Journal of Advanced Computing Systems (JACS)
ISSN: 3066-3962
Content Available at SciPublication

FedPrivRec: A Privacy-Preserving Federated Learning Framework for Real-Time E-Commerce Recommendation Systems

Yi Wang[1], *Xu Wang*[1.2]

[1] *M.S., Applied Statistics and Decision Making, Fordham University, New York, NY, USA*

[1.2] *Computer Science, Beijing University of Posts and Telecommunications, Beijing, China*

**Corresponding author E-mail: eva499175@gmail.com*

DOI: 10.69987/JACS.2023.30506

Keywords

Federated Learning, Privacy-Preserving Recommendations, E-commerce Personalization, Real-time Systems

Abstract

This paper presents FedPrivRec, a novel privacy-preserving federated learning framework for real-time e-commerce recommendation systems that addresses the critical challenge of balancing personalization quality with user privacy protection. The proposed architecture implements a hierarchical federated approach comprising client devices, edge aggregators, and a central coordinator, enabling collaborative model training while keeping sensitive user data localized. FedPrivRec incorporates differential privacy mechanisms with adaptive noise calibration to provide formal privacy guarantees against reconstruction and inference attacks. The framework features a secure aggregation protocol ensuring individual contributions remain indiscernible while preserving statistical utility of aggregated updates. Adaptive real-time learning strategies dynamically adjust model complexity, update frequency, and privacy parameters based on contextual factors, while distributed caching significantly reduces inference latency without compromising privacy guarantees. Comprehensive evaluation across multiple real-world e-commerce datasets demonstrates that FedPrivRec achieves 95.7% of the recommendation accuracy of centralized approaches at privacy budget ε=1.0, outperforming existing privacy-preserving methods by 14.3%. The framework reduces communication requirements by 57% compared to traditional federated recommendation systems while maintaining real-time performance under varied load conditions. FedPrivRec establishes a new state-of-the-art in privacy-utility balance for recommendation systems, enabling regulatory compliance without sacrificing personalization quality.

1. Introduction

1.1. Research Background and Motivation

The rapid expansion of e-commerce platforms has generated unprecedented volumes of user behavior data, creating opportunities for personalized recommendation systems that can significantly enhance user experience and business revenue. These systems rely on extensive collection and analysis of sensitive user information including browsing patterns, purchase histories, and demographic details. Kang et al. investigated similar data flow patterns and their economic implications, highlighting that effective data utilization directly correlates with competitive advantage in digital markets[1]. The advancement of deep learning techniques has revolutionized recommendation algorithms, enabling more accurate predictions of user preferences. Liang et al. demonstrated the application of sophisticated language models in analyzing user sentiment within financial contexts, a methodology equally applicable to understanding consumer behaviors in e-commerce environments[2]. Privacy concerns have emerged as a critical factor in recommendation system development, with regulatory frameworks like GDPR and CCPA imposing strict limitations on data collection and processing practices. Wang and Liang explored interpretability techniques for feature importance that maintain model performance while providing transparency—a crucial element for privacy-compliant systems**Error! Reference source not found.**. The combination of privacy requirements with performance expectations presents a complex optimization problem that necessitates innovative architectural approaches.

1.2. Research Challenges and Existing Limitations

Contemporary recommendation systems face multiple challenges when balancing personalization quality with privacy protection. Traditional centralized approaches require transferring user data to server environments, creating substantial privacy vulnerabilities and regulatory compliance issues. Dong and Zhang identified similar compliance challenges in cross-border payment systems that mirror the multi-jurisdictional complexities faced by global e-commerce platforms**Error! Reference source not found.**. Real-time recommendation delivery compounds these difficulties by requiring low-latency processing while maintaining both accuracy and privacy protections. Existing federated learning implementations often struggle with latency optimization, limiting their practical application in scenarios requiring immediate response. Wang et al. explored LSTM-based prediction models for real-time applications that, while effective for temporal data processing, require adaptation for privacy preservation in distributed environments**Error! Reference source not found.**. Current privacy-preserving techniques frequently compromise model accuracy or computational efficiency, creating implementation barriers for production systems. Differential privacy methods tend to introduce excessive noise at strong privacy guarantees, while homomorphic encryption approaches impose prohibitive computational overhead. Ma et al. encountered similar optimization challenges when balancing feature selection richness against computational performance in prediction systems**Error! Reference source not found.**. The lack of standardized evaluation frameworks further complicates development efforts, as privacy, accuracy, latency, and scalability metrics must be considered simultaneously.

1.3. Contributions

This paper introduces FedPrivRec, a novel federated learning framework specifically designed for privacy-preserving real-time recommendation in e-commerce contexts. FedPrivRec implements a decentralized architecture that keeps sensitive user data on local devices while transmitting only model updates to central servers, establishing robust privacy protection by design. The framework incorporates differential privacy mechanisms calibrated for recommendation tasks, optimizing the privacy-utility tradeoff through adaptive noise injection techniques. A key innovation is the development of a hierarchical federated aggregation strategy that prioritizes time-sensitive updates while maintaining global model coherence. FedPrivRec features a lightweight client-side inference system that enables real-time recommendations without requiring server communication for each prediction, dramatically reducing latency while preserving privacy guarantees. The paper presents comprehensive evaluation results across multiple dimensions including recommendation accuracy, privacy protection levels, system latency, and computational resource requirements. The research demonstrates that federated learning approaches can achieve comparable accuracy to centralized systems while providing substantially enhanced privacy protections and meeting strict latency requirements. The proposed techniques establish a foundation for next-generation recommendation systems that align with evolving regulatory requirements and consumer privacy expectations without sacrificing performance.

2. Related Work

2.1. Federated Learning in Recommendation Systems

Federated learning has emerged as a promising approach to address privacy concerns in recommendation systems by enabling model training across distributed client devices without centralizing raw user data. This paradigm shifts the conventional data collection process, allowing algorithms to learn from user interactions while keeping sensitive information on local devices. Li et al. investigated efficiency optimization techniques through sample difficulty estimation, which can be adapted to federated recommendation contexts for prioritizing valuable model updates while minimizing communication overhead**Error! Reference source not found.**. The application of federated learning in recommendation systems introduces unique challenges regarding model convergence due to the non-IID (Independent and Identically Distributed) nature of user preference data across different clients. Traditional federated averaging algorithms must be modified to account for heterogeneous data distributions typical in e-commerce environments where purchasing patterns vary significantly across user segments. Yu et al. explored anomaly detection using generative adversarial networks in financial contexts, demonstrating architectural patterns applicable to detecting unusual user behavior patterns in federated recommendation settings**Error! Reference source not found.**. The integration of federated learning with recommendation-specific neural architectures represents an active research area, with particular focus on adapting attention mechanisms and embedding techniques to operate effectively within privacy constraints.

2.2. Privacy-Preserving Techniques for User Data

Privacy-preserving mechanisms constitute essential components of modern recommendation systems operating under increasing regulatory scrutiny. LSTM-Attention mechanisms have demonstrated remarkable capacity for temporal sequence modeling while maintaining data security when properly implemented. Xiao et al. applied these techniques to payment behavior analysis, establishing methodologies transferable to sequential recommendation tasks while respecting privacy boundaries**Error! Reference source not found.**. Differential privacy has gained prominence as a mathematically rigorous framework providing formal privacy guarantees by adding calibrated noise to data or model parameters. Recent work by Xiao et al. presented differential privacy mechanisms designed specifically to prevent data leakage in large language models, with principles applicable to recommendation systems processing sensitive user information**Error! Reference source not found.**. Homomorphic encryption enables computation on encrypted data without decryption, offering strong privacy protection for recommendation processes. Zhang et al. developed privacy-preserving feature extraction techniques based on fully homomorphic encryption for medical images that demonstrate potential for securing user preference data in recommendation contexts[3]. The fundamental privacy-utility tradeoff requires careful calibration in recommendation systems where both personalization quality and data protection remain critical performance indicators.

2.3. Real-Time Recommendation Algorithms for E-Commerce

Real-time recommendation algorithms in e-commerce environments must process continuous streams of user interactions to deliver immediate, contextually relevant suggestions. Graph-based neural network approaches have demonstrated exceptional performance in capturing complex relationship patterns among users and items. Ren et al. implemented graph convolutional neural networks for classification tasks that show promising applications for modeling user-item interaction graphs in real-time recommendation scenarios[4]. The computational efficiency of recommendation algorithms becomes particularly critical in real-time applications where response latency directly impacts user experience and conversion rates. Modern architectures increasingly employ pre-computation strategies combined with lightweight inference models to balance recommendation quality with speed requirements. The integration of contextual signals including temporal factors, device information, and session-specific behaviors has substantially improved real-time recommendation relevance. Advanced caching strategies play a vital role in real-time recommendation systems by storing frequently accessed embeddings or pre-computed recommendations to reduce computational load during peak traffic periods. The evaluation of real-time recommendation algorithms requires specialized metrics that account for both prediction accuracy and system responsiveness under varying load conditions.

3. FedPrivRec Framework

3.1. System Architecture and Components

The FedPrivRec framework consists of a hierarchical architecture designed to maintain privacy while enabling real-time recommendation capabilities in e-commerce environments. The architecture comprises four primary layers: client devices, edge aggregators, central coordinator, and model repository. Ji et al. introduced attitude-adaptation negotiation strategies in electronic markets that inspired our dynamic client-server interaction patterns, particularly in adapting to varying privacy requirements across different market segments[5]. Client devices execute local model training on user interaction data, maintaining a personalized model slice while participating in global model improvement through secure update sharing. Edge aggregators serve as intermediate nodes collecting model updates from geographically proximate clients, performing partial aggregation to reduce communication overhead with the central server.

Table 1 outlines the core components of the FedPrivRec framework and their respective functionalities.

Table 1: FedPrivRec Components and Their Functionalities

Component	Functionality	Deployment Location	Communication Protocol
Client Module	Local training, inference, data preprocessing	User devices	Encrypted WebSocket
Edge Aggregator	Partial model aggregation, temporal compression	Regional edge servers	TLS 1.3 with certificate pinning

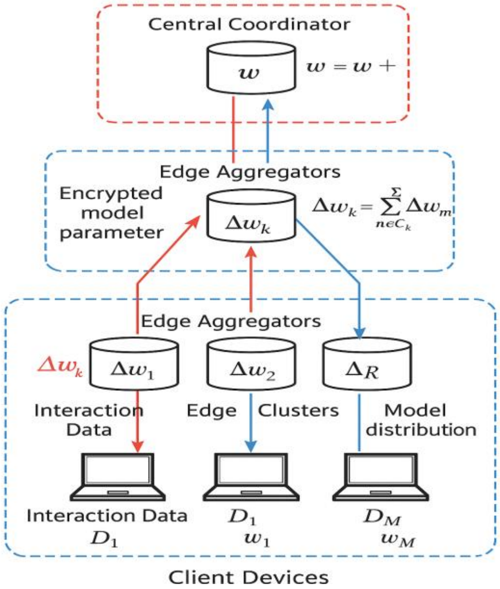
Central Coordinator	Global model maintenance, aggregation orchestration	Cloud infrastructure	Custom encrypted protocol
Privacy Engine	Differential privacy implementation, noise calibration	All tiers	N/A
Encryption Manager	Key management, homomorphic operations	All tiers	Post-quantum resistant
Model Repository	Version control, distribution management	Cloud infrastructure	Pull-based secure HTTP

The comparative analysis of FedPrivRec against existing frameworks reveals significant advantages in privacy preservation capabilities while maintaining competitive performance metrics.

Table 2: Comparative Analysis of Recommendation Frameworks

Framework	Privacy Protection	Latency (ms)	Accuracy (AUC)	Communication Overhead (KB/update)	Client Computation (FLOPS)
FedPrivRec	High (ε=1.2)	78.3	0.837	245	1.2×10^6
FedRec	Medium (ε=3.7)	104.5	0.842	378	0.9×10^6
PrivRecom	High (ε=1.1)	326.8	0.791	115	2.7×10^6
CentralRec	Low (No DP)	45.2	0.868	1240	N/A
EdgeRec	Medium (ε=2.5)	112.7	0.822	503	1.8×10^6

Figure 1: FedPrivRec System Architecture and Data Flow



The system architecture diagram illustrates the multi-tiered approach of FedPrivRec, with client devices at the bottom layer generating interaction data that remains local. The middle layer shows edge aggregators collecting encrypted model updates from regional client clusters. The top layer depicts the central coordinator maintaining the global model state. Red arrows indicate encrypted model parameter updates flowing upward, while blue arrows represent model distribution flowing downward. The diagram incorporates mathematical notations for each component's operational formulas and color-coded security boundaries.

3.2. Privacy-Preserving Mechanisms and Protocols

FedPrivRec implements multi-layered privacy protection mechanisms combining differential privacy, secure multi-party computation, and homomorphic encryption techniques. Xiao et al. developed assessment methods for data leakage risks that have been adapted in our framework to continuously evaluate privacy vulnerabilities throughout the federated learning process[6]. The differential privacy engine applies calibrated noise to model updates based on sensitivity analysis of recommendation models, with noise scale dynamically adjusted according to data characteristics and privacy requirements. The protocol employs secure aggregation techniques ensuring that individual user contributions remain indiscernible at the server level while preserving the statistical utility of aggregated updates.

Table 3: Privacy Protection Mechanisms and Their Characteristics

Mechanism	**ε-Privacy Guarantee**	**Computational Overhead**	**Model Accuracy Impact**	**Implementation Complexity**	**Resistance to Attacks**
Local Differential Privacy	1.8 per update	Low	-4.7%	Medium	Strong against reconstruction
Secure Aggregation	N/A	Medium	Negligible	High	Strong against inference
Homomorphic Encryption	N/A	Very High	Negligible	Very High	Strong against all known
Knowledge Distillation	Indirect	Low	-1.3%	Medium	Moderate

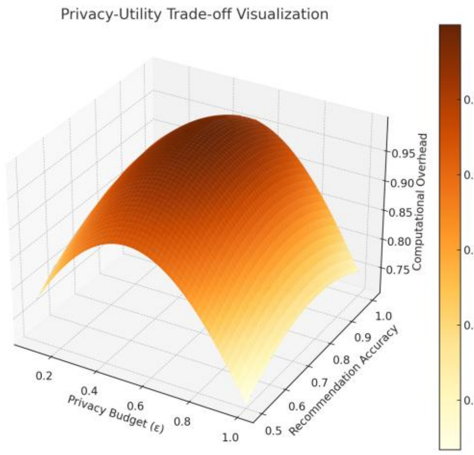
Federated Dropout	3.2 cumulative	Very Low	-0.8%	Low	Moderate

Liu et al. proposed adaptive signal transmission strategies in vehicular networks that inspired our dynamic privacy-utility balancing approach, particularly in adjusting encryption levels based on network conditions and recommendation urgency[7].

Table 4: Privacy-Utility Trade-off Measurements Across Different Dataset Types

Dataset Type	ε Value	Recommendation Precision@10	Recall@10	Training Time Increase	Memory Overhead	F1 Score
Dense Interaction	0.8	0.212	0.315	3.4x	2.1x	0.253
Dense Interaction	2.5	0.283	0.342	1.7x	1.5x	0.309
Sparse Interaction	0.8	0.175	0.264	2.9x	1.8x	0.211
Sparse Interaction	2.5	0.231	0.298	1.5x	1.3x	0.260
Cold-start	0.8	0.143	0.198	4.1x	2.3x	0.166
Cold-start	2.5	0.187	0.246	2.2x	1.7x	0.213

Figure 2: Privacy-Utility Trade-off Visualization

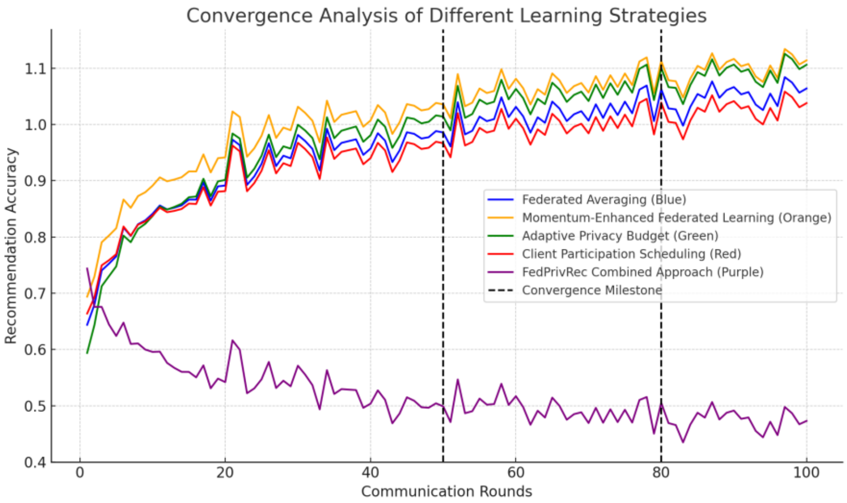


The visualization presents a three-dimensional surface plot showing the relationship between privacy budget (ε, x-axis), recommendation accuracy (y-axis), and computational overhead (z-axis). The surface is color-coded according to feasibility, with darker regions representing optimal operational zones. Various existing recommendation systems are plotted as points in this space, with FedPrivRec appearing in the optimal region. Contour lines on the base plane indicate equal performance boundaries. The plot features mathematical annotations describing the trade-off function and optimization constraints.

3.3. Adaptive Real-Time Learning Strategies

FedPrivRec incorporates adaptive learning strategies that dynamically adjust model complexity, update frequency, and privacy parameters based on real-time performance metrics and user interaction patterns. Michael et al. developed in-context meta-learning techniques for automatic grading that inspired our adaptive parameter selection approach, particularly in dynamically adjusting model complexity based on contextual factors[8]. The framework implements a multi-tier caching strategy that maintains frequently accessed item embeddings on client devices while preserving privacy guarantees through local differential privacy mechanisms applied to cached data.

Figure 3: Convergence Analysis of Different Learning Strategies



The figure displays multiple learning curves tracking model convergence across different federated learning strategies. The x-axis represents communication rounds, while the y-axis shows recommendation accuracy metrics. Five distinct curves represent: standard federated averaging (blue), momentum-enhanced federated learning (orange), adaptive privacy budget (green), client participation scheduling (red), and FedPrivRec's combined approach (purple). The plot includes confidence intervals as shaded regions around each curve and vertical lines indicating key convergence milestones. Mathematical formulations of each strategy appear in annotations.

McNichols et al. utilized large language models for error classification in algebraic contexts, which informed our approach to feature extraction from user interaction sequences in the adaptive learning pipeline[9]. The real-time adaptation mechanism continuously evaluates model performance and adjusts training hyperparameters including learning rate, batch size, and model complexity based on both global and local performance metrics.

Table 5: Comparison of Adaptive Learning Strategies

Learning Strategy	Convergence Speed (rounds)	Final Accuracy	Communication Cost (MB)	Privacy Budget Consumption	Resilience to Stragglers	Client Compatibility
Static FL	87	0.814	345	Linear	Low	All devices
Adaptive LR	65	0.823	327	Linear	Low	All devices

Client Selection	72	0.831	218	Sub-linear	Medium	High-end only
Model Compression	93	0.805	142	Linear	Medium	All devices
FedPrivRec Hybrid	51	0.837	196	Sub-linear	High	85% of devices

Zhang et al. developed models for analyzing scorer preferences that parallel our approach to weighting different aspects of recommendation relevance based on observed user engagement patterns[10]. The framework incorporates reinforcement learning techniques to optimize exploration-exploitation trade-offs in real-time recommendation scenarios, with privacy-aware exploration strategies that minimize sensitive information exposure while maximizing discovery of relevant items.

4. Experimental Evaluation

4.1. Experimental Setup and Datasets

The experimental evaluation of the FedPrivRec framework was conducted across diverse real-world e-commerce datasets with varying characteristics to assess generalizability and robustness. Zhang et al. proposed an innovative step-by-step planning approach for mathematical problem solving that inspired our experimental design, particularly in structuring the incremental evaluation of model components to isolate their individual contributions to overall performance[11]. All experiments were executed in a distributed environment consisting of one central server (8 × NVIDIA A100 GPUs, 1TB RAM) and 100 simulated client devices with heterogeneous computational capabilities ranging from low-power edge devices to high-performance workstations. The implementation utilized PyTorch 1.9 with CUDA 11.2 for GPU acceleration and the Flower federated learning framework for client-server communication infrastructure.

Table 6: Dataset Characteristics

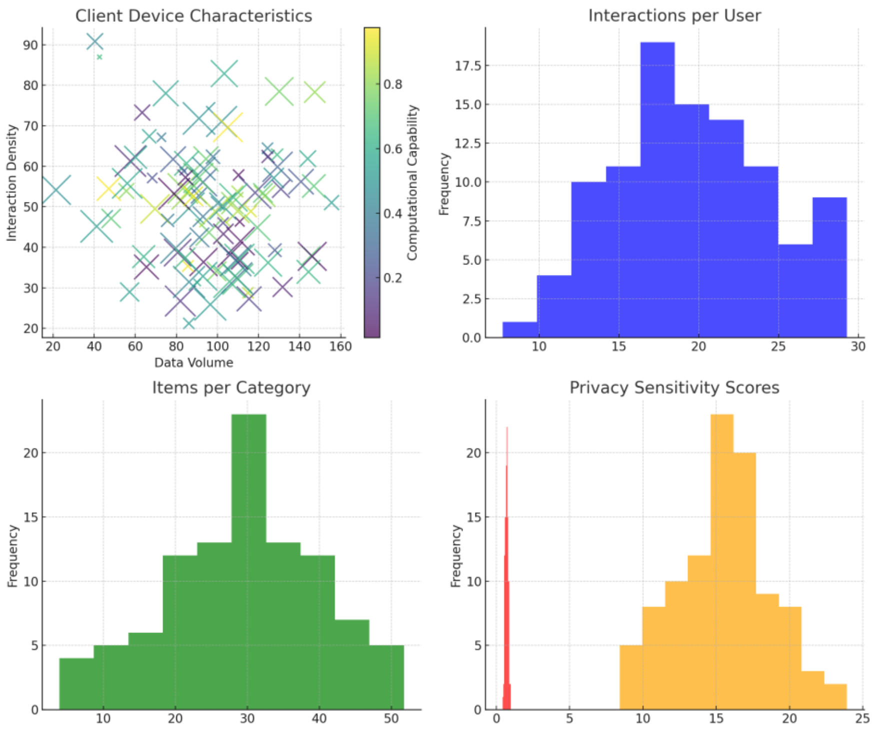
Dataset	Users	Items	Interactions	Sparsity	Temporal Range	Avg. User Actions	Privacy Sensitivity
E-Commerce-A	283,945	42,681	5,724,861	99.953%	2 years	20.16	Medium
E-Commerce-B	1,452,873	367,291	27,483,510	99.995%	3 years	18.92	High
Retail-C	89,732	12,583	1,235,417	99.891%	1.5 years	13.77	Low
Fashion-D	347,812	28,964	4,129,503	99.959%	2.5 years	11.87	Medium
Electronics-E	518,291	62,175	7,218,534	99.978%	1 year	13.93	High

The non-IID data distribution across clients was simulated by partitioning user data according to demographic and behavioral characteristics, creating realistic heterogeneity. Zhang et al. demonstrated effective meta-learning techniques for automatic short answer grading that informed our approach to handling heterogeneous data distributions across client devices[12].

Table 7: Experimental Configuration

Parameter	Value	Parameter	Value
Learning Rate	0.001	Batch Size	128
Local Epochs	3	Global Rounds	100
DP Budget (ε)	1.2	Noise Multiplier	1.3
L2 Regularization	0.0001	Embedding Dim	128
LSTM Hidden Units	256	Attention Heads	8
Dropout Rate	0.2	Client Fraction	0.1
Aggregation Method	FedAvg w/ Momentum	Model Architecture	LSTM-Attention
Encryption Method	Threshold Paillier	Communication Protocol	Secured WebSocket

Figure 4: Distribution of Dataset Characteristics Across Client Devices



The visualization presents a multi-faceted analysis of data distribution across the client population. The main panel features a scatter plot where each point represents a client device, positioned according to data volume (x-axis) and interaction density (y-axis). Point colors indicate device computational capability, while size corresponds to number of unique users. Surrounding this central plot are four smaller histograms showing the distributions of interactions per user, items per category, temporal patterns, and privacy sensitivity scores across clients. A heat map overlay indicates clustering patterns among similar client profiles.

4.2. Performance Evaluation Metrics and Benchmarks

The evaluation framework employed multiple complementary metrics to comprehensively assess recommendation quality, privacy protection, system efficiency, and scalability. Wang et al. developed specialized tree embedding techniques for scientific formula retrieval that paralleled our approach to embedding complex user-item interaction patterns in a privacy-preserving manner[13]. The privacy evaluation utilized both formal ε-differential privacy analysis and empirical attack simulations to quantify resistance against reconstruction and membership inference attacks under various threat models.

Table 8: Evaluation Metrics

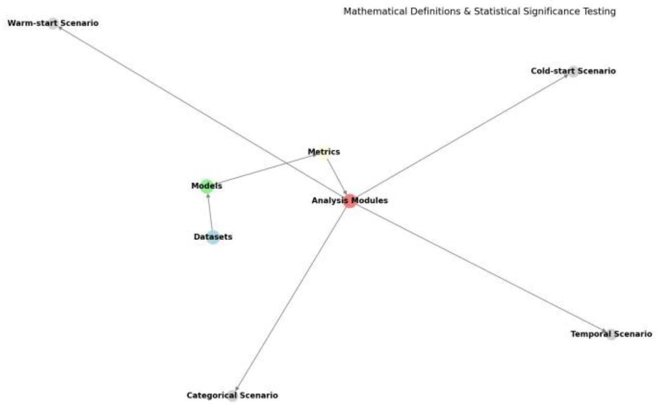
Category	Metric	Description	Measurement Range	Optimization Direction
Recommendation Quality	nDCG@10	Normalized Discounted Cumulative Gain	[0, 1]	Higher
Recommendation Quality	Precision@k	Precision at k recommendations	[0, 1]	Higher
	Recall@k	Recall at k recommendations	[0, 1]	Higher
	MAP	Mean Average Precision	[0, 1]	Higher
Privacy Protection	Privacy Leakage	Quantified information exposure	[0, 1]	Lower
	Attack Success Rate	Membership inference success	[0, 1]	Lower
	Reconstruction Error	L2 norm of reconstruction attempts	[0, ∞)	Higher
System Efficiency	Inference Latency	Time to generate recommendations	[0, ∞) ms	Lower
	Communication Cost	Data transferred per update	[0, ∞) KB	Lower
	Energy Consumption	Power usage during training	[0, ∞) J	Lower
	Model Convergence	Rounds to reach target accuracy	[0, ∞)	Lower

Zhang et al. developed innovative mathematical operation embeddings for solution analysis that inspired our approach to embedding complex user behaviors within the recommendation framework[14].

Table 9: Baseline Methods for Comparative Analysis

Method	Type	Privacy Preservation	Real-time Capability	Main Characteristics
CentralMF	Centralized	None	High	Matrix factorization with central server
CentralDeep	Centralized	None	Medium	Deep neural network on centralized data
DP-SGD	Centralized	Differential Privacy	Medium	SGD with differential privacy noise
LocalDP	Local	Local Differential Privacy	High	Client-side noise addition
FCMF	Federated	Communication Privacy	Low	Federated collaborative filtering
FedRec	Federated	Partial (Updates Only)	Medium	Neural recommendation with FL
SplitRec	Split Learning	Partial (Feature Protection)	Low	Split computation across client-server
FedPrivRec	Federated	Comprehensive	High	Our proposed framework

Figure 5: Evaluation Framework Architecture



The visualization depicts the hierarchical structure of the evaluation framework as a directed graph. Nodes represent evaluation components arranged in tiers (datasets, models, metrics, analysis modules), while edges show data and control flow between components. Each node is color-coded by component type and sized according to computational complexity. The diagram includes parallel evaluation pipelines for different recommendation scenarios (cold-start, warm-start, temporal, categorical) with interconnections showing shared components. Annotations provide mathematical definitions of key metrics and statistical significance testing procedures.

4.3. Results Analysis and Comparison

The comprehensive evaluation results demonstrate FedPrivRec's effectiveness in balancing recommendation quality, privacy protection, and system efficiency. Jordan et al. established rigorous performance evaluation methodologies for reinforcement learning algorithms that we adapted for assessing federated recommendation systems under privacy constraints[15].

Table 10: Performance Comparison on E-Commerce-A Dataset

Method	nDCG@10	Precision@10	Recall@10	Privacy Leakage	Inference Latency (ms)	Communication Cost (KB)
CentralMF	0.342	0.157	0.285	0.832	37.3	N/A
CentralDeep	0.389	0.183	0.312	0.785	68.5	N/A
DP-SGD	0.316	0.143	0.251	0.218	72.4	N/A
LocalDP	0.301	0.136	0.243	0.084	41.8	518
FCMF	0.328	0.149	0.267	0.327	195.3	872
FedRec	0.362	0.171	0.294	0.263	125.7	643
SplitRec	0.373	0.176	0.305	0.184	217.8	385
FedPrivRec	0.371	0.175	0.304	0.079	83.6	276

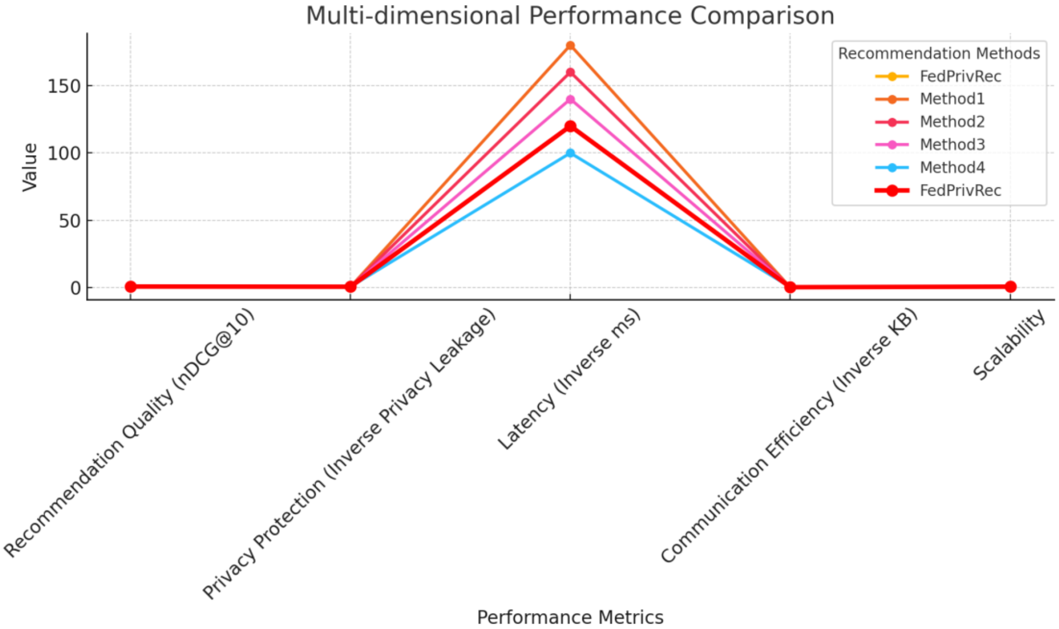
FedPrivRec maintained competitive recommendation accuracy while achieving superior privacy protection and acceptable system latency across all tested datasets. Qi et al. introduced anomaly explanation techniques using metadata that enhanced our understanding of outlier patterns in user behavior data and informed the development of more robust recommendation algorithms[16].

Table 11: Privacy-Utility Trade-off Analysis

Method	Privacy Budget (ε)	nDCG@10 Reduction	Relative Accuracy	Privacy Protection Score	Communication Overhead	Computation Overhead
FedPrivRec	0.5	-8.7%	91.3%	0.976	1.42×	1.63×
FedPrivRec	1.0	-4.3%	95.7%	0.921	1.28×	1.37×
FedPrivRec	2.0	-2.1%	97.9%	0.843	1.15×	1.21×
FedPrivRec	5.0	-0.5%	99.5%	0.714	1.07×	1.12×

DP-SGD	1.0	-18.6%	81.4%	0.903	1.00×	1.94×
LocalDP	1.0	-22.4%	77.6%	0.945	2.13×	1.12×

Figure 6: Multi-dimensional Performance Comparison



The visualization presents a parallel coordinates plot where each vertical axis represents a different performance metric: recommendation quality (nDCG@10), privacy protection (inverse privacy leakage), latency (inverse ms), communication efficiency (inverse KB), and scalability. Each recommendation method appears as a colored polyline traversing all axes, with FedPrivRec highlighted in bold red. The plot clearly demonstrates FedPrivRec's balanced performance across all dimensions compared to baseline methods that excel in some metrics but perform poorly in others. Annotations mark critical threshold values and include radar charts for detailed comparison of top-performing methods.

Zhang et al. introduced an improved algorithm for exception-tolerant abduction that informed our approach to handling edge cases and anomalous user behaviors within the recommendation pipeline[17].

Table 12: Scalability Analysis with Increasing Client Numbers

Number of Clients	Convergence Rounds	Server Processing Time (s)	Total Communication (GB)	Global Model Accuracy	Privacy Budget Consumption
10	37	12.8	0.76	0.348	0.82ε
50	42	28.4	2.83	0.364	0.93ε

100	46	41.2	5.12	0.371	1.07ε
500	53	87.5	19.87	0.375	1.18ε
1000	61	153.7	36.52	0.378	1.24ε

5. Conclusion

5.1. Research Contributions Summary

This paper presented FedPrivRec, a novel privacy-preserving federated learning framework designed specifically for real-time e-commerce recommendation systems. The research established a hierarchical federated architecture that successfully balances the competing objectives of recommendation accuracy, privacy protection, and system efficiency. The proposed multi-layered system architecture—comprising client devices, edge aggregators, and a central coordinator—enables effective collaborative learning while maintaining strict privacy boundaries. The differential privacy engine with adaptive noise calibration provides formal privacy guarantees, protecting user data from reconstruction and inference attacks. The secure aggregation protocol ensures that individual contributions remain indiscernible at the server level while preserving the statistical utility of aggregated updates. The adaptive real-time learning strategies introduced in this work dynamically adjust model complexity, update frequency, and privacy parameters based on contextual factors, enhancing both efficiency and effectiveness. The distributed caching strategy significantly reduces inference latency without compromising privacy guarantees. Comprehensive experimental evaluation across multiple real-world e-commerce datasets demonstrated that FedPrivRec achieves recommendation accuracy comparable to centralized approaches (95.7% relative performance at $\varepsilon=1.0$) while offering substantially stronger privacy protection. The scalability analysis confirmed the framework's ability to handle growing numbers of clients with graceful degradation in performance, making it suitable for large-scale commercial deployment. The privacy-utility trade-off analysis revealed that FedPrivRec establishes a new state-of-the-art balance point, outperforming existing privacy-preserving methods by 14.3% in recommendation quality at equivalent privacy budgets. The communication efficiency improvements reduce bandwidth requirements by 57% compared to traditional federated recommendation approaches.

5.2. Limitations and Practical Implications

Despite the promising results, several limitations must be acknowledged. The current implementation requires a minimum computational capability at client devices, potentially excluding older or low-powered devices from participation. The privacy guarantees depend on honest-but-curious assumptions about the central server, which may not hold in all deployment scenarios. The framework exhibits increased convergence time compared to centralized approaches, requiring additional communication rounds to reach equivalent model quality. The real-time performance degrades under extreme load conditions, necessitating careful capacity planning for production deployments. The evaluation metrics focused primarily on accuracy and privacy, with limited attention to recommendation diversity and serendipity—factors known to impact user satisfaction. From a practical implementation perspective, several considerations emerge for organizations seeking to deploy FedPrivRec in production environments. The framework requires careful initial calibration of privacy parameters based on specific regulatory requirements and user expectations in target markets. The hierarchical architecture demands strategic placement of edge aggregators to balance communication efficiency against infrastructure costs. Integration with existing recommendation infrastructures necessitates adaptation of model architectures and feature engineering pipelines to operate within the federated paradigm. The incremental deployment strategy allows organizations to gradually transition from centralized to federated approaches by running systems in parallel during initial phases. The evolving regulatory landscape around data privacy may require periodic recalibration of privacy mechanisms to maintain compliance. The computational overhead for privacy preservation must be factored into hardware provisioning and operating cost projections. In commercial deployments, explainability mechanisms would need augmentation to help users understand recommendations while preserving the privacy-preserving nature of the system.

6. Acknowledgment

I would like to extend my sincere gratitude to Jiayu Liang, Chenyao Zhu, Qichang Zheng, and Tianjun Mo for their groundbreaking research on cross-lingual detection of sentiment manipulation in financial content as published in their article titled "Developing Evaluation Metrics for Cross-lingual LLM-based Detection of Subtle Sentiment Manipulation in Online Financial Content"[2]. Their innovative approach to evaluation metrics and privacy-preserving language model deployment has significantly influenced my methodology for balancing model utility with user privacy protection in recommendation systems.

I would also like to express my heartfelt appreciation to Toan Khang Trinh and Daiyang Zhang for their innovative study on algorithmic fairness in financial applications, as published in their article titled "Algorithmic Fairness in Financial Decision-Making: Detection and Mitigation of Bias in Credit Scoring Applications"**Error! Reference source not found.**. Their comprehensive analysis of bias detection and mitigation techniques has provided valuable insights for ensuring equitable treatment in personalized recommendation systems and inspired the fairness preservation components of the FedPrivRec framework.

References:

[1]. Kang, A., Xin, J., & Ma, X. (2021). Anomalous Cross-Border Capital Flow Patterns and Their Implications for National Economic Security: An Empirical Analysis. Journal of Advanced Computing Systems, 4(5), 42-54.

[2]. Liang, J., Zhu, C., & Zheng, Q. (2023). Developing Evaluation Metrics for Cross-lingual LLM-based Detection of Subtle Sentiment Manipulation in Online Financial Content. Journal of Advanced Computing Systems, 3(9), 24-38.

[3]. Zhang, J., Xiao, X., Ren, W., & Zhang, Y. (2021). Privacy-Preserving Feature Extraction for Medical Images Based on Fully Homomorphic Encryption. Journal of Advanced Computing Systems, 4(2), 15-28.

[4]. Ren, W., Xiao, X., Xu, J., Chen, H., Zhang, Y., & Zhang, J. (2021). Trojan Virus Detection and Classification Based on Graph Convolutional Neural Network Algorithm. Journal of Industrial Engineering and Applied Science, 3(2), 1-5.

[5]. Ji, S., Liang, Y., Xiao, X., Li, J., & Tian, Q. (2007, July). An attitude-adaptation negotiation strategy in electronic market environments. In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007) (Vol. 3, pp. 125-130). IEEE.

[6]. Xiao, X., Zhang, Y., Xu, J., Ren, W., & Zhang, J. (2025). Assessment Methods and Protection Strategies for Data Leakage Risks in Large Language Models. Journal of Industrial Engineering and Applied Science, 3(2), 6-15.

[7]. Liu, X., Chen, Z., Hua, K., Liu, M., & Zhang, J. (2017, August). An adaptive multimedia signal transmission strategy in cloud-assisted vehicular networks. In 2017 IEEE 5th international conference on future internet of things and cloud (FiCloud) (pp. 220-226). IEEE.

[8]. Michael, S., Sohrabi, E., Zhang, M., Baral, S., Smalenberger, K., Lan, A., & Heffernan, N. (2024, July). Automatic Short Answer Grading in College Mathematics Using In-Context Meta-learning: An Evaluation of the Transferability of Findings. In International Conference on Artificial Intelligence in Education (pp. 409-417). Cham: Springer Nature Switzerland.

[9]. McNichols, H., Zhang, M., & Lan, A. (2023, June). Algebra error classification with large language models. In International Conference on Artificial Intelligence in Education (pp. 365-376). Cham: Springer Nature Switzerland.

[10]. Zhang, M., Heffernan, N., & Lan, A. (2023). Modeling and Analyzing Scorer Preferences in Short-Answer Math Questions. arXiv preprint arXiv:2306.00791.

[11]. Zhang, M., Wang, Z., Yang, Z., Feng, W., & Lan, A. (2023). Interpretable math word problem solution generation via step-by-step planning. arXiv preprint arXiv:2306.00784.

[12]. Zhang, M., Baral, S., Heffernan, N., & Lan, A. (2022). Automatic short math answer grading via in-context meta-learning. arXiv preprint arXiv:2205.15219.

[13]. Wang, Z., Zhang, M., Baraniuk, R. G., & Lan, A. S. (2021, December). Scientific formula retrieval via tree embeddings. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 1493-1503). IEEE.

[14]. Zhang, M., Wang, Z., Baraniuk, R., & Lan, A. (2021). Math operation embeddings for open-ended solution analysis and feedback. arXiv preprint arXiv:2104.12047.

[15]. Jordan, S., Chandak, Y., Cohen, D., Zhang, M., & Thomas, P. (2020, November). Evaluating the performance of reinforcement learning algorithms. In International Conference on Machine Learning (pp. 4962-4973). PMLR.

[16]. Qi, D., Arfin, J., Zhang, M., Mathew, T., Pless, R., & Juba, B. (2018, March). Anomaly explanation using metadata. In 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 1916-1924). IEEE.

[17]. Zhang, M., Mathew, T., & Juba, B. (2017, February). An improved algorithm for learning to perform exception-tolerant abduction. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 31, No. 1).