science, Faculty of Science, University of Abuja, Nigeria

³Department of Islamic Education, Universitas Muhammadiyah Surakarta, Indonesia, and The Agakhan High School, Mombasa, Kenya

^{1*}mustapha.maisuna@uniabuja.edu.ng, ²muhammed.akanbi@uniabuja.edu.ng,

³g000249216@student.ums.ac.id

Abstract

Objective: The rapid expansion of Islamic banking across Africa, Southeast Asia, and the GCC region requires credit assessment frameworks that are privacy-preserving, data-efficient, and strictly Shari‘ah-compliant. This study proposes FedIslami, a novel federated learning framework designed to train credit-scoring models collaboratively across distributed Islamic bank branches without transmitting sensitive raw client records. **Theoretical framework:** The study is theoretically grounded in the Islamic principle of Amānah (trusteeship of client data) and Maqāsid al-Shari‘ah objectives, establishing an ethical foundation for data privacy, algorithmic justice, and religious compliance within modern financial engineering. **Literature Review:** Existing literature highlights that conventional machine learning models violate data trusteeship through centralised data aggregation and systematically incorporate interest-rate exposure metrics, debt-service-coverage ratios, and other Ribā-indexed features that are impermissible under Shari‘ah law. **Method:** FedIslami systematically excises fourteen identified Ribā-contaminated features, replacing them with Shari‘ah-permissible analogues. Utilising FedAvg with differential privacy (DP-FedAvg) and homomorphic encryption secure aggregation, the model was validated on 214,736 anonymised financing records (2019–2024) across nine Islamic banks in Nigeria, Malaysia, UAE, and Bangladesh. **Results:** FedIslami achieved outstanding predictive accuracy with an AUC of 0.894, a Gini coefficient of 0.788, and a Kolmogorov-Smirnov statistic of 0.581, significantly outperforming non-federated centralised baselines (0.871) and conventional federated models retaining Ribā features (0.842). The audit confirmed full compliance with AAOIFI Governance Standard No. 7 and IFSB-16. **Implications:** This research demonstrates that privacy-preserving federated learning effectively bridges performance gaps between modern Islamic and conventional credit-scoring systems while simultaneously reinforcing institutional ethical and religious data-governance obligations. **Novelty:** FedIslami introduces the first dual-layer privacy-preserving federated learning architecture that simultaneously addresses client privacy and algorithmic Shari‘ah compliance through systemic Ribā feature elimination and Maqāsid-aligned variable substitution.

Keywords: federated learning, shari‘ah-compliant credit scoring, ribā elimination, islamic banking, differential privacy

*Corresponding Author: mustapha.maisuna@uniabuja.edu.ng



This work is licensed under a Creative Commons Attribution 4.0 International License ([CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)).

INTRODUCTION

The global Islamic finance industry reached an estimated asset base of USD 4.5 trillion by 2024, registering compound annual growth of 10.2% over the preceding five-year period driven primarily by retail and corporate financing products in Nigeria, Malaysia, the UAE, Bangladesh, and Saudi Arabia [1]. As IFIs scale their retail financing portfolios, the demand for robust automated credit-scoring systems has intensified. However, adapting conventional credit-scoring methodologies to the Islamic banking context presents challenges that are simultaneously technical and theological in nature [2].

From a theological standpoint, *Ribā*, broadly encompassing any predetermined, fixed increment on a monetary loan, is categorically prohibited in classical Islamic jurisprudence and operationalised as a bright-line prohibition in contemporary Shari‘ah standards issued by the Accounting and Auditing Organisation for Islamic Financial Institutions (AAOIFI) and the Islamic Financial Services Board (IFSB) [3]. The prohibition extends beyond contractual structures to encompass informational inputs: a credit-scoring model that incorporates features derived from interest rate benchmarks, conventional debt-service ratios, or credit card utilisation rates embedding interest charges is, in the view of a majority of contemporary scholars, relying on *Ribā*-contaminated information in its decision-making, thereby compromising the Shari‘ah integrity of the financing decision [4].

From a technical standpoint, the standard remedy of centralising all client data at a single model-training node conflicts with the Islamic ethical construct of *Amānah* (trusteeship), which obligates custodians of entrusted data to protect it from unnecessary exposure, and with the increasingly stringent data-localisation regulations operative in key Islamic finance jurisdictions including Nigeria (NDPR 2019), Malaysia (PDPA 2010, revised 2023), the UAE (PDPL 2021), and Bangladesh (Digital Security Act 2018). The confluence of Shari‘ah imperatives and regulatory requirements creates a design constraint that conventional and even most Islamic banking technology providers have not systematically addressed [5].

Federated learning (FL), introduced by McMahan et al. and subsequently extended through differential privacy augmentations and secure aggregation protocols, offers a principled resolution: model parameters rather than raw data are exchanged between distributed training nodes, enabling collaborative learning without centralised data exposure [6]. Despite the theoretical alignment between FL’s privacy guarantees and Islamic ethical data stewardship, no published work to the authors’ knowledge has constructed an FL credit-scoring framework that simultaneously: (i) enforces DP-noise-protected parameter aggregation; (ii) systematically identifies and eliminates *Ribā*-contaminated input features; (iii) substitutes Shari‘ah-permissible feature analogues; and (iv) validates the resulting system through formal Shari‘ah scholarly review [7].

This paper makes the following contributions: (1) a taxonomy of *Ribā*-contaminated credit-scoring features and their Shari‘ah-permissible substitutes, grounded in *Maqāsid al-Shari‘ah* and endorsed by three Shari‘ah scholars; (2) the FedIslami architecture a DP-FedAvg framework with homomorphic encryption-based secure aggregation tailored for IFI deployments; (3) empirical evaluation on 214,736 real financing records from nine Islamic banks across four jurisdictions; and (4) a Shari‘ah compliance audit protocol for federated credit-scoring systems, proposed as a template for industry-wide adoption [8].

The exponential expansion of Islamic banking across Africa, Southeast Asia, and the Gulf Cooperation Council (GCC) regions underscores a pivotal transformation in contemporary ethical finance [9]. Driven primarily by retail and corporate financing products in major growth hubs such as Nigeria, Malaysia, the United Arab Emirates, Bangladesh, and Saudi Arabia, Islamic Financial Institutions (IFIs) are scaling their financing portfolios at unprecedented rates. To sustain this momentum, streamline underwriting, and manage credit risk effectively, the demand for robust, automated credit-scoring systems has intensified [10]. However, adapting conventional credit-scoring methodologies to the Islamic banking

domain presents severe challenges that are simultaneously technical, regulatory, and theological in nature.

From a jurisprudential standpoint, Shari'ah governance as codified by international regulatory bodies including the Accounting and Auditing Organisation for Islamic Financial Institutions (AAOIFI) and the Islamic Financial Services Board (IFSB) strictly prohibits interest (Riba), speculative uncertainty (Gharar), and unethical business activities [11]. This prohibition extends beyond transactional structures to the underlying data inputs of predictive analytics: standard credit-scoring models that incorporate interest-derived features or conventional debt metrics are theological non-starters [12]. Concurrently, the Islamic ethical concept of Amanah (trusteeship) places a severe religious obligation on financial institutions to safeguard entrusted customer data from exposure. This theological constraint directly intersects with stringent data-localisation regulations, such as Nigeria's NDPR and Malaysia's PDPA, which restrict cross-border raw data sharing [13].

Federated Learning (FL) provides a principled resolution to this structural tension by enabling collaborative machine learning model training across distributed banking nodes without centralising raw customer data. Although FL has gained traction in conventional finance, its systematic application within Shari'ah-compliant frameworks remains unaddressed [14]. To bridge this critical research gap, the primary novelty of this study lies in pioneering the first multi-jurisdictional, Shari'ah-compliant FL credit-scoring framework. The core scientific novelty includes: (1) integrating a Shari'ah-governed feature filtering protocol that eliminates Riba-tainted variables before local gradient updates; (2) conducting an extensive empirical validation on a novel multi-national dataset of 214,736 anonymised financing application records collected from nine IFIs across four jurisdictions between 2019 and 2024; and (3) designing a communication-efficient, shallow two-layer decision head capable of harmonising gradient updates across highly heterogeneous client hardware [15]. Furthermore, our novelty encompasses evaluating temporal generalisation across a multi-year held-out test split, ensuring robust performance against macroeconomic shifts in Islamic retail markets.

The profound implications of this study span theoretical, operational, and policy dimensions within the global Islamic financial ecosystem. From a theoretical perspective, this work establishes a conceptual paradigm for "Shari'ah-by-Design" machine learning, demonstrating that privacy-preserving algorithms can directly reflect religious ethics [16]. Operationally, the framework allows competing IFIs to collaboratively build high-precision credit scoring models without risking customer privacy violations, breaching national data sovereignty, or sacrificing competitive advantage. This dramatically reduces default risk while expanding ethical credit access to previously unbanked populations. Regulatively, our findings provide an actionable, empirical reference for standard-setting bodies such as AAOIFI, IFSB, and national central banks to draft standardised governance frameworks for AI adoption [17]. Ultimately, this architecture establishes a practical blueprint for institutional trust and scalable technical compliance across global Islamic finance networks, proving that cutting-edge privacy technologies and strict religious principles can harmoniously unite to forge a secure, equitable financial future.

LITERATURE REVIEW

Credit Scoring in Islamic Finance: State of the Art

Credit risk assessment in IFIs has historically relied on qualitative Shari'ah-board-delegated judgement, adapted CAMELS rating frameworks, and, more recently, logistic regression models that simply remove interest-related variables without substituting principled Shari'ah-grounded alternatives [18]. Machine learning applications in Islamic credit scoring gained momentum between 2018 and 2022, with studies by Abdou & Pointon,

Zainudin et al., and Mohd Isa et al. demonstrating that gradient-boosted trees and neural networks achieve superior discriminatory power relative to logistic regression in Islamic retail financing contexts [19]. However, none of these studies addressed the dual challenge of data privacy and Ribā feature contamination systematically. Chamboko & Bravo highlighted that Islamic microfinance institutions in sub-Saharan Africa face a compounded disadvantage: limited internal data and regulatory barriers to data sharing, making federated approaches particularly apt [20].

Federated Learning: Foundations and Financial Applications

The canonical FL framework of McMahan et al. Fed Avg coordinates a central server and K distributed clients through iterative rounds of local stochastic gradient descent (SGD) followed by weighted parameter averaging. Subsequent work established that FedAvg is vulnerable to membership inference attacks and gradient inversion, motivating the addition of (i) differential privacy via Gaussian noise injection into gradients, and (ii) secure aggregation using cryptographic protocols that prevent the server from inspecting individual client updates [21]. FL has been applied to financial fraud detection, credit risk assessment in conventional banking, and insurance underwriting, but Islamic finance applications remain almost absent from the peer-reviewed literature, representing a significant gap this paper addresses [22].

Shari‘ah Compliance in FinTech: The Ribā Feature Problem

Al-Suwailem provides the jurisprudential basis for understanding that algorithmic financial models engaging with Ribā-indexed data as informational inputs rather than contractual terms occupy a contested but increasingly scrutinised Shari‘ah space. The Shari‘ah Review Bureau (SRB) and AAOIFI’s Shari‘ah Standard No. 57 on Codes of Conduct for Employees of Islamic Financial Institutions collectively imply that data used in Islamic financial decision-making should, to the greatest extent feasible, be free of Ribā contamination [23]. Laldin & Furqani articulate this within Maqāsid al-Shari‘ah’s five objectives (preservation of religion, life, intellect, lineage, and property), arguing that Hifz al-Māl (preservation of property/wealth) mandates not only the prohibition of Ribā in contracts but also in the informational architectures of Islamic financial institutions. Despite this scholarly foundation, no computational operationalisation of Ribā feature detection and elimination in ML pipelines exists in the literature [24].

Shari‘ah Framework: Ribā Feature Taxonomy and Permissible Substitutes

A three-stage Shari‘ah audit was conducted in consultation with three scholars holding doctoral qualifications in Islamic jurisprudence and Islamic finance (collectively holding ijaazah in fiqh al-mu‘amalāt from Al-Azhar University, Madinah Islamic University, and the International Islamic University Malaysia). The audit proceeded through: (1) enumeration of all candidate features drawn from conventional credit-scoring practice; (2) classification of each feature against a Shari‘ah permissibility rubric; and (3) derivation of functionally equivalent Shari‘ah-permissible substitutes grounded in Maqāsid al-Shari‘ah objectives [25]. Table 1 presents the 14 eliminated Ribā-contaminated features alongside their permissible analogues.

Table 1. Ribā-Contaminated Credit Features and Their Shari‘ah-Permissible Substitutes

Eliminated Feature (Ribā-Contaminated)	Shari‘ah Objection	Permissible Substitute	Maqāsid Basis
Conventional interest rate paid (annualised)	Direct Ribā metric	Profit rate on Murābaḥah/Ijārah contracts paid	Hifz al-Māl
Credit card balance/utilisation rate	Interest-accruing debt measure	Tawāruq/Qard Hasan repayment consistency	Hifz al-Māl
Mortgage interest outstanding	Ribā al-nasī‘ah (deferment Ribā)	Home financing (BBA/Musharakah Mutanaqisah) residual	Hifz al-Māl
Debt-service coverage ratio (DSCR)	Based on interest charges in the denominator	Islamic profit distribution coverage ratio	Hifz al-Māl
Conventional loan-to-value (LTV) ratio	Assumes interest-amortised loan value	Asset-backed financing-to-asset value ratio	Hifz al-Māl
Overdraft interest charges	Ribā on current account excess	Qard Hasan overdraft utilisation frequency	Hifz al-‘Aql
Late payment interest penalties	Ribā al-faddl (excess in exchange)	Charitable donation (tabaḥṛru‘) penalty adherence	Hifz al-Dīn
Annual percentage rate (APR) history	Aggregate Ribā cost index	Wa’d fulfilment rate on Islamic instruments	Hifz al-Māl
Compound interest accrued on savings	Ribā on savings via compounding	Investment profit rate (Mudārabah account)	Hifz al-Māl
Balance transfer interest rate accepted	Voluntary engagement with Ribā	Asset refinancing (Tawarruq) frequency	Hifz al-Māl
Conventional insurance premium paid	May embed Gharar & Ribā components	Takaful contribution regularity index	Hifz al-Nafs
Government bond yield held in portfolio	Interest-bearing instrument exposure	Sukuk holding proportion in portfolio	Hifz al-Māl
Personal loan interest rate (%)	Direct Ribā contractual feature	Personal financing profit rate (Islamic)	Hifz al-Māl
Hire purchase interest component.	Ribā element in conventional HP	Ijārah Muntahia Bittamlik payment record	Hifz al-Māl

The permissibility rubric applied three criteria drawn from AAOIFI Shari‘ah Standard No. 21 and IFSB-16: (i) the feature must not be derived from or indexed to a Ribā-based rate; (ii) the underlying transaction generating the data must be a Shari‘ah-compliant contract; and (iii) the feature’s predictive use must not create an incentive structure that indirectly promotes Ribā-bearing financial behaviour. Features surviving this filter were retained; those failing were substituted using functionally analogous Islamic contract data as indicated in Table 1.

The FedIslami Framework

System Architecture

FedIslami consists of three architectural layers: (1) a Shari'ah Feature Governance Layer (SFGL) that enforces the feature taxonomy at each client node before any model training commences; (2) a Privacy-Preserving Federated Training Layer (PPFTL) implementing DP-FedAvg with homomorphic encryption-based secure aggregation; and (3) a Shari'ah-Auditable Inference Layer (SAIL) that enforces explainability constraints and generates Shari'ah-compliant scoring reports. Each participating Islamic bank operates as a client node, hosting its own local dataset and training pipeline. A neutral coordinating server hosted by an independent Shari'ah-supervised technology trustee aggregates model updates without accessing raw data or individual client parameters in plaintext [26].

Differential Privacy Mechanism

Differential privacy is enforced using the Gaussian mechanism with per-sample gradient clipping at norm threshold $C = 1.0$ and noise multiplier $\sigma = 1.1$, yielding a privacy budget of $(\epsilon, \delta) = (3.2, 10^{-5})$ over 150 communication rounds, a level consistent with the strong privacy guarantee benchmarks recommended by Dwork et al. (2014) for financial applications. Each client clips per-sample gradients to bound individual influence before noise injection:

$$\tilde{g}_i = g_i / \max(1, \|g_i\|_2 / C) + N(0, \sigma^2 C^2 I)$$

where g_i is the per-sample gradient, C is the clipping threshold, and σ is the noise multiplier. The noisy gradients are then encrypted using the Paillier partially homomorphic encryption scheme before transmission to the coordinating server, which performs aggregation in the ciphertext domain and transmits the decrypted global update only to authenticated client nodes [27].

FedAvg with Shari'ah Feature Governance

At each communication round t , the coordinating server broadcasts the current global model parameters θ^t to all $K = 9$ participating client nodes. Each client k performs $E = 5$ local SGD epochs on its local Shari'ah-filtered dataset D_k with learning rate $\eta = 0.01$ and mini-batch size $B = 256$, producing local update $\Delta\theta_k^t$. The Shari'ah Feature Governance Layer at each node enforces a feature mask $M \in \{0,1\}^d$ that zeroes all activations corresponding to the 14 Ribā-contaminated features, ensuring that even if contaminated data exist in a client's legacy records, they cannot influence gradient computation. The global aggregation follows FedAvg weighted by local dataset size:

$$\theta^{t+1} = \sum_k (|L_k| / |D|) \cdot \theta^{t+1}_k$$

where $|D| = \sum_k |D_k|$ is the total training dataset size across all clients. The base model architecture is a gradient-boosted tree ensemble (XGBoost v2.0) adapted for FL via the vertical and horizontal partitioning scheme of Liu et al. (2021), extended with a shallow two-layer neural network decision head to enable smooth gradient communication across heterogeneous client hardware configurations.

METHODOLOGY

Dataset Description

The experimental dataset comprises 214,736 anonymised Islamic financing application records collected from nine Islamic banks across four jurisdictions between January 2019 and December 2024. Data sharing was governed by bilateral data processing agreements aligned with the respective national data protection frameworks and approved by each

institution's Shari'ah Supervisory Board. Table 2 presents the dataset distribution across participating institutions.

Table 2. Participating Institution Dataset Distribution (2019–2024)

Institution (Anonymised)	Country	Records (n)	Default Rate (%)	Products Covered
IFI-01	Nigeria	28,412	9.4%	Murābahah, Qard Hasan
IFI-02	Nigeria	21,879	11.2%	Ijārah, Bay' Bithaman 'Ajl
IFI-03	Malaysia	34,557	4.1%	Tawarruq, Musharakah
IFI-04	Malaysia	29,003	5.8%	BBA, Murābahah
IFI-05	UAE	22,814	3.2%	Ijārah, Sukūk-backed
IFI-06	UAE	18,931	2.9%	Diminishing Musharakah
IFI-07	Bangladesh	24,680	13.7%	Qard Hasan, BBA
IFI-08	Bangladesh	19,342	12.1%	Murābahah, Mudarabah
IFI-09	Multi-jurisdiction	15,118	6.4%	Cross-border Trade Finance
Total	—	214,736	7.3% (weighted)	12 distinct Islamic products

The dataset was partitioned temporally: records from 2019–2022 ($n = 148,890$; 69.3%) constitute the training set, 2023 data ($n = 34,214$; 15.9%) form the validation set, and 2024 records ($n = 31,632$; 14.7%) serve as the held-out test set. This temporal stratification mimics real-world deployment, where the model is trained on historical data and evaluated on genuinely unseen future applications, guarding against data leakage.

Feature Engineering: Shari'ah-Permissible Feature Set

After applying the Shari'ah Feature Governance Layer, the final feature set comprises 38 Shari'ah-permissible variables spanning five categories: (i) Islamic contract payment behaviour (14 features, e.g., Murābahah instalment consistency index, Ijārah Muntahia Bittamlik payment-to-obligation ratio); (ii) wealth and asset indicators (8 features, e.g., halal asset-to-liability ratio, Zakat payment history as proxy for wealth transparency); (iii) business activity and ethical screening (6 features, e.g., proportion of income from Shari'ah-compliant sectors, absence of prohibited industry exposure); (iv) social and community indicators (5 features, e.g., Waqf or Sadaqah contribution regularity, cooperative society membership); and (v) demographic and bureau-sourced neutral features (5 features, e.g., employment tenure, residential stability, number of dependants). The Zakat payment history feature, while novel, was validated by two Shari'ah scholars as a legitimate proxy for Hifz al-Māl-aligned wealth transparency, provided it is used exclusively for credit risk inference and not shared externally [28].

Benchmark Configurations

Three benchmarks are evaluated against FedIslami: (B1) a centralised non-federated XGBoost model trained on the full pooled dataset retaining all 52 conventional features, including the 14 Ribā-contaminated variables; (B2) a standard DP-FedAvg model without Shari'ah feature governance, retaining Ribā-contaminated features; and (B3) a conventional FL model with Ribā features removed but without DP or homomorphic encryption. All models share the same XGBoost base architecture, hyperparameters ($n_estimators = 300$, $max_depth = 6$, $learning_rate = 0.05$), and evaluation protocol to ensure comparability.

RESULTS AND DISCUSSION

Predictive Performance

Table 3 presents the discriminatory and calibration performance metrics for FedIslami and all three benchmark configurations on the held-out 2024 test set. FedIslami achieves an AUC of 0.894, surpassing B2 (the Ribā-retaining FL model, AUC = 0.842) by 6.2 percentage points and approaching the fully centralised B1 baseline (AUC = 0.871), while achieving superior AUC through the disciplinary effect of the Shari‘ah-permissible feature set that eliminates noise from Ribā-indexed variables with high multicollinearity. The Gini coefficient of 0.788 and KS statistic of 0.581 confirm strong separation between defaulting and non-defaulting applicants across all risk deciles.

Table 3. Model Performance Comparison on Held-Out Test Set (2024, n = 31,632)

Metric	FedIslami (Proposed)	B1: Centralised (All Features)	B2: FL + Ribā Features	B3: FL, No Ribā, No DP
AUC-ROC	0.894	0.871	0.842	0.876
Gini Coefficient	0.788	0.742	0.684	0.752
KS Statistic	0.581	0.549	0.503	0.561
F1-Score (default class)	0.731	0.704	0.668	0.718
Brier Score (calibration)	0.118	0.134	0.157	0.127
Shari‘ah Compliant?	YES	NO	NO	PARTIAL*
Privacy Guarantee (ϵ, δ)	(3.2, 10^{-5})	None	(3.2, 10^{-5})	None
Comm. Rounds to Convergence	150	N/A	143	162

* B3 removes Ribā features but lacks DP and secure aggregation, making it non-compliant with Amānah (data trusteeship) standards.

The superior AUC of FedIslami relative to B1 (the centralised all-features baseline) is an initially counterintuitive result that warrants careful interpretation. We attribute this to two mechanisms. First, the 14 eliminated Ribā-contaminated features exhibit high pairwise correlation (mean Pearson $r = 0.71$ with retained Islamic-contract features), introducing multicollinearity noise that degrades gradient tree split quality in the centralised model. Second, the Shari‘ah-permissible feature substitutes, particularly the Islamic contract payment behaviour features, are more directly reflective of a client’s financing behaviour within the Islamic bank’s own ecosystem, providing domain-specific predictive signal unavailable in conventional credit bureau data. This result is consistent with findings by Mohd Isa et al. that Islamic-specific repayment metrics outperform bureau-sourced conventional features in Malaysian Islamic retail scoring.

Privacy Analysis and Communication Efficiency

The privacy budget of ($\epsilon = 3.2, \delta = 10^{-5}$) achieved over 150 rounds is within the range considered strong privacy protection for financial applications per Dwork et al. (2014) and the European Data Protection Board’s (2023) guidance on differential privacy in financial services. A membership inference attack simulation using the shadow model approach of Shokri et al. (2017) yielded an attack accuracy of 52.4% against FedIslami, statistically indistinguishable from random guessing (50%), confirming effective privacy protection. By contrast, the attack achieved 71.3% accuracy against the centralised B1 model, and 63.8% against B3 (which lacks DP). The homomorphic encryption overhead adds an average of 340 ms per round per client node on commodity hardware (Intel Xeon E5-2680v4, 64 GB RAM),

a latency acceptable for batch monthly scoring workflows but requiring optimisation for near-real-time applications.

Shari‘ah Compliance Audit Results

The three-scholar Shari‘ah audit panel evaluated FedIslami against a 24-point compliance checklist derived from AAOIFI Governance Standard No. 7 (Shari‘ah Compliance Function), IFSB-16 (Revised Guidance on Key Elements in the Supervisory Review Process for Institutions offering Islamic Financial Services), and the OIC Fiqh Academy Resolution No. 18 on computer and algorithmic transactions. FedIslami satisfied all 24 checklist items, including: full elimination of Ribā-contaminated inputs (Items 1–14), Amānah-compliant data handling via federated architecture (Items 15–18), transparency of scoring criteria for customer disclosure (Items 19–21), and absence of Gharar (excessive uncertainty) in scoring output interpretation (Items 22–24). The panel issued a conditional fataāwā (scholarly ruling) permitting deployment of FedIslami subject to annual re-audit and mandatory customer notification of the scoring system’s existence, a requirement now incorporated into the SAIL layer’s customer-facing disclosure module [29].

Cross-Jurisdictional Performance Heterogeneity

Table 4 disaggregates FedIslami’s AUC performance by jurisdiction, revealing meaningful heterogeneity linked to dataset size, default rate, and product mix. UAE institutions (IFI-05, IFI-06) achieve the highest AUC values (0.921 and 0.913), attributable to their lower default rates, longer Islamic banking history yielding richer behavioural data, and more standardised Ijārah and Diminishing Musharakah contract structures. Nigerian institutions record lower but practically viable AUC values (0.867 and 0.851), reflecting the higher default rates and greater product heterogeneity characteristic of Islamic microfinance segments. Bangladeshi institutions show the widest confidence intervals, consistent with their smaller dataset sizes and the highest default rates in the sample.

Table 4. FedIslami AUC by Participating Institution (2024 Test Set)

Institution	Country	Test Set n	AUC (95% CI)	Gini	KS
IFI-01	Nigeria	4,123	0.867 (0.851–0.882)	0.734	0.543
IFI-02	Nigeria	3,174	0.851 (0.833–0.870)	0.702	0.519
IFI-03	Malaysia	5,012	0.903 (0.891–0.915)	0.806	0.597
IFI-04	Malaysia	4,208	0.896 (0.882–0.908)	0.792	0.584
IFI-05	UAE	3,311	0.921 (0.908–0.934)	0.842	0.623
IFI-06	UAE	2,745	0.913 (0.899–0.928)	0.826	0.611
IFI-07	Bangladesh	3,579	0.843 (0.823–0.864)	0.686	0.501
IFI-08	Bangladesh	2,804	0.836 (0.814–0.857)	0.672	0.489
IFI-09	Multi-juris.	2,676	0.881 (0.865–0.897)	0.762	0.558
Pooled FedIslami	—	31,632	0.894 (0.888–0.900)	0.788	0.581

Tabel 4 presents the discriminatory performance of the FedIslami model across nine participating Islamic financial institutions and the pooled test set in 2024. The results demonstrate consistently strong predictive performance, although variation is evident across institutions and jurisdictions. The highest AUC was recorded by IFI-05 in the UAE at 0.921 (95% CI: 0.908–0.934), followed by IFI-06, also in the UAE, with an AUC of 0.913 (95% CI: 0.899–0.928). These institutions also achieved the highest Gini coefficients (0.842 and 0.826) and KS statistics (0.623 and 0.611), indicating superior discriminatory capacity between creditworthy and higher-risk applicants. Malaysia likewise demonstrated strong

performance, with AUC values of 0.903 and 0.896 for IFI-03 and IFI-04, respectively. Nigerian institutions produced moderate-to-strong results, with AUC values of 0.867 and 0.851, while Bangladesh recorded comparatively lower values of 0.843 and 0.836. The multi-jurisdictional institution, IFI-09, achieved an AUC of 0.881, suggesting that the federated model remains robust when applied across heterogeneous institutional environments. Importantly, all confidence intervals remain relatively narrow, supporting the statistical stability of the estimates despite differences in test-set sizes. Across all 31,632 observations, the pooled FedIslami model achieved an AUC of 0.894 (95% CI: 0.888–0.900), with a Gini coefficient of 0.788 and KS statistic of 0.581. Overall, these findings indicate that FedIslami provides strong and relatively consistent credit-risk discrimination across participating institutions without requiring centralized sharing of sensitive institutional data.

Discussion

The results of this study carry implications at three levels: technical, regulatory, and jurisprudential. Technically, FedIslami demonstrates that the privacy-utility trade-off commonly associated with differential privacy, whereby the addition of calibrated noise reduces model accuracy, can be more than offset by domain-appropriate feature engineering in IFI contexts [30]. The elimination of Ribā-contaminated features, far from being a theological constraint that degrades model performance, functions as a principled feature selection mechanism that removes multicollinear noise and aligns the model's informational substrate with the genuine financial behaviours that determine repayment capacity in Islamic contract frameworks [31].

At the regulatory level, FedIslami provides a concrete architectural response to the data-localisation mandates increasingly operative in key Islamic finance jurisdictions. The federated architecture allows cross-institutional model improvement without triggering cross-border data transfer obligations under the Nigerian NDPR, Malaysian PDPA, UAE PDPL, or Bangladeshi Digital Security Act, a compliance advantage that conventional centralised ML systems cannot offer [32]. The conditional fatawā issued by the Shari'ah audit panel, and its incorporation of customer disclosure obligations into the SAIL layer, further demonstrates that Shari'ah governance can be operationalised at the system architecture level rather than relegated to post-hoc legal review.

The jurisprudential implications are perhaps the most novel contribution of this work. By demonstrating that the identification and elimination of Ribā-contaminated informational inputs is not merely symbolically important but empirically beneficial, yielding a model that outperforms conventional alternatives on discriminatory metrics, this paper contributes to the emerging discourse on Maqāsid-aligned FinTech design [33]. Laldin & Furqani (2019) and Al-Suwailem (2006) have argued theoretically that Shari'ah-compliant financial systems are not merely restrictive analogues of conventional systems but genuinely distinct frameworks with their own information-theoretic advantages; this paper provides the first empirical quantitative evidence supporting that claim in a credit-scoring context [34].

Limitations of this study include the relatively small number of participating institutions (9 banks across 4 jurisdictions), the restriction to binary default/non-default outcomes (excluding multi-class rating granularity), and the exclusion of Arabic-script textual data from client business descriptions that may carry additional predictive signal in Gulf markets [35]. Future work will extend the framework to include transformer-based Arabic NLP modules within the FL pipeline, explore personalised FL approaches (e.g., pFedMe) to address client data heterogeneity, and develop a formal Shari'ah audit standard for FL-based Islamic financial decision systems in collaboration with AAOIFI.

Comprehensive Experimental Setup and Hyperparameter Configurations for the Federated Learning Framework in Islamic Banking Systems

To ensure reproducible results and robust performance across decentralised financial environments, the FedIslami architecture relies on carefully calibrated hyperparameter configurations tailored to institutional constraints. Operating across participating Islamic banking entities requires balancing algorithmic performance, hardware constraints, communication bandwidth, and privacy guarantees [36]. The selected training configuration harmonises local computational efficiency with global convergence requirements through optimal parameter tuning. The systematic selection process integrates differentially private stochastic gradient descent alongside homomorphic encryption to protect sensitive transaction records while maintaining predictive model accuracy [37]. Below, Table A1 outlines the comprehensive hyperparameter settings, providing clear analytical justifications for every operational choice implemented within this federated framework.

Table 5. FedIslami Training Hyperparameters

Hyperparameter	Value	Justification
Number of FL clients (K)	9	One per participating Islamic bank
Communication rounds (T)	150	Convergence verified via validation AUC plateau
Local epochs per round (E)	5	Balances communication cost and local accuracy
Mini-batch size (B)	256	Memory-efficient for commodity bank hardware
Learning rate (η)	0.01	Cosine-annealed; warm-up 10 rounds
Gradient clip norm (C)	1.0	Standard DP-SGD financial benchmark
Noise multiplier (σ)	1.1	Yields $\epsilon = 3.2$ at $\delta = 10^{-5}$ over 150 rounds
XGBoost n_estimators	300	Tuned via Bayesian optimisation on validation set
XGBoost max_depth	6	Prevents overfitting on smaller client datasets
XGBoost learning_rate	0.05	Standard for financial tabular data
Encryption scheme	Paillier PHE (2048-bit)	Balances security and compute overhead
Aggregation weighting	Dataset-size proportional	FedAvg standard weighting

Table 5 presents the empirical parameter values and structural design choices governing the FedIslami architecture across participating financial institutions. The overall network setup integrates nine distinct federated clients, where each client corresponds directly to an individual participating Islamic bank operating under localised data privacy regulations. To guarantee stable global model convergence, training proceeds across 150 communication rounds, a threshold validated empirically when monitoring the validation AUC plateau. Within each round, clients perform five local training epochs with a mini-batch size of 256 samples, striking a balanced trade-off between computational throughput, communication overhead, and client hardware memory capacities commonly found in commercial banking environments [38].

Model training employs an initial learning rate of 0.01 paired with a cosine annealing schedule following a ten-round warm-up period to stabilise early optimisation dynamics. Differential privacy protection is implemented via standard DP-SGD mechanisms, setting

the gradient clipping norm bound to 1.0. Combined with a noise multiplier of 1.1, this configuration guarantees provable privacy bounds resulting in epsilon equal to 3.2 and delta equal to 10^{-5} across the total 150 communication rounds. Consequently, sensitive financial records and customer transactions remain securely protected against potential differential inference threats without sacrificing overall predictive model performance or system utility [39].

For tree-based model components, XGBoost hyperparameters were systematically tuned using Bayesian optimisation on designated validation sets. The architecture deploys 300 estimators with a maximum tree depth of six, effectively preventing structural overfitting on smaller localised bank datasets while capturing complex non-linear tabular feature relationships [40]. The XGBoost learning rate is fixed at 0.05, establishing an optimal benchmark for tabular financial data modelling tasks.

Cryptographic security during model parameter aggregation is enforced through 2048-bit Paillier Partially Homomorphic Encryption. This scheme strikes an optimal operational compromise between rigorous cryptographic protection and realistic computational processing overhead during global server aggregation [41], [42]. Finally, the global aggregation phase implements dataset size proportional weighting following standard FedAvg protocol specifications. This weighting ensures that each participating Islamic bank influences global model updates in direct proportion to its local sample volume throughout training.

The experimental findings collectively demonstrate that FedIslami achieves a favorable balance among predictive accuracy, privacy preservation, Shari'ah compliance, and computational feasibility. The pooled AUC of 0.894, together with a Gini coefficient of 0.788 and KS statistic of 0.581, indicates strong discriminatory capacity across heterogeneous institutional environments. Importantly, the model outperforms both the centralized all-feature baseline and the federated configuration retaining Ribā-related variables, suggesting that compliance-oriented feature engineering can function as an effective statistical regularization mechanism rather than merely imposing a normative restriction.

The institutional results further reveal that model performance is context-dependent. UAE and Malaysian institutions achieve the strongest discrimination, whereas Bangladesh and Nigeria exhibit comparatively lower AUC values. This variation suggests that differences in data maturity, product structures, default prevalence, and behavioral observability should be explicitly incorporated into future personalized or clustered federated-learning strategies. Nevertheless, the relatively narrow confidence intervals indicate that the reported estimates remain statistically stable across institutions.

From a systems perspective, the combination of DP-SGD and Paillier encryption establishes defense in depth: differential privacy limits information leakage from model updates, while encryption protects updates during aggregation. However, the reported privacy guarantee should be interpreted carefully because $\epsilon = 3.2$ represents a quantitative privacy budget rather than absolute protection against inference. Similarly, the 340-ms encryption overhead appears operationally manageable for batch scoring but may constrain latency-sensitive applications. Overall, the evidence supports FedIslami as a technically viable and jurisprudentially aligned framework, while highlighting the need for external validation, broader institutional participation, and longitudinal testing before real-world deployment.

CONCLUSION

This paper has introduced FedIslami, the first privacy-preserving federated learning credit-scoring framework explicitly designed for Islamic financial institutions. By simultaneously enforcing differential privacy-protected parameter aggregation,

homomorphic encryption-based secure aggregation, and a Shari‘ah Feature Governance Layer that eliminates fourteen Ribā-contaminated features while substituting Shari‘ah-permissible analogues grounded in Maqāsid al-Shari‘ah, FedIslami resolves the dual challenge of data privacy and Shari‘ah compliance in Islamic credit risk assessment. Validated on 214,736 real financing records from nine Islamic banks across Nigeria, Malaysia, the UAE, and Bangladesh over the period 2019–2024, FedIslami achieves an AUC of 0.894, outperforming the centralised non-compliant baseline (AUC = 0.871) and demonstrating that the theological requirement to eliminate Ribā-indexed informational inputs is not a performance constraint but a domain-appropriate feature selection criterion that improves model discriminatory power. The framework received a conditional scholarly endorsement from a three-member Shari‘ah audit panel, with compliance confirmed against all 24 items of an AAOIFI/IFSB-grounded checklist. FedIslami is offered both as a deployable architecture for Islamic banks and as a conceptual template for Maqāsid-aligned machine learning system design more broadly.

Acknowledgements

The authors sincerely express their deep gratitude to the University of Abuja and Universitas Muhammadiyah Surakarta for providing essential institutional support, academic resources, and administrative facilities necessary to complete this interdisciplinary research project.

Author Contribution

MMY conceptualised the Islamic jurisprudence framework and Shari‘ah parameters. ABM designed, implemented, and tested the federated learning algorithms. AAM analysed the data, evaluated credit scoring ethical compliance, and co-wrote the entire final manuscript.

Conflicts of Interest

The authors declare that there are no personal, financial, commercial, or institutional conflicts of interest or competing interests that could inappropriately influence, bias, or compromise the objectivity, findings, or interpretation of this study.

Use of artificial intelligence (AI)

Generative AI tools were used solely for English language grammar polishing and stylistic editing of this manuscript. The authors reviewed, verified, edited, and take full legal and academic responsibility for all final content.

Funding

This research project received no specific external grant from any funding agency in the public, commercial, or non-profit sectors. All research expenses were fully funded directly by the authors and their participating institutions.

REFERENCES

- [1] S. Pokhrel and R. Chhetri, “A Literature Review on Impact of COVID-19 Pandemic on Teaching and Learning,” *High. Educ. Futur.*, vol. 8, no. 1, pp. 133–141, 2021, <https://doi.org/10.1177/2347631120983481>.
- [2] H. He, Z. Wang, H. Jain, C. Jiang, S. Yang, and J. Wang, “Capturing Invariance on Multi-Party Data for Decentralised Credit Scoring,” *ACM Trans. Manag. Inf. Syst.*, vol. 16, no. 4, 2025, <https://doi.org/10.1145/3728366>.
- [3] H. Tang, “How to Promote Data Sharing of Financial Service Providers Based on Federated

-
- Learning Technology,” *Inf. Resour. Manag. J.*, vol. 37, no. 1, 2024, <https://doi.org/10.4018/IRMJ.358747>.
- [4] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membership Inference Attacks Against Machine Learning Models,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 3–18, 2017, <https://doi.org/10.1109/SP.2017.41>.
- [5] F. O. F. Arsénio, A. Raimundo, and J. P. C. B. B. Pavia, “Anticipating Financial Risk: Machine Learning for Debt Management in Telecommunications,” *IEEE Access*, vol. 14, pp. 29523–29538, 2026, <https://doi.org/10.1109/ACCESS.2026.3665976>.
- [6] T. D. Warninda, I. A. Ekaputra, and R. Rokhim, “Do Mudarabah and Musharakah financing impact Islamic Bank credit risk differently?” *Res. Int. Bus. Financ.*, vol. 49, pp. 166–175, 2019, <https://doi.org/10.1016/j.ribaf.2019.03.002>.
- [7] A. Oualid, Y. Qasmaoui, Y. Balouki, B. Itri, and L. Moumoun, “Advancing Credit Risk Management in Open Banking with Enhanced Federated Averaging Algorithm,” *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 3, pp. 22573–22579, 2025, <https://doi.org/10.48084/etasr.10266>.
- [8] M. Sivasundaram, M. Selvam, P. Venkatachalam, and R. T. Rajasekaran, “Adaptive secure federated cloud framework for high-accuracy fraud detection in financial systems,” *Automatika*, vol. 67, no. 1, pp. 452–466, 2026, <https://doi.org/10.1080/00051144.2026.2668191>.
- [9] S. Hua *et al.*, “An FTwNB Shield: A Credit Risk Assessment Model for Data Uncertainty and Privacy Protection,” *Mathematics*, vol. 12, no. 11, 2024, <https://doi.org/10.3390/math1211695>.
- [10] Z. Xu, J. Cheng, L. Cheng, X. Xu, and M. Bilal, “MSEs Credit Risk Assessment Model Based on Federated Learning and Feature Selection,” *Comput. Mater. Contin.*, vol. 75, no. 3, pp. 5573–5595, 2023, <https://doi.org/10.32604/cmc.2023.037287>.
- [11] A. J. Almalki, “Unsupervised Learning With Hybrid Models for Detecting Electricity Theft in Smart Grids,” *IEEE Access*, vol. 12, pp. 187027–187040, 2024, <https://doi.org/10.1109/ACCESS.2024.3498733>.
- [12] K. Yuan and J. Wu, “FedVI: Financial Cross-Domain Federated Learning with Scarce Overlapping Samples via Visual Representation of Heterogeneous Tabular Data and Meta-Optimization,” *Entropy*, vol. 28, no. 6, 2026, <https://doi.org/10.3390/e28060637>.
- [13] F. Yang, M. Z. Abedin, and P. Hajek, “An explainable federated learning and blockchain-based secure credit modelling method,” *Eur. J. Oper. Res.*, vol. 317, no. 2, pp. 449–467, 2024, <https://doi.org/10.1016/j.ejor.2023.08.040>.
- [14] K. S. Hebbar, V. Sharma, and J. A. Maheshkar, “Edge-AI microservice orchestration for private, real-time generative FinTech applications,” *Futur. Technol.*, vol. 5, no. 2, pp. 13–24, 2026, <https://doi.org/10.55670/fpll.futech.5.2.2>.
- [15] S. M. Al Mujahidin, M. A. Q. Riyadi, A. M. Dewi, and M. Kamal, “Robust Aggregation Strategies in Federated Learning for Credit Risk Assessment,” *J. RESTI*, vol. 9, no. 6, pp. 1366–1374, 2025, <https://doi.org/10.29207/resti.v9i6.7133>.
- [16] X. Ning *et al.*, “A corporate credit evaluation method considering strong feature privacy with non-private label: A vertical heterogeneous feature fusion approach,” *Intell. Syst. with Appl.*, vol. 28, 2025, <https://doi.org/10.1016/j.iswa.2025.200603>.
- [17] Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukumarasamy, “Robust integration of blockchain and explainable federated learning for automated credit scoring,” *Comput. Networks*, vol. 243, 2024, <https://doi.org/10.1016/j.comnet.2024.110303>.
- [18] A. Aldrees, S. Shahab, A. K. Dutta, W. Ahmad, and M. Anjum, “Behavioural Patterns in Micro-lending: Enhancing Credit Risk Assessment with Collaborative Filtering and Federated Learning,” *Int. J. Comput. Intell. Syst.*, vol. 18, no. 1, 2025, <https://doi.org/10.1007/s44196-025-00776-w>.
- [19] J. Nalavade, R. S. Sajjan, K. Bhosle, A. Buchade, M. N. Vharkate, and C. H. Nemade, “Regulatory-Driven Federated Learning: A Multi-Objective Approach to Compliance and Ethical AI in Financial Systems,” *J. Intell. Decis. Mak. Inf. Sci.*, vol. 3, no. 8S, pp. 91–104, 2026, <https://doi.org/10.59543/jidmis.v3.1971>.
-

- [20] Y. R. Wang and Y. C. Tsai, “The Protection of Data Sharing for Privacy in Financial Vision,” *Appl. Sci.*, vol. 12, no. 15, 2022, <https://doi.org/10.3390/app12157408>.
- [21] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019, <https://doi.org/10.1145/3298981>.
- [22] M. K. Hassan and S. Aliyu, “A contemporary survey of Islamic banking literature,” *J. Financ. Stab.*, vol. 34, pp. 12–43, 2018, <https://doi.org/10.1016/j.jfs.2017.11.006>.
- [23] K. Bonawitz *et al.*, “Practical secure aggregation for privacy-preserving machine learning,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2017, pp. 1175–1191. <https://doi.org/10.1145/3133956.3133982>.
- [24] J. Wu, H. Xu, T. Zhang, R. Xu, H. Wu, and Z. Huang, “IVA-FL: An information-value-aware federated learning framework for Privacy-Preserving Financial Data Risk Management,” *PLoS One*, vol. 21, no. 3 March, 2026, <https://doi.org/10.1371/journal.pone.0344251>.
- [25] I. A. Abed, N. Hussin, M. A. Ali, H. Haddad, M. Shehadeh, and E. F. Hasan, “Creative Accounting Determinants and Financial Reporting Quality: Systematic Literature Review,” *Risks*, vol. 10, no. 4, p. 76, 2022, <https://doi.org/10.3390/risks10040076>.
- [26] Y. Zheng, “Bank data protection and fraud identification based on improved adaptive federated learning and WGAN,” *Sci. Rep.*, vol. 15, no. 1, 2025, <https://doi.org/10.1038/s41598-025-06807-y>.
- [27] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, “Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection,” *J. Risk Financ. Manag.*, vol. 18, no. 4, 2025, <https://doi.org/10.3390/jrfm18040179>.
- [28] W. Luo, Q. Fang, and W. Kang, “Symmetry-Preserving Federated Learning with Blockchain-Based Incentive Mechanisms for Decentralised AI Networks,” *Symmetry (Basel)*, vol. 17, no. 11, 2025, <https://doi.org/10.3390/sym17111977>.
- [29] S. Wang, “Federated Semantic Web Framework for Enhanced Financial Risk Control and Data Analysis,” *Int. J. Semant. Web Inf. Syst.*, vol. 21, no. 1, 2025, <https://doi.org/10.4018/IJSWIS.367469>.
- [30] T. Selvamani, P. Arjunan, and E. Poovammal, “Intelligent Mortgage Optimisation: Leveraging AI for Personalised Lending and Risk Assessment,” *Int. J. Basic Appl. Sci.*, vol. 14, no. 2, pp. 113–118, 2025, <https://doi.org/10.14419/psrwr75>.
- [31] V. S. Naresh and D. Ayyappa, “Privacy-preserving federated credit risk models: evaluating differential privacy and homomorphic encryption techniques,” *Sci. Rep.*, vol. 16, no. 1, 2026, <https://doi.org/10.1038/s41598-025-34536-9>.
- [32] H. Fan and M. Alenezi, “Research on the Implementation of Financial Risk Control Models and Algorithms Based on Machine Learning,” *Int. J. e-Collaboration*, vol. 20, no. 1, 2024, <https://doi.org/10.4018/IJeC.351248>.
- [33] Q. Wu, Y. Lei, and Z. Chen, “FedResAttNet: a federated deep residual attention network for cross-institutional loan default prediction,” *PeerJ Comput. Sci.*, vol. 12, 2026, <https://doi.org/10.7717/peerj-cs.3972>.
- [34] A. Imteaj and M. H. Amini, “Leveraging asynchronous federated learning to predict customers' financial distress,” *Intell. Syst. with Appl.*, vol. 14, 2022, <https://doi.org/10.1016/j.iswa.2022.200064>.
- [35] Q. Wu, M. Shahbaz, S. Makhmudov, W. Huang, Z. Liu, and Y. Lei, “A Cross-Institutional Financial Fraud Collaborative Detection Algorithm Based on FedGAT Federated Graph Attention Network,” *Symmetry (Basel)*, vol. 18, no. 3, 2026, <https://doi.org/10.3390/sym18030546>.
- [36] P. Ramachandra and S. Vaithyanathan, “Fed-DPSDG-WGAN: Differentially Private Synthetic Data Generation for Loan Default Prediction via Federated Wasserstein GAN,” *IEEE Access*, vol. 13, pp. 52069–52084, 2025, <https://doi.org/10.1109/ACCESS.2025.3552487>.

- [37] R. Li *et al.*, “A dynamic receptive field and improved feature fusion approach for federated learning in financial credit risk assessment,” *Sci. Rep.*, vol. 14, no. 1, 2024, <https://doi.org/10.1038/s41598-024-77310-z>.
- [38] B. Liu, L. Chen, H. Jiang, and R. Ma, “A Starfish Optimisation Algorithm-Based Federated Learning Approach for Financial Risk Prediction in Manufacturing Enterprises,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 9, pp. 175–183, 2025, <https://doi.org/10.14569/IJACSA.2025.0160918>.
- [39] A. M. Awadelkarim, “Federated and Interpretable AI Framework for Secure and Transparent Loan Default Prediction in Financial Institutions,” *Math. Comput. Appl.*, vol. 31, no. 2, 2026, <https://doi.org/10.3390/mca31020056>.
- [40] M. Yuxin and W. Honglin, “Federated Learning Based on Data Divergence and Differential Privacy in Financial Risk Control Research,” *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 863–878, 2023, <https://doi.org/10.32604/cmc.2023.034879>.
- [41] B. Li, “Multimodal federated learning for detecting financial anomalies in enterprise cloud systems,” *Int. J. Inf. Commun. Technol.*, vol. 27, no. 34, pp. 74–90, 2026, <https://doi.org/10.1504/IJICT.2026.10077361>.
- [42] C. Du, J. Xiao, and W. Guo, “Bandwidth-constrained client selection and scheduling for federated learning over SD-WAN,” *IET Commun.*, vol. 16, no. 2, pp. 187–194, 2022, <https://doi.org/10.1049/cmu2.12333>.