IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, April 2025
Impact Factor: 7.67

Enhancing Privacy and Efficiency in Ride-Matching Systems through Federated Learning

Wendy Nicola Tomusoni, Tashinga Bwanali, Wagner Marques, Aditya Dayal Tyagi
Department of Computer Science and Engineering
School of Engineering and Technology, Sharda University, Greater Noida, India
2022808783.wendy@ug.sharda.ac.in, 2022809445.tashinga@ug.sharda.ac.in, 2022811805.wagner@ug.sharda.ac.in
adityadayaltyagi@gmail.com

Abstract: *Ride-matching companies gather user data in real-time about their locations and preferred travel routes, as well as their previously taken rides. However, this type of data centralization presents significant privacy concerns. Cyber criminals can target such centralized databases, which would then expose users to data leaks as well as misuse of confidential information. A possible solution to the aforementioned problem is provided by federated learning, which decentralizes the learning process by keeping user data on their devices and only sending updates to the model. While making it more difficult for unauthorized individuals to access personal data, federated learning still provides high quality services for ride matching. Our work demonstrates that privacy preserving methods like secure aggregation and differential privacy provide data protection alongside efficient performance. Secure aggregation collects updates from multiple users prior to transmission to hide the identity of individual users, while differential privacy obfuscates the identity of the user by adding noise, making them much harder to extract. Both methods allow for the construction of federated learning systems that are privacy aware and do not use traditional methods of machine learning. Though, certain challenges still exist such as disparity in data, communication costs, and the variety in devices. While federated learning makes use of out-of-the-box computer systems, the varying capacity of the hardware and the quality of the networks may affect the learning process. To solve these problems, the model and communication design optimization has to be done for effective operation. Even with these restrictions set, in comparison to other methods, federated learning is superior considering the fact that it protects privacy greatly, improves the intelligence of the system, and provides a friendly user experience. Doing so reduces the chances of privacy infringement which builds trust in ride-sharing apps, making them easier to use and safer*

Keywords: Federated Learning, Ride-Matching, Privacy, Decentralized AI, Secure Data Processing

DOI: 10.48175/IJARSCT-24956