Blogs of The AI Edge: Federated ML application at edge

https://www.lfedge.org/2021/10/21/akraino-r5-spotlight-on-the-ai-edge-federated-machine-learning-at-the-edge/

Enzo Zhang zifan wu haihui wang Ryan Anderson

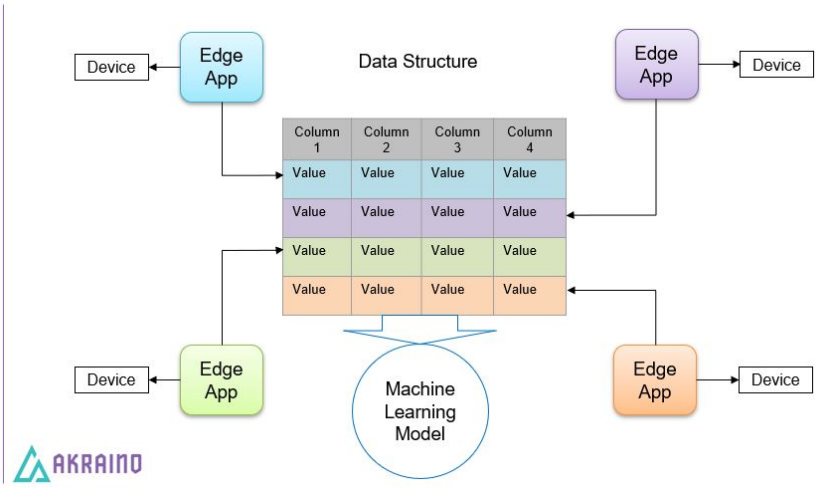
By: Enzo Zhang Zifan Wu Haihui Wang, and Ryan Anderson

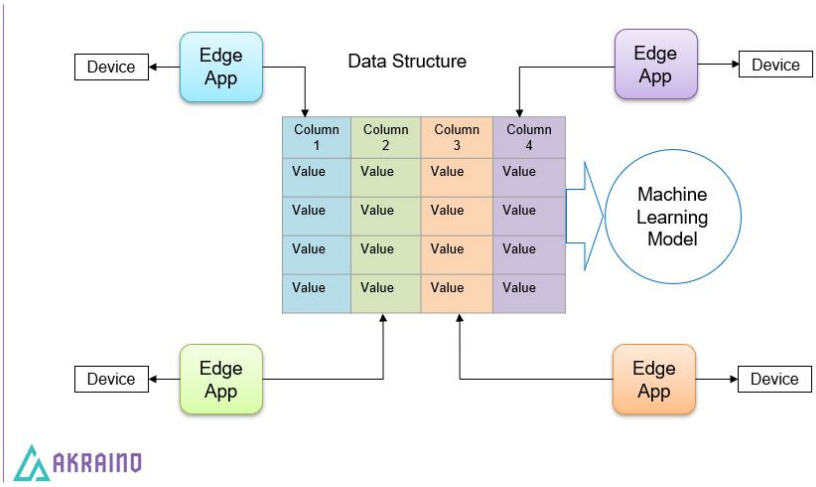
All attributes of each row data for Federated Machine Learning (ML) come from more than one edge provider. Each side has no ability on its own to hold all of the required data to function as designed. Specific edges (or edge sides) can be pretty limited in terms of edge computing capabilities for a variety of reasons/conditions

The application *must cover more than one edge* while also c*ollecting and exchanging data between edges*. Meanwhile, a method must be applied to make sure the communication between these edges is secure enough for all participants.

Here are some examples of AI edge application use cases to illustrate:

- Deploy more than one edge
- No more extra storage space
- A few computing units
- Deal with data locally
- Network ability
- Share data each other
- Work together with ML
- Data security





Applications group data from edges based on security methods; but data privacy is still managed by the Federated Machine Learning framework. Data, as an input of a ML model, is in a central site, and exchange of data occurs after ML processes are done. Required data gets sent back to the edge for its next process.

Many key components are required to make the case work well and machine learning run successfully:.

1. Data transfer and group
2. Data collect and distribute
3. Federated Machine Learning framework
4. Security encryption algorithm

This functionality, integrated with the framework, can enable edge applications to run right correctly and securely.