ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 2 Issue 4, December 2022 / Page No: 161-162
Paper Id: JETA-V2I4P124 / Doi: 10.56472/25832646/JETA-V2I4P124

Original Article

The Use of Federated Learning for Digital Advertising Measurement

Varun Chivukula
Independent Researcher, USA.

Abstract: *Federated learning (FL) allows collaborative model training across decentralized devices or datasets without the need for raw data sharing, preserving user privacy. This paper explores FL's application in randomized control trial (RCT) measurement for digital advertising and other domains, emphasizing privacy-preserving techniques. We present a theoretical framework, demonstrate its implementation, and analyze its advantages, limitations, and recommendations.*

Keywords: *Federated Learning, Randomized Control Trials, Privacy Enhancing Technologies, Digital Advertising.*

I. INTRODUCTION

Randomized control trials (RCTs) are foundational to causal inference, used extensively in advertising to measure the effectiveness of campaigns. Traditional RCT implementations require centralized data collection, which often involves handling personally identifiable information (PII). This raises compliance and privacy challenges under regulations such as GDPR and CCPA.

Federated learning (FL) offers a solution by enabling decentralized analysis where raw data remains local. This work demonstrates the feasibility of using FL to measure RCTs while preserving privacy, ensuring accurate estimation of treatment effects without sharing PII.

II. FEDERATED LEARNING FOR RCT MEASUREMENT

A. Fundamentals of Federated Learning

In federated learning, devices collaboratively train a global model while keeping local data private. Each device computes model updates based on its local data and sends these updates (e.g., gradients or summary statistics) to a central server for aggregation.

B. RCT Overview

In an RCT, participants are randomly assigned to treatment ($T = 1$) or control ($T = 0$) groups. Key metrics include:

- Conversion rate (CR): Proportion of users converting in each group.
- Average treatment effect (ATE): The difference in outcomes between treatment and control groups.

Let:

- Yi: Observed outcome for user i.
- Ti : Treatment assignment (1 for treatment, 0 for control).

The average treatment effect is expressed as:

$$ATE = E[Yi \mid Ti = 1] - E[Yi \mid Ti = 0].$$

C. Secure Aggregation in FL for RCTs

Federated learning can compute $E[Yi \mid Ti]$ values locally for each group, with devices sending encrypted aggregated statistics to the central server. Privacy is enhanced using differential privacy, adding noise to ensure no individual user's contribution is identifiable.

III. METHODOLOGY

A. Experiment Design

An RCT simulation was conducted with 100,000 users, divided equally into treatment and control groups. Metrics evaluated included:

- Conversion rate (CR).
- Lift (L), calculated as:

$$L = \{CRtreatment - CRcontrol\}/\{CRcontrol\} \times 100$$

B. Federated RCT Workflow

- Local Model Updates: Each device computes local statistics (E[Yi | Ti] and encrypts them.
- Secure Aggregation: Aggregated statistics are combined centrally without exposing individual data.
- Global Metric Computation: Metrics like CR, ATE, and L are computed at the server level.

C. Comparison with Centralized RCTs

Performance of FL-based RCTs was compared against traditional centralized RCTs on accuracy, privacy, and computational efficiency.

IV. RESULTS

A. Metrics Comparison

Metric	Centralized Approach	Federated Learning Approach
Conversion Rate (Treatment)	15.2%	15.1%
Conversion Rate (Control)	12.0%	11.9%
Lift (LLL)	26.7%	26.9%

B. Privacy Impact

Federated learning ensured no raw data or PII left user devices. Differential privacy added calibrated noise to aggregated metrics, maintaining compliance with GDPR and CCPA while preserving measurement accuracy.

C. Computational Efficiency

While FL required additional communication and computation compared to centralized approaches, lightweight models ensured manageable overhead.

V. DISCUSSION

A. Benefits

- Privacy Preservation: No PII is transmitted, addressing compliance with privacy regulations.
- Real-Time Analysis: Metrics are computed without centralizing data, enabling faster insights.
- Scalability: FL scales effectively to large user bases and datasets.

B. Challenges

- Noise Impact: Differential privacy introduces trade-offs between privacy and accuracy.
- Infrastructure Requirements: Requires robust communication and computation capabilities.
- Model Complexity: Advanced models increase local computation demands.

VI. RECOMMENDATIONS

- Model Simplification: Use lightweight algorithms like logistic regression for initial implementations.
- Balanced Privacy Settings: Fine-tune noise parameters in differential privacy to maintain accuracy.
- Cross-Platform Collaboration: Develop standardized FL frameworks for widespread adoption in RCTs.

VII. CONCLUSION

Federated learning represents a promising paradigm for conducting privacy-preserving RCTs in digital advertising and other fields. By eliminating the need for raw data exchange, FL addresses regulatory challenges while maintaining measurement accuracy. Further research on improving model efficiency and privacy trade-offs will enable broader adoption.

VIII. REFERENCES

[1] McMahan, H. B., Ramage, D., et al. (2017). "Communication-Efficient Learning of Deep Networks from Decentralized Data." *Proceedings of AISTATS*.

[2] Dwork, C., & Roth, A. (2014). "The Algorithmic Foundations of Differential Privacy." *Foundations and Trends in Theoretical Computer Science*.

[3] Hard, A., Rao, K., et al. (2018). "Federated Learning for Mobile Keyboard Prediction." *arXiv:1811.03604*.

[4] Bonawitz, K., et al. (2019). "Practical Secure Aggregation for Privacy-Preserving Machine Learning." *ACM CCS*.

[5] Pearl, J. (2009). "Causality: Models, Reasoning, and Inference." Cambridge University Press.