Federated Learning on the Edge: A scalable and efficient platform using Kubernetes and Docker for smart distributed systems

Mir Hassan, Kasim Sinan Yildirim, and Giovanni Iacca
└Department of Information Engineering and Computer Science
University of Trento, Trento Italy

Abstract

Edge Computing platforms have become increasingly important for enabling smart distributed systems, such as smart cities or buildings and intelligent transportation systems. As a decentralized machine learning approach, Federated learning is a promising solution for training models on edge devices while preserving data privacy. We propose an edge computing platform for federated learning based on Kubernetes and Docker, enabling efficient communication and computation optimization among edge devices. Our proposed platform includes a privacy-preserving mechanism to protect sensitive data during training. We will evaluate the performance of our proposed platform through experiments on a real-world dataset and compare it with existing solutions.

1. Motivations, state of the Art

Major problems with edge devices are the security and privacy of the data, ensuring the integrity and consistency of the models, and handling device failures and network disruptions.

Existing Approaches and Tools

- **TensorFlow Federated** framework enables easy and scalable deployment of federated learning algorithms on edge devices.
- **EdgeX Foundry** platform enables developers to deploy and manage IoT applications and IoT devices. EdgeX provides a containerized architecture.
- **Kubernetes-based federated learning** framework leverages the features of Kubernetes, such as horizontal scaling and fault tolerance, to enable efficient training of ML models on distributed systems.

2. Impact

Federated learning on edge platforms with Kubernetes and Docker can have a significant impact on the field of distributed ML by improving scalability, reducing latency and bandwidth consumption, and improving data privacy and security. The proposed platform can make it easier and more accessible for developers to build and deploy distributed ML applications, leading to the development of new applications and services that were previously not possible.

3. Proposed method

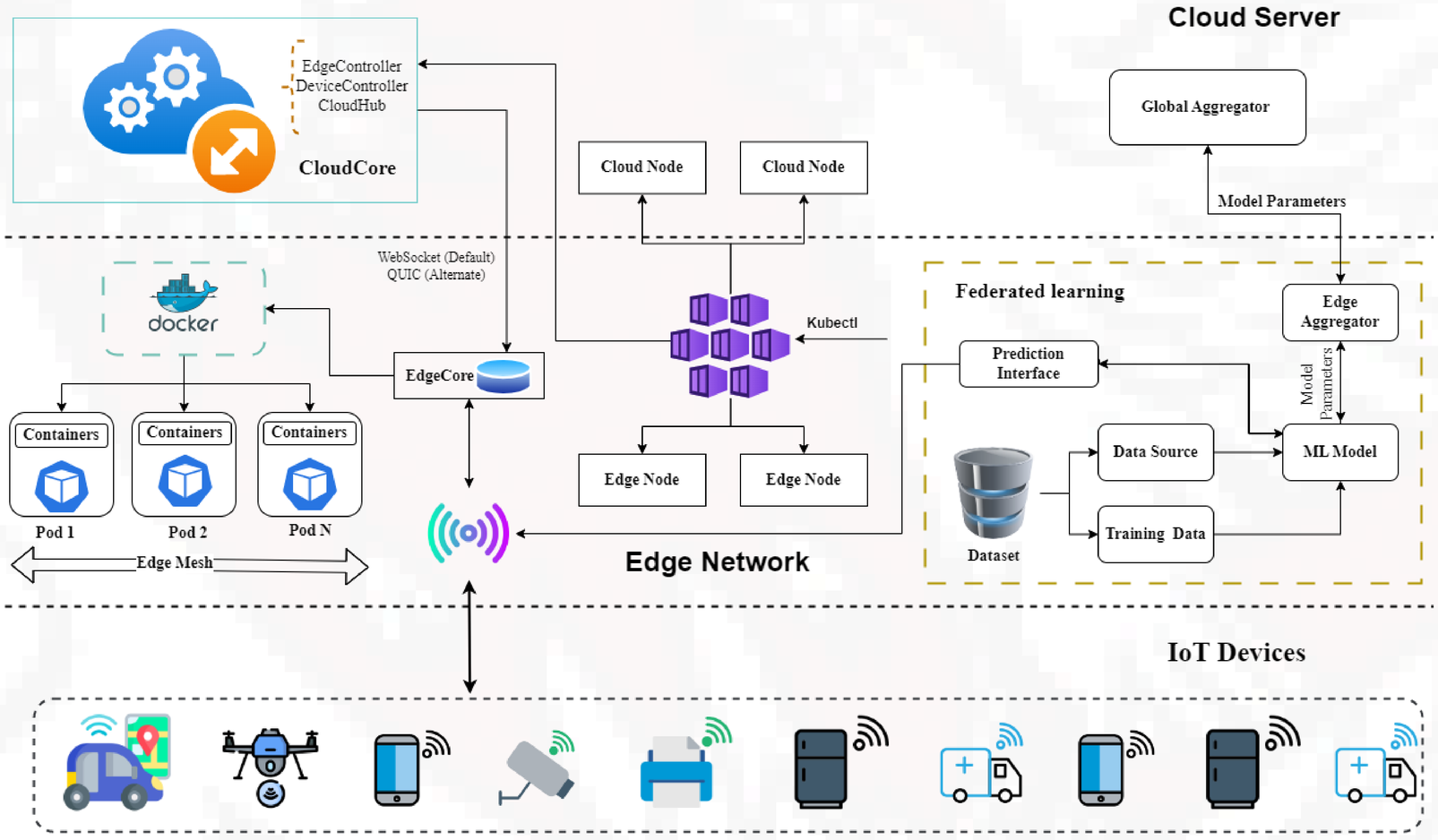

Figure 1: A proposed conceptual architecture

- **Edge computing infrastructure**: This step involves setting up a set of edge computing resources and connectivity to the Internet or a central cloud service.
- **Install and configure Kubernetes and Docker:** This step involves setting up a Docker registry to store and distribute container images encapsulating and running the federated learning algorithms.
- **Develop federated learning algorithms:** This step involves designing and developing models that can train on distributed datasets and produce a global model that represents the collective knowledge of the nodes.
- **Implement data management and security protocols:** To ensure the privacy and security of data used in federated learning, this step includes encryption, user authentication, access control, and privacy-preserving techniques.

4. Case Study

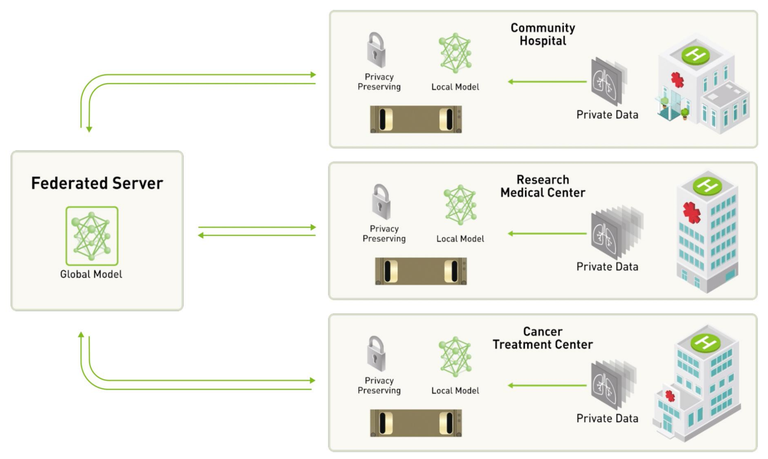

Figure 2: A hospital case study

Figure 3: Edge Computing Challenges

5. Conclusion

An Edge computing platform for federated learning based on Kubernetes and Docker can significantly impact the field of distributed ML by improving scalability, reducing latency and bandwidth consumption, and improving data privacy and security.

Corresponding author:
Mir Hassan
mir.hassan@unitn.it

ICT Days 2023
April 18, Trento, Italy