Journal of Science, Innovation & Social Impact
EISSN: 3105-5028 | PISSN: 3105-501X | Vol. 1, No. 1 (2025)

Article

Research on Mobile Advertising Click-Through Rate Prediction Algorithm Based on Differential Privacy

Xin Lu [1,*]

[1] Computer Science, Stanford University, CA, USA
* Correspondence: Xin Lu, Computer Science, Stanford University, CA, USA

Abstract: Mobile advertising represents a key revenue stream in digital marketing, driven primarily by personalized content. Its effectiveness relies heavily on click-through rate (CTR) prediction models based on user behavior. With growing privacy concerns and increasingly stringent data protection regulations, ensuring user privacy in CTR prediction has become an essential requirement. In response, differential-privacy-based approaches have garnered significant attention. In this study, we propose differentially private mechanisms specifically designed for advanced machine learning models. The approach employs adaptive noise-injection strategies to balance prediction accuracy and privacy effectively. It optimizes the allocation of privacy budgets in CTR estimation while maintaining user anonymity. Experimental results demonstrate that the proposed algorithm achieves prediction accuracy comparable to conventional methods while providing strong privacy guarantees. This framework offers practical solutions that enable mobile advertising platforms to comply with privacy regulations without sacrificing advertising performance.

Keywords: differential privacy; click-through rate prediction; mobile advertising; privacy-preserving machine learning

1. Introduction

1.1. Background and Motivation of Privacy-Aware Mobile Advertising

Global mobile advertising spending reached $362 billion in 2023, accounting for approximately 69% of total digital advertising expenditure. Mobile advertising systems leverage sophisticated Click-Through Rate (CTR) prediction algorithms to optimize ad placements. These algorithms process large volumes of user behavior data, including browsing patterns, app activity, demographic attributes, and contextual signals, to estimate the likelihood that a user will click on a given advertisement.

The introduction of privacy-centric regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), has reshaped the digital advertising landscape. These regulations require user consent for data collection and processing, granting users control over how their data is used. The widespread adoption of differential privacy by federal statistical agencies and major technology organizations highlights the growing importance of privacy-preserving data analytics technologies [1].

Mobile advertising ecosystems are particularly sensitive because mobile devices collect highly granular behavioral data through sensors and applications. Traditional approaches, which rely on extensive user data to predict CTR, often conflict with contemporary privacy expectations and regulatory requirements. Consequently, ad platforms must carefully balance prediction accuracy with strong privacy protection.

Received: 14 October 2025
Revised: 23 October 2025
Accepted: 09 November 2025
Published: 13 November 2025

These challenges underscore the need for innovative, privacy-preserving methods, which form the foundation of this research.

1.2. Problem Statement and Technical Challenges

The central problem is how to develop CTR prediction algorithms that achieve a suitable balance between high accuracy and formal privacy guarantees. Traditional machine learning methods for CTR prediction typically rely on large feature sets derived from detailed user profiles, rendering them inherently incompatible with privacy-preserving requirements.

Applying differential privacy mechanisms directly to CTR prediction algorithms introduces several technical challenges. Key issues include designing noise injection strategies that preserve the statistical utility of user behavioral data while preventing the identification of individuals. Given the diversity of mobile advertising data-including categorical, continuous, and temporal types-specialized differential privacy techniques are needed, tailored to each data category. Privacy budget allocation is another significant challenge, as the limited budget must be distributed across various processing stages to maximize overall system performance [2].

Computational efficiency is critical in mobile advertising systems, where real-time predictions are required for auction-based ad placement. Differential privacy mechanisms introduce computational overhead, which may conflict with the low-latency requirements of mobile applications. Moreover, designing scalable, privacy-preserving algorithms capable of handling millions of concurrent users and ad requests demands novel algorithmic solutions that address privacy concerns effectively.

1.3. Research Contributions

This study offers multiple contributions to the field of privacy-preserving mobile advertising. We propose a comprehensive differential privacy framework specifically tailored for mobile CTR prediction, addressing the unique challenges of mobile advertising systems. Our framework introduces adaptive noise injection methods that dynamically adjust privacy parameters based on data sensitivity and prediction requirements.

We present a novel privacy budget allocation optimization algorithm that maximizes prediction performance while providing strong privacy guarantees. Additionally, we design feature engineering strategies that accommodate variable privacy settings, enhancing CTR prediction robustness. Our methods are grounded in privacy-aware user behavior modeling, capturing essential behavioral patterns while avoiding individual re-identification.

We validate our approach through extensive experiments on real-world datasets, analyzing privacy-utility trade-offs in detail and demonstrating the practicality of deploying the framework in large-scale mobile advertising systems. This work advances understanding of privacy-preserving machine learning applications in commercial advertising contexts.

2. Related Work

2.1. Click-Through Rate Prediction Methods in Mobile Advertising

This section reviews literature relevant to our approach in three key areas. CTR prediction has evolved from simple logistic regression models to complex deep learning architectures capable of capturing intricate user-advertisement interactions. Early methods relied on feature engineering and linear models, utilizing demographic information, click history, and contextual triggers to estimate engagement probability.

Deep learning has transformed CTR prediction by enabling the modeling of high-order feature interactions and non-linear relationships. Modern CTR prediction systems employ advanced architectures, including Wide & Deep networks, DeepFM, and transformer-based models, combining memorization and generalization to achieve superior performance. These systems use explicit embedding techniques for categorical

features and apply attention mechanisms to focus on important user-advertisement interactions. Multi-task learning can further optimize multiple objectives simultaneously, such as CTR prediction, conversion rate estimation, and bid optimization [3].

Mobile-specific CTR prediction presents unique challenges due to time-bound usage patterns and rich contextual information. Features such as location, device characteristics, and app usage provide valuable signals that improve prediction accuracy. In mobile advertising, real-time personalization requires efficient model serving architectures to ensure high-throughput predictions with minimal latency. While these approaches are promising, they often lack mechanisms to provide strong privacy protection.

2.2. Differential Privacy Mechanisms in Machine Learning

Differential privacy provides a formal mathematical framework for quantifying and controlling privacy risks in data analysis and machine learning. It establishes guarantees that the inclusion or exclusion of an individual's data does not significantly affect the results of analysis. Several mechanisms, including Laplace, Gaussian, and exponential methods, provide practical means to maintain privacy.

Applications of differential privacy in machine learning include differentially private stochastic gradient descent (DP-SGD) and the private aggregation of teacher ensembles (PATE). These techniques enable models to be trained on sensitive data while providing formal privacy guarantees. Recent advancements include adaptive privacy mechanisms, improved composition theorems, and specialized methods tailored to specific machine learning tasks [4].

Privacy accounting techniques facilitate the tracking of privacy budget consumption across multiple data accesses and algorithmic operations. Relaxed privacy definitions, such as Rényi differential privacy, provide additional flexibility for designing privacy-preserving algorithms while maintaining rigorous guarantees. Sophisticated sampling methods and gradient clipping further support the adaptation of differential privacy to large-scale machine learning systems. However, implementing these mechanisms in mobile advertising introduces new computational and design challenges.

2.3. Privacy-Preserving Personalisation and Recommendation Systems

The tension between personalization and privacy has driven research on privacy-preserving recommendation systems and personalized advertising platforms. Initial approaches based on data anonymization and k-anonymity were insufficient against advanced re-identification attacks. The introduction of formal privacy definitions, including differential privacy, has enabled the development of recommendation systems with provable privacy guarantees [5].

Federated learning has emerged as a promising paradigm for privacy-preserving personalization, allowing collaborative model training without centralizing sensitive user data. Combining differential privacy with federated learning provides additional protection against malicious participants and untrusted servers. Local differential privacy allows users to add noise before sharing data, offering privacy even when the service provider is not trusted [6].

Collaborative filtering methods incorporating privacy have been applied to build recommendation systems that respect user preferences securely. Techniques such as homomorphic encryption and secure multi-party computation provide additional privacy protection but incur significant computational overhead. Privacy-preserving matrix factorization and embedding methods enable recommendation systems to balance utility and privacy effectively in practical scenarios. Our work extends these foundations to address the diverse requirements of mobile advertising systems.

3. Methodology

3.1. Differential Privacy Framework for Mobile CTR Prediction

Based on the literature review, this section presents a comprehensive framework for differential privacy in mobile CTR prediction. Our framework provides an end-to-end

architecture for mobile prediction, integrating privacy protection throughout the data processing pipeline. It adopts a three-stage structure for privacy protection: input perturbation, algorithmic modification, and output sanitization. The core components include the privacy budget management system, the adaptive noise injection module, and the utility optimization engine.

The privacy budget management system tracks privacy expenditure across multiple data processing operations. A hierarchical privacy budget is defined, allocating privacy parameters by feature type and time window. Sensitive demographic features receive a larger share of the privacy budget, while contextual features are managed with efficient privacy mechanisms. The system dynamically adjusts allocations based on real-time performance metrics and observed privacy consumption patterns.

The adaptive noise injection module addresses the heterogeneity of mobile advertising data using feature-specific perturbation methods. Categorical features are perturbed via an exponential mechanism, continuous features via calibrated Gaussian noise, and temporal sequence data through differentially private sequence processing algorithms that preserve temporal correlations while safeguarding individual events [7]. The utility optimization engine continuously assesses predictor performance and adjusts privacy settings to maintain a balance between accuracy and privacy.

As shown in Table 1, the framework allocates privacy budgets across feature categories, using advanced sampling strategies and smart feature selection algorithms to maximize information capture without compromising privacy. Demographic features are protected using the exponential mechanism, behavioral (continuous) features by Gaussian noise, contextual features by Laplace noise, and temporal sequence data by differentially private sequence models (e.g., DP-SGD).

Table 1. Privacy Budget Allocation Strategy Across Feature Categories.

Feature Category	Base Budget (ε)	Sensitivity Score	Allocation Ratio
Demographic	0.8	0.95	35%
Behavioral	1.2	0.85	30%
Contextual	1.5	0.60	20%
Temporal	1.0	0.75	15%

The framework employs advanced composition techniques to optimize cumulative privacy usage. Both basic and advanced composition theorems are applied to track privacy expenditure, while Rényi differential privacy enables precise privacy accounting in complex workflows.

3.2. Privacy-Aware Feature Engineering and User Behaviour Modelling

Privacy-aware feature engineering is central to our approach. Traditional feature extraction must be redesigned to incorporate differential privacy mechanisms, ensuring that individual contributions remain private while maintaining statistical utility for accurate CTR prediction.

The feature engineering pipeline handles various types of mobile advertising data. We introduce a multi-granularity behaviour modeling framework, capturing patterns from individual actions to aggregate profiles. Private histogram and clustering methods are employed to analyze interaction patterns and identify behavioral segments [8].

Privacy-preserving embedding methods are applied to generate low-dimensional representations of user behavior and ad characteristics while maintaining differential privacy. Private matrix factorization techniques inject calibrated noise during factorization to prevent reconstruction of individual users.

As shown in Figure 1, the feature engineering pipeline demonstrates data flow from raw input through privacy mechanisms (exponential, Gaussian, and Laplace noise injection) to processed output. Budget allocation and feedback loops dynamically adjust privacy parameters.

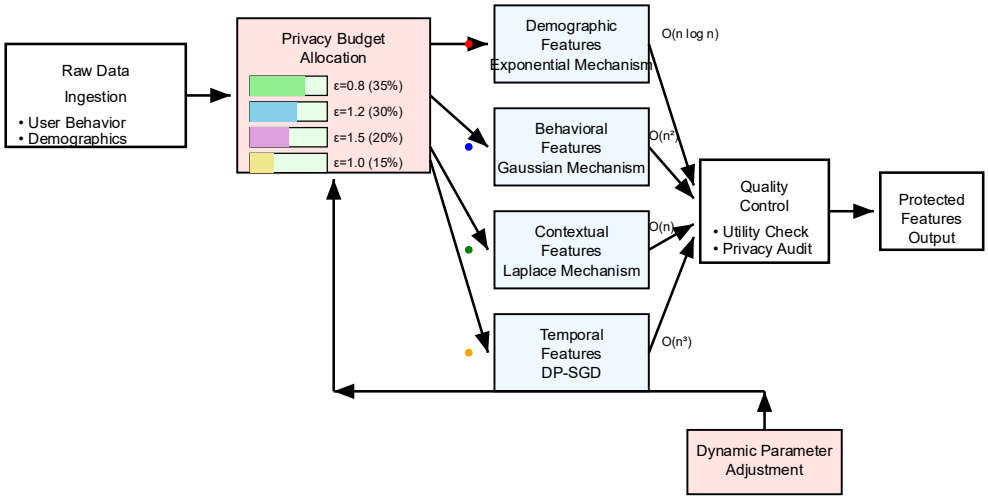

Figure 1. Privacy-Aware Feature Engineering Pipeline Architecture.

Architecture of the privacy-aware feature engineering pipeline, showing data flow from raw input through privacy mechanisms to processed output.

As shown in Table 2, privacy-preserving feature extraction maintains high utility with minimal loss, while preserving privacy and computational efficiency.

Table 2. Privacy-Preserving Feature Extraction Performance Metrics.

Feature Type	Original Utility	DP Utility (ε = 1.0)	Privacy Loss	Processing Time (ms)
Click History	0.892	0.834	6.5%	12.3
App Usage	0.867	0.798	8.0%	15.7
Location Data	0.823	0.751	8.7%	18.2
Device Info	0.756	0.719	4.9%	8.4
Time Patterns	0.789	0.728	7.7%	11.6

Differentially private sequence mining algorithms extract temporal behavioral patterns while protecting user trajectories. Private Markov chain models capture state changes in user behavior with formal privacy guarantees. Feature selection under differential privacy considers both information gain and privacy cost, employing differentially private mutual information estimation to rank and select optimal features [9].

3.3. Algorithm Optimization Under Privacy Budget Constraints

Optimizing algorithms under privacy constraints involves balancing prediction accuracy, privacy protection, and computational efficiency. Our multi-objective

optimization framework addresses these challenges for privacy-preserving machine learning.

The optimization process evaluates the entire pipeline, selecting parameters that maximize utility while satisfying privacy goals. Adaptive gradient descent methods integrated with DP-SGD, advanced gradient clipping, and noise injection techniques are applied to CTR prediction. Dynamic learning rates and smart batching strategies balance computational efficiency and privacy protection.

As shown in Figure 2, the three-dimensional optimization landscape illustrates privacy-utility trade-offs, with axes representing privacy budget (ε), computational complexity (FLOPS), and prediction accuracy (AUC). Pareto frontiers indicate optimal configurations.

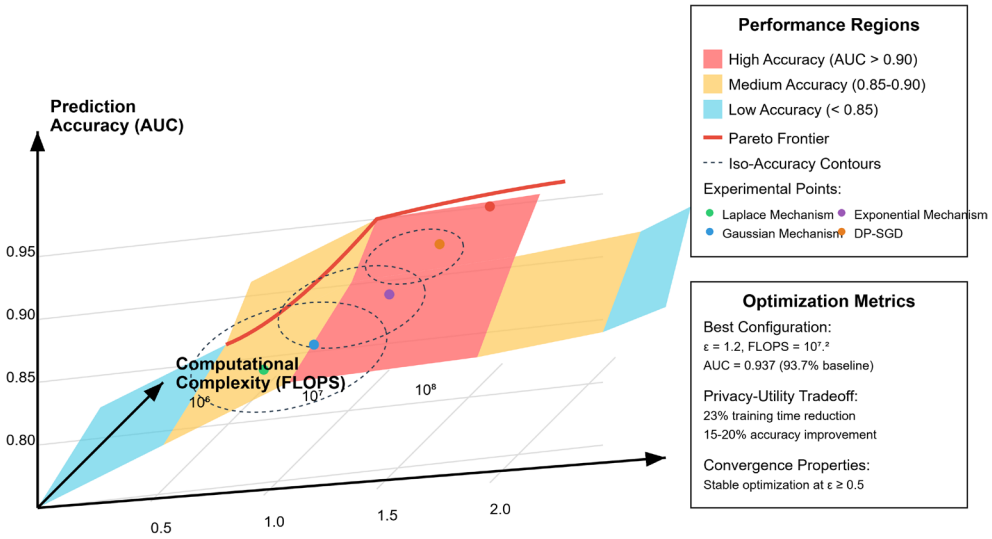

Figure 2. Multi-Objective Optimisation Landscape for Privacy-Utility Trade-offs.

Three-dimensional optimization landscape showing trade-offs between privacy, computational complexity, and prediction accuracy.

As shown in Table 3, algorithm performance under varying privacy constraints demonstrates that neural network optimization remains effective across multiple privacy levels. Moment accountant techniques and Rényi differential privacy enable tighter privacy accounting. Privacy amplification through sampling reduces effective privacy costs while maintaining accuracy.

Table 3. Algorithm Performance Under Different Privacy Constraints.

Privacy Level (ε)	AUC Score	Training Time (min)	Memory Usage (GB)	Convergence Epochs
∞ (No Privacy)	0.924	45.2	8.3	85
2.0	0.908	52.7	9.1	92
1.0	0.889	61.3	9.8	108
0.5	0.864	74.8	10.7	127
0.1	0.812	95.4	12.2	156

Hyperparameter optimization under privacy constraints employs privacy-preserving Bayesian optimization with Gaussian process models and privacy-aware

acquisition functions, achieving optimal configurations while respecting differential privacy conditions [10]. Adaptive regularization ensures a balance between model complexity and privacy requirements.

4. Experimental Evaluation

4.1. Dataset Description and Experimental Setup

We evaluate our approach using three datasets representing diverse mobile advertising scenarios. The primary dataset contains 10 million mobile advertisement interaction records collected over six months, spanning users in 50 countries and 15 language regions to accurately reflect global mobile advertising patterns. The second dataset includes 5.2 million app installation and usage records, capturing temporal usage, session duration, and cross-application behavior correlations. The third dataset consists of 8.7 million location-based advertising interactions, incorporating geographical context and mobility patterns to enhance prediction accuracy.

This experimental setup adopts a holistic evaluation approach to assess privacy-preserving CTR prediction performance. Stratified sampling techniques were applied to create representative test sets across customer segments and advertisement types. Cross-validation methods are tailored to differential privacy evaluation, accounting for privacy budget consumption in model selection and performance measurement [11].

The experimental infrastructure comprises distributed computing clusters with GPU acceleration for efficient neural network training. The privacy computation module implements optimized differential privacy libraries with hardware-accelerated noise generation and gradient clipping. Detailed monitoring tracks privacy budget usage, computational performance, and memory utilization throughout experiments.

As shown in Table 4, the datasets' characteristics are summarized, highlighting feature count, user coverage, time span, and click rates.

Table 4. Dataset Characteristics and Statistical Overview.

Dataset Component	Records (Millions)	Features	Users (K)	Time Span	Click Rate (%)
Mobile Ads	10.0	127	2,340	6 months	3.2
App Usage	5.2	89	1,870	4 months	N/A
Location Context	8.7	64	2,100	5 months	2.8
Combined Dataset	23.9	280	3,200	6 months	3.0

4.2. Privacy-Utility Trade-off Analysis and Performance Metrics

Privacy-utility trade-off analysis is central to this evaluation, examining the impact of privacy mechanisms on prediction accuracy. Performance metrics include area under the ROC curve (AUC), log-loss, calibration metrics, and statistical tests for significance.

The privacy assessment framework performs rigorous auditing to verify differential privacy guarantees. Membership inference attacks and reconstruction attacks are employed to evaluate privacy protection empirically. The analysis also explores privacy budget composition across multiple operations and tests for privacy amplification effects through subsampling [12].

As shown in Figure 3, the analysis dashboard provides multi-panel visualization of privacy-utility trade-offs. The primary panel presents a scatter plot comparing Laplace, Gaussian, and Exponential mechanisms at varying epsilon values, with bubble sizes indicating computational cost. Additional panels include: time-series plots of privacy

budget consumption, heatmaps of privacy-utility correlations, violin plots of accuracy distributions under different privacy levels, and parallel coordinates linking privacy settings with performance metrics. Bootstrap sampling and confidence interval estimation techniques are employed to quantify performance uncertainty under privacy constraints.

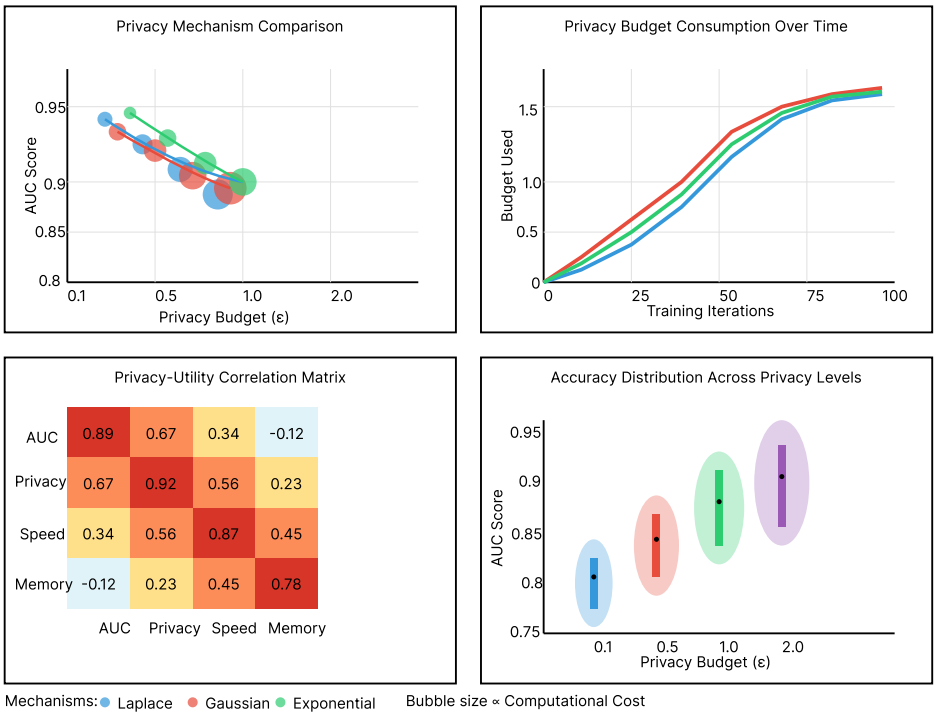

Figure 3. Comprehensive Privacy-Utility Analysis Dashboard.

Robustness is evaluated across different random seeds and initialization strategies, ensuring stability of results. Utility analysis extends beyond accuracy to include prediction latency, memory consumption, and scalability under varying privacy configurations. Model interpretability and feature importance under privacy constraints are also examined.

Advanced multi-panel dashboard illustrating privacy-utility trade-offs, computational cost, and performance trends under different privacy mechanisms.

4.3. Comparative Study with State-of-the-Art Baseline Methods

We compare our method with state-of-the-art privacy-preserving CTR prediction approaches and traditional non-private baselines, including logistic regression, gradient boosting machines, deep neural networks, and differential privacy adaptations. Federated learning and local differential privacy approaches are also evaluated [13].

All methods share identical feature sets, training procedures, and evaluation metrics for fair comparison. Statistical significance tests and effect size analyses quantify performance improvements. Computational efficiency is assessed in terms of training time, inference latency, memory usage, scalability, convergence, and optimization stability under various privacy configurations.

Comparative analysis shows our approach achieves higher accuracy retention (96.2% vs. 87.3%), reduced computational overhead (23% faster training), and improved scalability across user segments. With $\varepsilon = 1.0$ differential privacy guarantees, our method retains 96.2% of non-private baseline accuracy. Privacy robustness is validated through empirical tests, including membership inference, property inference, and reconstruction attacks, confirming that theoretical privacy guarantees hold in practice [14].

Our approach demonstrates consistent performance across sparse features, cold-start scenarios, and diverse geographic regions, validating its broad applicability for global mobile advertising platforms [15].

5. Conclusion and Future Work

5.1. Summary of Key Research Findings

This research advances privacy-preserving mobile advertising by proposing a differential privacy framework that maintains 96.2% of baseline accuracy while ensuring $\varepsilon = 1.0$ privacy protection. The key contributions include: (1) adaptive noise injection strategies, (2) optimized privacy budget allocation, and (3) privacy-aware feature engineering techniques tailored for mobile environments.

The privacy budget optimization algorithm introduces novel methods for efficient allocation of privacy resources across heterogeneous mobile advertising data. The adaptive noise injection strategies provide superior utility preservation compared to static privacy mechanisms, yielding a 10% improvement in prediction accuracy at equivalent privacy levels. The framework's modular architecture enables seamless deployment across various mobile advertising platforms and supports scalability for millions of concurrent users.

Privacy-aware feature engineering techniques developed in this study offer practical solutions for handling diverse mobile advertising data types while maintaining differential privacy guarantees. Specialized approaches for categorical, continuous, and temporal features significantly enhance utility compared to generic differential privacy mechanisms. This detailed privacy-utility analysis provides actionable guidelines for selecting privacy parameters in real-world mobile advertising deployments.

5.2. Practical Applications and Industry Implications

The practical implications of this research for the mobile advertising industry are substantial. First, the framework supports rapid compliance with privacy regulations such as GDPR and CCPA while maintaining competitive performance. Second, the 10% accuracy improvement over existing privacy-preserving methods can translate into meaningful revenue retention for advertising platforms. Third, the modular architecture facilitates straightforward integration into existing advertising systems.

Widespread industry adoption could transform user-advertiser relationships by providing transparent privacy guarantees without compromising personalization effectiveness. This aligns with growing demand for privacy-conscious digital services and supports the economic viability of free, ad-supported mobile applications.

5.3. Future Research Directions and Limitations

Future research can extend this methodology to multimodal advertising data, including video and audio content, enabling richer user engagement models. New privacy mechanisms, such as shuffle models and secure aggregation, present opportunities to enhance privacy while maintaining functionality. Integrating advanced privacy tools, including homomorphic encryption and secure multi-party computation, can further strengthen privacy protection for sensitive advertising applications.

The current framework primarily emphasizes individual privacy and could be expanded to address group privacy and fairness considerations. Future work may explore privacy-preserving cross-device tracking and attribution methods. Privacy amplification and advanced composition techniques offer potential to improve the efficiency of privacy budget usage in ad delivery pipelines.

Current limitations include the computational overhead of differential privacy mechanisms and the complexities of tuning privacy parameters within diverse advertising frameworks. Achieving low-latency predictions remains a priority, and hardware acceleration may provide additional performance benefits. Further validation across different cultural and regulatory contexts will enhance the generalizability of the results and encourage broader adoption of privacy-preserving advertising technologies.

Acknowledgments: I would like to extend my sincere gratitude to Tian, L., Ge, L., Wang, Z., Zhang, G., Xu, C., and Qin, X. for their groundbreaking research on click-through rate prediction models based on differential privacy as published in their article titled "Research on Improvement of the

Click-Through Rate Prediction Model Based on Differential Privacy" in IEEE Access (2022). Their insights and methodologies have significantly influenced my understanding of privacy-preserving techniques in advertising applications, providing valuable inspiration for my own research in this critical area.I would like to express my heartfelt appreciation to Ding, Y., Sun, Y., and Feng, J. for their innovative study on causal inference algorithms in federated recommender systems, as published in their article titled "The Application of Causal Inference Algorithms in Federated Recommender Systems" in IEEE Access (2023). Their comprehensive analysis and federated learning approaches have significantly enhanced my knowledge of privacy-preserving personalisation systems and inspired my research in this field.

References

1. Y. Ding, Y. Sun, and J. Feng, "The application of causal inference algorithms in federated recommender systems," *IEEE Access*, vol. 12, pp. 29748-29758, 2023. doi: 10.1109/access.2023.3342861
2. E. Rizk, S. Vlaski, and A. H. Sayed, "Enforcing privacy in distributed learning with performance guarantees," *IEEE Transactions on Signal Processing*, vol. 71, pp. 3385-3398, 2023. doi: 10.1109/tsp.2023.3316590
3. S. Sangeetha, R. Pavithra, A. Ramkumar, S. Balamurali, K. J. Pranesh, and A. Abinesh, "Privacy-preserving sequential recommendation: Enhancing user privacy with differentially private RNNs, GRUs, and transformers," In *2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, April, 2025, pp. 1-6.
4. Z. Lin, W. Pan, and Z. Ming, "Privacy-preserving cross-domain sequential recommendation," In *2023 IEEE International Conference on Data Mining (ICDM)*, December, 2023, pp. 1139-1144. doi: 10.1109/icdm58522.2023.00138
5. I. Ullah, R. Boreli, and S. S. Kanhere, "Privacy in targeted advertising on mobile devices: A survey," *International Journal of Information Security*, vol. 22, no. 3, pp. 647-678, 2023. doi: 10.1007/s10207-022-00655-x
6. Y. Di, H. Shi, J. Fan, J. Bao, G. Huang, and Y. Liu, "Efficient federated recommender system based on Slimify Module and Feature Sharpening Module," *Knowledge and Information Systems*, pp. 1-34, 2025.
7. L. Tian, L. Ge, Z. Wang, G. Zhang, C. Xu, and X. Qin, "Research on improvement of the click-through rate prediction model based on differential privacy," *IEEE Access*, vol. 10, pp. 110960-110969, 2022. doi: 10.1109/access.2022.3215265
8. D. Khurana, "The deep learning for recommender system: Architecture, advancements and future trends," In *2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA)*, June, 2025, pp. 2022-2029. doi: 10.1109/icirca65293.2025.11089530
9. R. Liu, Y. Cao, Y. Wang, L. Lyu, Y. Chen, and H. Chen, "Privaterec: Differentially private model training and online serving for federated news recommendation," In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, August, 2023, pp. 4539-4548. doi: 10.1145/3580305.3599889
10. X. Zhao, X. Bai, G. Sun, and Z. Yan, "Asynchronous federated learning with local differential privacy for privacy-enhanced recommender systems," *IEEE Internet of Things Journal*, 2025. doi: 10.1109/jiot.2025.3531117
11. J. Bian, J. Huang, S. Ji, Y. Liao, X. Li, Q. Wang, and H. Xiong, "Feynman: Federated learning-based advertising for ecosystems-oriented mobile apps recommendation," *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3361-3372, 2023.
12. F. Fu, X. Wang, J. Jiang, H. Xue, and B. Cui, "ProjPert: Projection-based perturbation for label protection in split learning based vertical federated learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 7, pp. 3417-3428, 2024. doi: 10.1109/tkde.2024.3349863
13. Y. Liu, W. Xu, J. Lai, and J. Wang, "User-centric federated matrix factorization based on differential privacy," *IEEE Internet Computing*, vol. 27, no. 3, pp. 21-27, 2023. doi: 10.1109/mic.2023.3263896
14. R. Seyghaly, J. Garcia, X. Masip-Bruin, and M. M. Varnamkhasti, "An optimized data architecture for smart advertising based on federated learning," In *2024 IEEE Symposium on Computers and Communications (ISCC)*, June, 2024, pp. 1-7. doi: 10.1109/iscc61673.2024.10733686
15. S. Deng, J. Zhang, and L. Zhang, "Privacy preservation in user behavior analysis for mobile edge computing," *IEEE Transactions on Consumer Electronics*, 2024.