Quantum Computing Empowered Federated Learning Framework with Deep Reinforcement Learning for IoT Security and Privacy

Saleh Alaraimi
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Alzahra Al Ajmi
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Isra Al-Ghafri
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Nouf Al Lawati
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Asma Al Balushi
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Rahaf Al-Gharabi
Electrical and Commuincation Engineering department National University for Science and Technology, College of Engineering
Muscat Oman

Abstract

The proposed system shows a federated learning architecture powered by quantum computing that uses deep reinforcement based learning as part of their IoT data security upgrade and subsequent privacy improvement. The framework is based on includes advanced quantum computation to speed up complex tasks while at the same time keeping information handling on a decentralized way among the several types of IoT devices. With the support of federated type learning, the system guarantees data confidentiality and also reduceds the privacy risks that may arise from centralized data repositories. The designed of deep reinforcement learning in the model allows that it can change the direction of the threat landscape quickly and its response ability and decision making are in real time are among the advantages. The objective of this research work is the synthesis of federated learning with quantum processing which is the main cause for scalability and adaptable in IoT environments, secure work. Their integrated approach, thus, goes a step further in not only enabling efficient distributed training phase over node and also ensuring privacy protection but also dealing with the issues that arise in current interconnected ecosystems.

Keywords

Quantum computing, federated learning, deep reinforcement, IoT data security, privacy preservation, decentralized architecture, adaptable framework, secure communication, quantum-improved processing, smart IoT systems.