IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁑ Peer-reviewed & Refereed journal ⁑ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11759

Privacy-Preserving Monitoring And Classification Of On-Screen Activities In E-Learning Using Federated Learning

Raghavendra O[1], Seema Nagaraj[2]

Student, Department of MCA, Bangalore Institute Of Technology, Karnataka, India[1]

Professor, Department of MCA, Bangalore Institute Of Technology, Karnataka, India[2]

Abstract: In e-learning, tracking and classification of on-screen endeavors are fundamental for identifying learner engagement and optimizing content delivery. However, traditional methods often compromise user privacy by centralizing sensitive data. In classify to improve privacy preservation, this research suggests a novel method for tracking and classifying on-screen activities using Federated Learning (FL). Our method allows data to remain decentralized on users' devices while leveraging aggregated models for analysis. We evaluate the performance of the FL-based system against traditional centralized methods, highlighting improvements in both privacy and accuracy.

I. INTRODUCTION

E-learning platforms have revolutionized education by providing flexible, scalable, and accessible learning experiences. Effective tracking and classification of on-screen activities, such as mouse movements, clicks, and time spent on tasks, are vital for assessing learner engagement and tailoring educational content. However, traditional centralized methods of tracking often pose significant privacy risks by requiring the transmission of sensitive data to a central server.

Federated Learning (FL) offers a promising solution by enabling machine learning models to be guided across decentralized data sources while keeping data local. This paper explores the integration of FL for privacy-preserving tracking and classification of on-screen activities in e-learning environments. We discuss the design, implementation, and evaluation of our FL-based system, relating its performing with regular methods in words of privacy protection and classification accuracy.

II. BACKGROUND AND RELATED WORK

2.1 E-Learning Analytics

E-learning analytics involves collecting and analyzing data on learners' interactions with educational content. Traditional methods often involve centralizing data on server-side applications for analysis. But, this draw near raises alarms about data privacy, particularly in light of the growing attention surrounding data privacy laws like GDPR.

2.2 Federated Learning

Federated Realizing is a decentralized approach to machine knowledge wherever demonstrates are cooperatively trained on several devices containing local data. Bringing the code to the information instead of the data to the code is the fundamental notion. FL aggregates locally trained models into a global model without transferring raw data, thus preserving privacy.

2.3 Privacy in E-Learning

Previous research dealt with a number of privacy-related issues in e-learning, such as learners confidentiality and confidentiality. But these approaches frequently fail of providing comprehensive privacy solutions, as they either degrade data utility or fail to fully anonymize data.

III. METHODOLOGY

3.1 Federated Learning Framework

Our proposed system utilizes a Federated Learning framework to track and classify on-screen activities while preserving user privacy. The framework comprises a global server and multiple client devices (learners' devices) that collaboratively train a model.

DOI: 10.17148/IARJSET.2024.11759

3.2 Data Collection and Processing

Local data on each client device includes on-screen activities such as click patterns, mouse movements, and time spent on tasks. This data is processed locally to extract relevant features for training the model. Feature extraction methods include:

- **Temporal Analysis**: Tracking the duration of interactions.
- **Spatial Analysis**: Mapping the locations of mouse clicks and movements.
- **Contextual Analysis**: Understanding the context of interactions based on screen content.

3.3 Model Training

Each client device files a local representation using its retain data. Using methods like Federated Averaging, the global server periodically aggregates these local models (FedAvg), creating a unified global model without accessing the raw data.

3.4 Privacy Mechanisms

To ensure privacy, we implement several mechanisms:

- **Differential Privacy**: Adding noise to the model updates to prevent data leakage.
- **Secure Aggregation**: Encrypting model updates during transmission to the server.
- **Local Data Anonymization**: Anonymizing data on client devices before feature extraction.

IV. EVALUATION

4.1 Experimental Setup

We evaluated our system using a dataset of simulated on-screen activities in an e-learning environment. The dataset included various interaction patterns representing different levels of learner engagement.

4.2 Performance Metrics

We assessed the system's performance using the following metrics:

- **Classification Accuracy**: The talent of the model to correctly classify on-screen activities.
- **Privacy Preservation**: The usefulness of privacy mechanisms in preventing data leakage.
- **Computational Efficiency**: The time and resources required for local training and global aggregation.

4.3 Results

Our outcome exhibit that the FL-based system achieves comparable, if not superior, classification accuracy to traditional centralized methods. Importantly, it provides significant improvements in privacy preservation, as evidenced by reduced data leakage and enhanced user anonymity.

V. DISCUSSION

5.1 Implications for E-Learning

The assumption of FL for on-screen activity tracking and classification addresses critical privacy concerns in e-learning. It empowers learners by saving management over their data while enabling educators to derive actionable insights from aggregated models.

5.2 Limitations and Future Work

While our approach enhances privacy, it introduces challenges such as increased computational overhead on client devices and potential model drift due to non-IID data distributions. The goal of future research will be to maximize model training efficiency. and addressing data heterogeneity.

VI. CONCLUSION

This paper presents a privacy-preserving approach to on-screen activity tracking and classification in e-learning using Federated Learning. Our method effectively balances the need for detailed learner analytics with the imperative to protect user privacy.

By keeping data decentralized and aggregating models, we offer a robust solution that can be widely adopted in privacy-sensitive educational settings.

DOI: 10.17148/IARJSET.2024.11759

REFERENCES

[1]. McMahan, B., et al. (2017). *Communication-Efficient Learning of Deep Networks from Decentralized Data*. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 54, 1273-1282.

[2]. Kairouz, P., et al. (2019). *Advances and Open Problems in Federated Learning*. arXiv preprint arXiv:1912.04977.

[3]. Zhang, Z., et al. (2020). *Federated Learning for Privacy-Preserving Interactive Advertising*. Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2492-2500.

[4]. Dwork, C., & Roth, A. (2014). *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends® in Theoretical Computer Science, 9(3-4), 211-407.

[5]. Konečný, J., et al. (2016). *Federated Learning: Strategies for Improving Communication Efficiency*. arXiv preprint arXiv:1610.05492.