Literature Analysis: What is Federated Learning?

Khoa Dang Nguyen

Table of Contents

1. Introduction

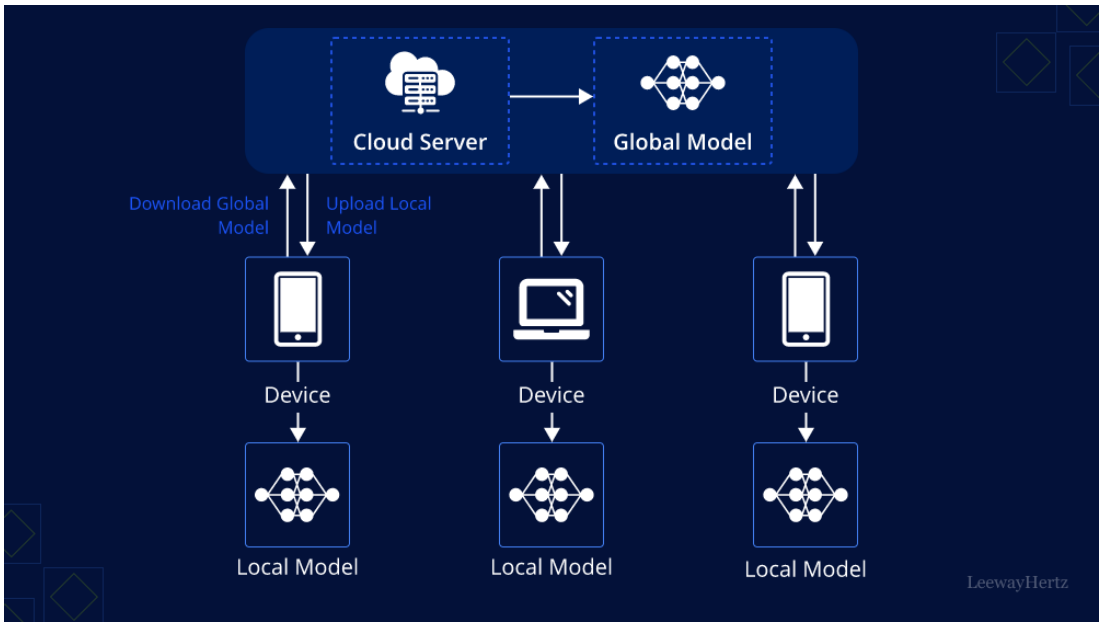
In this literature analysis, I aim to explore and explain the concept of Federated Learning (FL), an emerging technology in the field of artificial intelligence and machine learning. As a student involved in the Art-IE project, I wanted to understand this topic better, not just from a technical angle but also from a real-world perspective. The goal of this analysis is to present Federated Learning in a way that is easy to understand, while still being accurate and useful for professionals, students, and companies who are new to this area.

I used various sources, including project presentations, research papers, and real-world case studies, to build a clear picture of what Federated Learning is, why we need it, how it works, and where it is being applied. This document reflects my personal learning journey and how I see the potential of Federated Learning in improving data privacy, collaboration, and innovation.

2. Understanding Federated Learning

Federated Learning is a type of machine learning where multiple computers or devices work together to train a model. The unique thing is that the data does not get shared or moved to a central location. Instead, the learning happens locally on each device, and only the results (like updated model parameters) are shared. This is different from traditional machine learning, where all data must be collected and stored in one place before training can happen.

The idea behind Federated Learning is to respect data privacy. It allows people or organizations to benefit from shared machine learning without having to give away their private or sensitive information. For example, a hospital can help train a medical AI model without sending its patient records to another hospital or a cloud server.

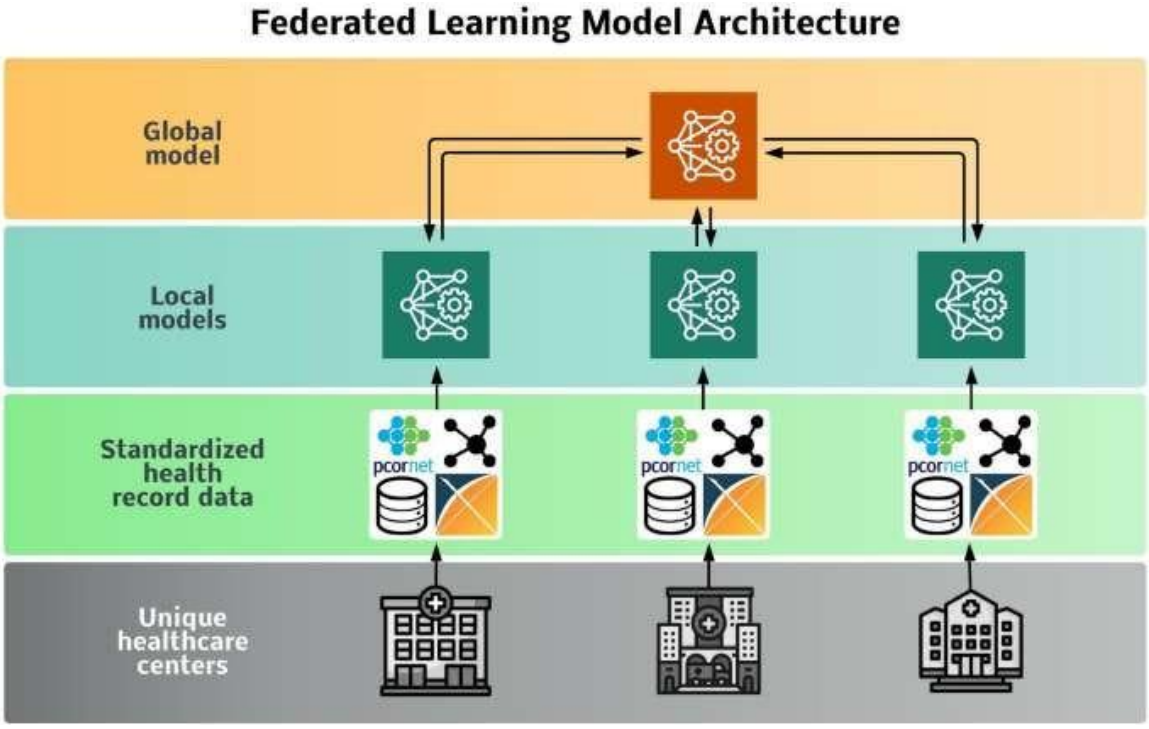


3. The Need for Federated Learning

There are many reasons why Federated Learning is becoming more important. First, data privacy laws like GDPR make it harder for organizations to move data around. Many companies have sensitive customer or patient data that they cannot legally share. Federated Learning solves this by keeping data on the device.

Second, in the real world, data is often spread out across different locations. For example, each smartphone has different user data. Collecting it all in one place would take a lot of time and computing power. Federated Learning lets each phone train a part of the model and send only what is needed.

Third, companies want to work together without losing control of their data. Federated Learning makes this possible. It helps build trust among different parties while still making it possible to develop powerful machine learning tools.



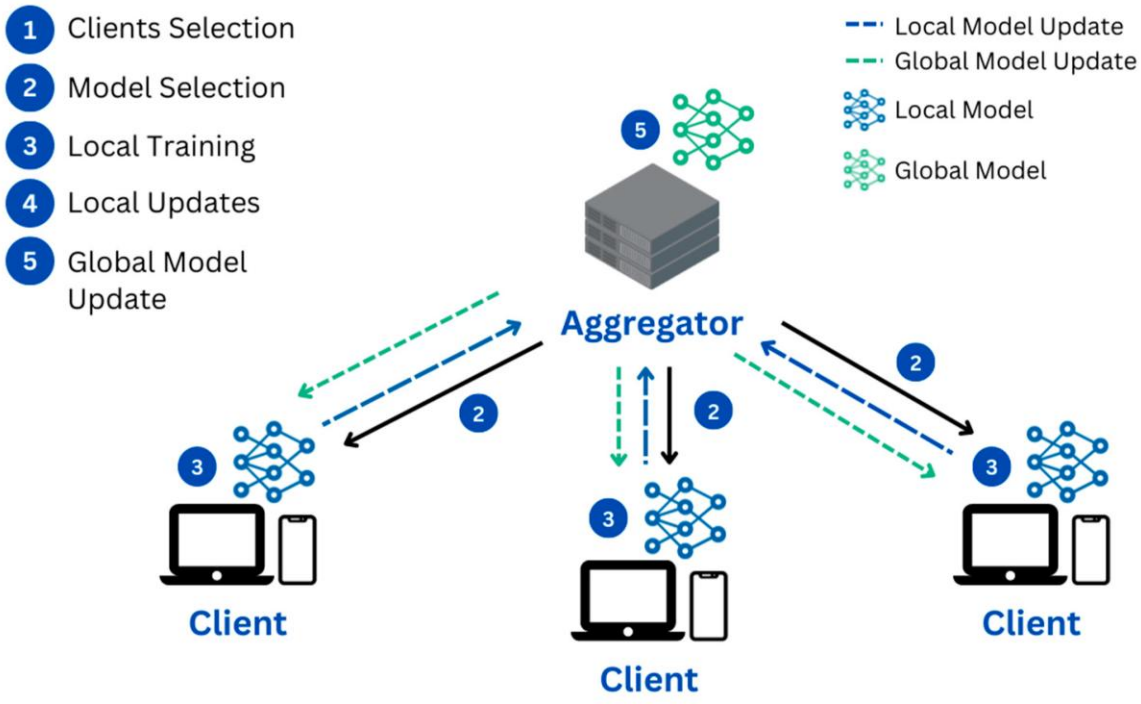
4. How Federated Learning Works in Detail

Federated Learning involves several steps that happen in rounds. Here is how the process usually works:

1. A central server creates a base machine learning model and sends a copy to all the clients (such as smartphones, hospitals, or companies).
2. Each client uses its local data to train the model. This step happens without moving any data outside the device.
3. After local training, each client sends back the updated model to the central server.
4. The server collects all the updates and averages them to create a new, improved global model.
5. This updated model is then sent back to the clients, and the process continues for multiple rounds until the model is accurate enough.

There are two types of Federated Learning:
- Horizontal Federated Learning: where each client has data with the same features but different users.
- Vertical Federated Learning: where clients have data about the same users but with different features.

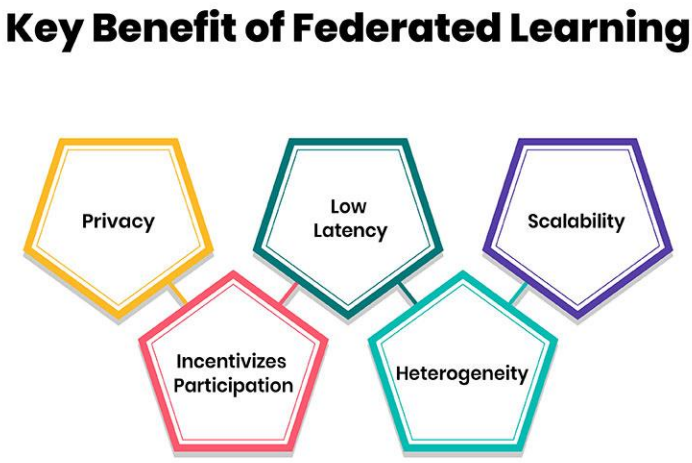
These different types make it flexible for many real-world use cases.



5. Benefits of Federated Learning

There are many benefits to using Federated Learning, both technical and practical:

- Data privacy: Since data never leaves the device, it reduces the risk of leaks or breaches.
- Collaboration: It allows different organizations to work together without needing to share their raw data.
- Efficiency: It reduces the need for large data centers to store and process all information.
- Personalization: In mobile apps, FL helps create models that adapt to each user without sending personal data to the cloud.



6. Real-world Applications

Federated Learning is already being used in different industries:

- Healthcare: Hospitals train models together to detect diseases using MRI scans without sharing patient data.
- Mobile technology: Apps like Google Keyboard and Siri use Federated Learning to learn from users without storing their personal information on servers.
- Logistics: Delivery companies use FL to optimize delivery routes based on local traffic data from multiple companies.
- Retail and marketing: Businesses can train models on customer behavior without sharing sensitive sales data.

These applications show that FL is not just a theory—it's already being used to solve real problems.

7. Technical and Ethical Challenges

Even though Federated Learning sounds ideal, it also comes with some challenges:

- Communication speed: Sending models back and forth can take time, especially if many devices are involved.
- Different data quality: Some devices have more data than others. This can lead to biased models.
- Security: While data is not shared, model updates might still leak information if not protected.
- Complexity: FL systems are harder to manage and require more coordination than central systems.

On the ethical side, it is important to ensure fairness. Some users or groups might not be represented equally, which can lead to biased AI systems. This is why developers need to test and evaluate their models carefully.

8. My Reflections on the Future of Federated Learning

As a student, I find Federated Learning inspiring. It shows that we can build strong AI systems without giving up on user privacy. I think FL will grow even more in the coming years, especially in sectors like education, government, and smart cities.

Working on the Art-IE project helped me see the value of designing systems that respect people's data. It also made me think about how to explain technical topics in ways that non-technical people can understand. I believe that the more we use FL, the more we need to focus on transparency and communication.

9. Conclusion

Federated Learning is a new and exciting approach to machine learning. It helps keep data safe, supports teamwork, and offers useful tools for many industries. In this literature analysis, I learned that FL is not only a technical idea but also a way to protect people's rights in the digital world. I look forward to exploring it more deeply in future projects.

10. References

- Fontys & Odisee. (2025). ART-IE Federated Learning knowledge sharing. Art-IE Project Slides.
- Fontys ICT. (2025). AI, ML, and Federated Learning Introduction. Art-IE Project Presentation.
- Pu, X., & Jonker, D. (2025). Presentatie Art-IE. Fontys ICT.
  Kairouz, P., McMahan, H. B., Avent, B., et al. (2019).
- Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210.
  https://www.researchgate.net/publication/337904104_Advances_and_Open_Problems_in_Federated_Learning