ABSTRACT

This study evaluates the application of federated XGBoost for detecting risky addresses in Ethereum blockchain transactions within a multi exchange simulation scenario. The study uses centralized learning as a baseline to assess the extent to which the federated approach can maintain model utility under distributed data conditions without sharing raw data. Experiments were conducted using horizontal partitioning based on the Independent and Identically Distributed (IID) assumption, which posits that the data distribution across each exchange entity is uniform and independent, ensuring no differences in data characteristics between partitions. The evaluation covers model utility metrics including PR-AUC, precision, recall, and F1-score as well as operational implications such as runtime and communication costs. The results show that federated XGBoost is able to maintain highly competitive performance compared to the centralized baseline, with a PR-AUC of 0.9962 versus 0.9975 and an accuracy of 97.11% versus 97.75%, indicating minimal performance degradation in a homogeneous distribution scenario. Convergence analysis indicates that the federated model achieves stability within a relatively limited number of rounds and maintains a feature representation pattern consistent with the centralized model. However, this performance comes at the cost of increased end to end runtime and communication overhead, which are dominant factors in system efficiency. These findings confirm the existence of a trade off between model performance and operational efficiency in federated learning, where distributed approaches can approach the optimal performance of centralized systems but are sensitive to communication costs and network conditions. This research contributes as an initial empirical baseline in the study of federated AML on blockchain data, emphasizing that evaluations of federated learning should not only focus on accuracy but also on operational feasibility within a federated learning environment.

ABSTRAK

Penelitian ini mengevaluasi penerapan *federated* XGBoost untuk deteksi alamat berisiko pada transaksi *blockchain* Ethereum dalam skenario *simulasi multi exchange*. Penelitian ini menggunakan *centralized learning* sebagai *baseline* untuk menilai sejauh mana pendekatan *federated* mampu mempertahankan utilitas model pada kondisi data terdistribusi tanpa berbagi data mentah. Eksperimen dilakukan melalui partisi horizontal berbasis *Independent and Identically Distributed* (IID), yaitu asumsi bahwa distribusi data pada setiap *exchange* bersifat seragam dan independen. Evaluasi mencakup metrik utilitas model berupa PR-AUC, *precision*, *recall*, F1-score, dan *accuracy*, serta aspek operasional berupa *runtime* dan *communication cost*. Hasil penelitian menunjukkan bahwa *federated XGBoost* mampu mempertahankan performa yang kompetitif terhadap *centralized baseline*, dengan PR-AUC sebesar 0,9962 dibandingkan 0,9975 dan akurasi sebesar 97,11% dibandingkan 97,75%. Hasil tersebut menunjukkan adanya degradasi utilitas yang relatif kecil pada skenario distribusi homogen. Analisis konvergensi menunjukkan bahwa model *federated* mencapai performa terbaik pada *round* ke-4 dan cenderung stabil pada *round* berikutnya, meskipun hasil akhir pada *test set* mengalami penurunan dibandingkan performa validasi. Temuan ini mengindikasikan adanya *trade off* antara utilitas model dan efisiensi operasional, karena performa yang mendekati *centralized learning* diperoleh dengan konsekuensi tambahan berupa peningkatan *end to end runtime* dan *communication overhead*. Keterbatasan penelitian ini terletak pada penggunaan skenario simulasi IID dan belum mencakup kondisi non IID, jumlah *client* yang lebih besar, maupun integrasi langsung pada sistem *exchange* nyata. Penelitian selanjutnya disarankan untuk mengevaluasi *federated* XGBoost pada skenario non IID, menguji skala federasi yang lebih luas, serta menerapkan optimasi komunikasi dan mekanisme *privacypreserving* tambahan.