QFLAT: Quantum Federated Learning with Adaptive Trust for Secure and Efficient IoV Networks: An Innovative Approach

Ahmed Alruwaili and Sardar M. N. Islam (**Naz***)*
ISILC, Victoria University**,** Melbourne, Australia.

Emails: Ahmed.Alruwaili@live.vu.edu.au and Sardar.Islam@vu.edu.au

Context: This study demonstrates the profound impact of quantum technologies and computing in addressing real-world challenges by applying a quantum machine learning approach to develop safer and more efficient transportation systems. The Internet of Vehicles (IoV) is revolutionising transportation through its unique characteristics, such as vehicle-to-vehicle and vehicle-to-infrastructure communication, but these networks face significant challenges in data security, real-time decision-making, and efficient model training. **Limitation and Challenge:** While Federated Learning (FL) provides a privacy-preserving solution for decentralised model training, classical FL implementations struggle with scalability, latency, and vulnerability to adversarial attacks. **Objective and Methodology:** This research introduces a novel Quantum Federated Learning (QFL) framework that harnesses the power of quantum computing to enhance both the efficiency and security of FL in IoV networks**.** Our approach integrates two key innovations: an adaptive trust management system (TMS) that dynamically adjusts trust thresholds based on the average trust scores of participating vehicles, and a Quantum Support Vector Classifier (QSVC) that categorises vehicles as trusted or untrusted based on their computed trust scores. The QSVC leverages quantum algorithms to potentially achieve improved performance over classical methods, enhancing the system's real-time decision-making capabilities in IoV networks. **Experimental Work and Results:** We evaluated our QFL framework using the MNIST dataset, augmented with injected noise to simulate various attack scenarios in IoV networks. Our experiments demonstrate that QFL significantly outperforms classical FL in critical areas. The QSVC classification results show improved accuracy in identifying trusted and untrusted vehicles, enhancing network security. Analysis of vehicle trust scores with the adaptive threshold reveals a more dynamic and responsive trust management system, adapting effectively to changing network conditions. Furthermore, we observed a marked improvement in the system's robustness against adversarial attacks, with QFL maintaining higher accuracy levels compared to classical FL under various attack scenarios. These outcomes collectively contribute to accelerated training speed, reduced latency in model updates, and enhanced overall security and reliability of the federated learning process in IoV contexts. **Conclusion and Future Research:** This innovative research offers a more secure, efficient, and scalable approach to distributed learning in vehicular networks, paving the way for future advancements in IoV technology. Further research can explore the benefits of adopting more advanced quantum machine learning algorithms based on formal modelling of the IoV system using game theory models and algorithms.

Keywords: Quantum Federated Learning, Internet of Vehicles, Trust Management, Quantum Support Vector Classifier, Adversarial Robustness