AI 2025
SUMMER SCHOOL
ai.uni-jena.de

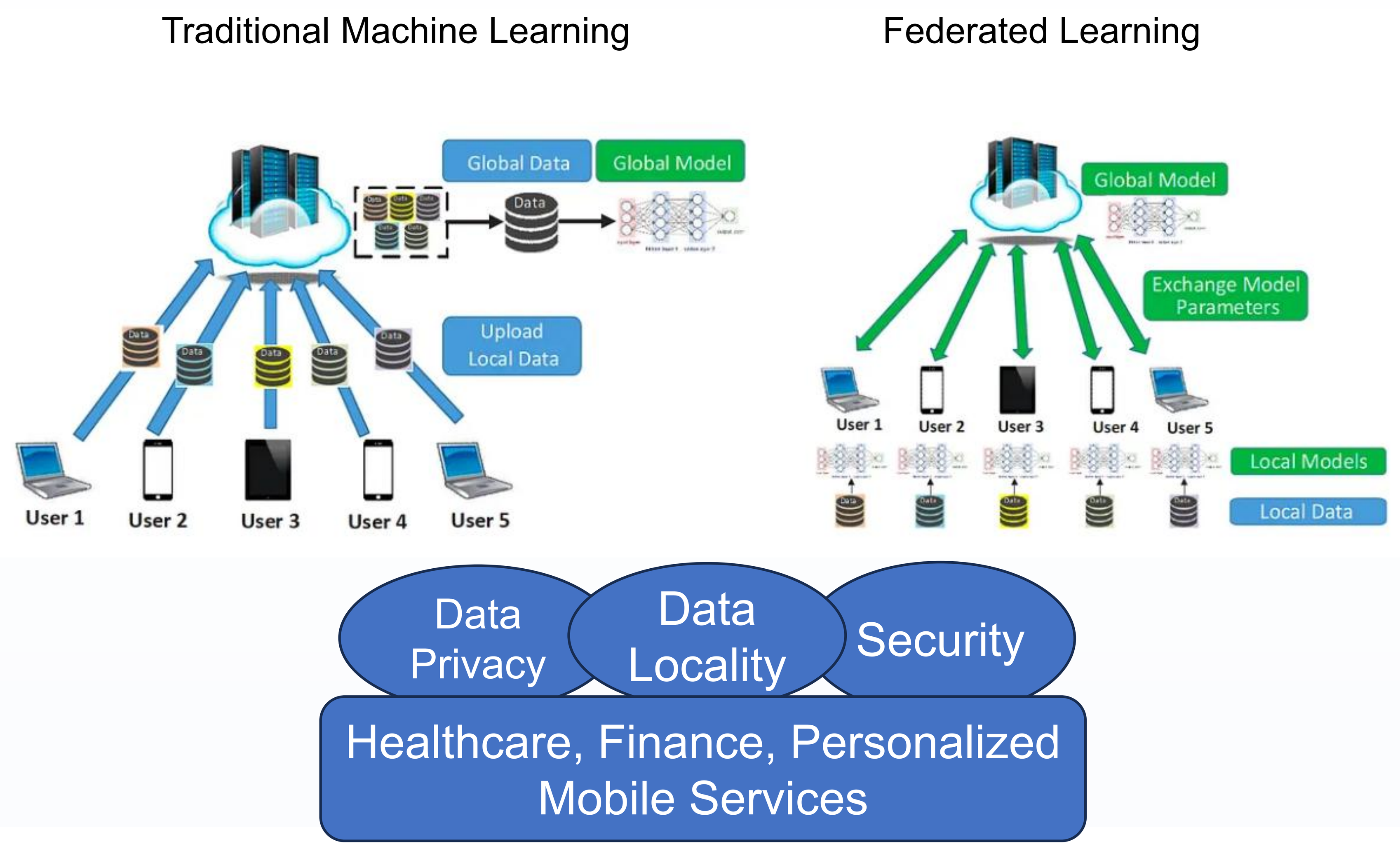
Federated Learning on Mobile Devices

Yamdjeu Sitcheu Mariza

Faculty of Mathematics and Computer Sciences
Friedrich Schiller University Jena

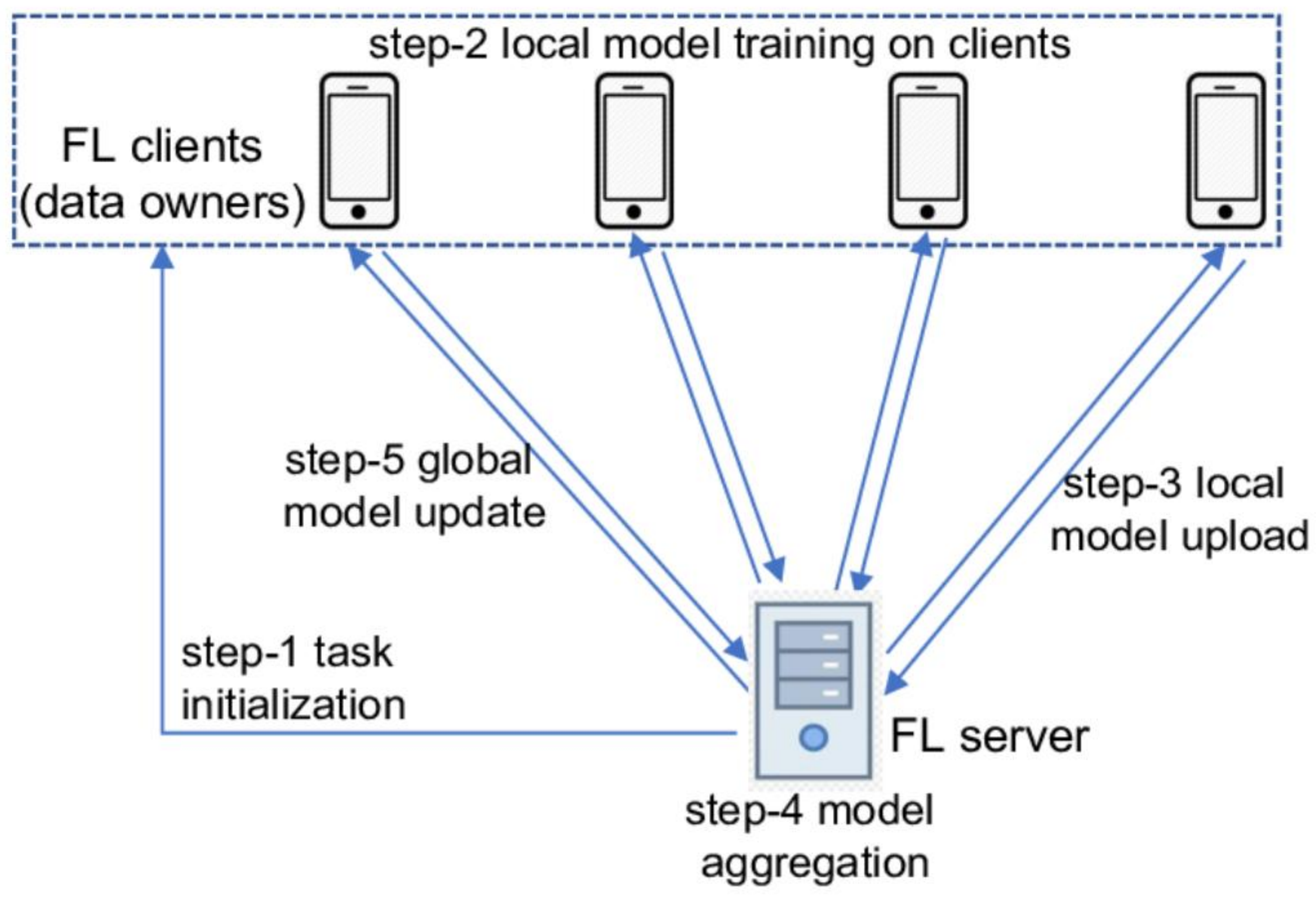
Motivation

As more people use mobile devices and edge computing becomes more common, it's now easier to run machine learning models right at the edge. Nevertheless, the traditional practice require data to be uploaded to the central server, consequently raising various concerns such as privacy and communication. [1]



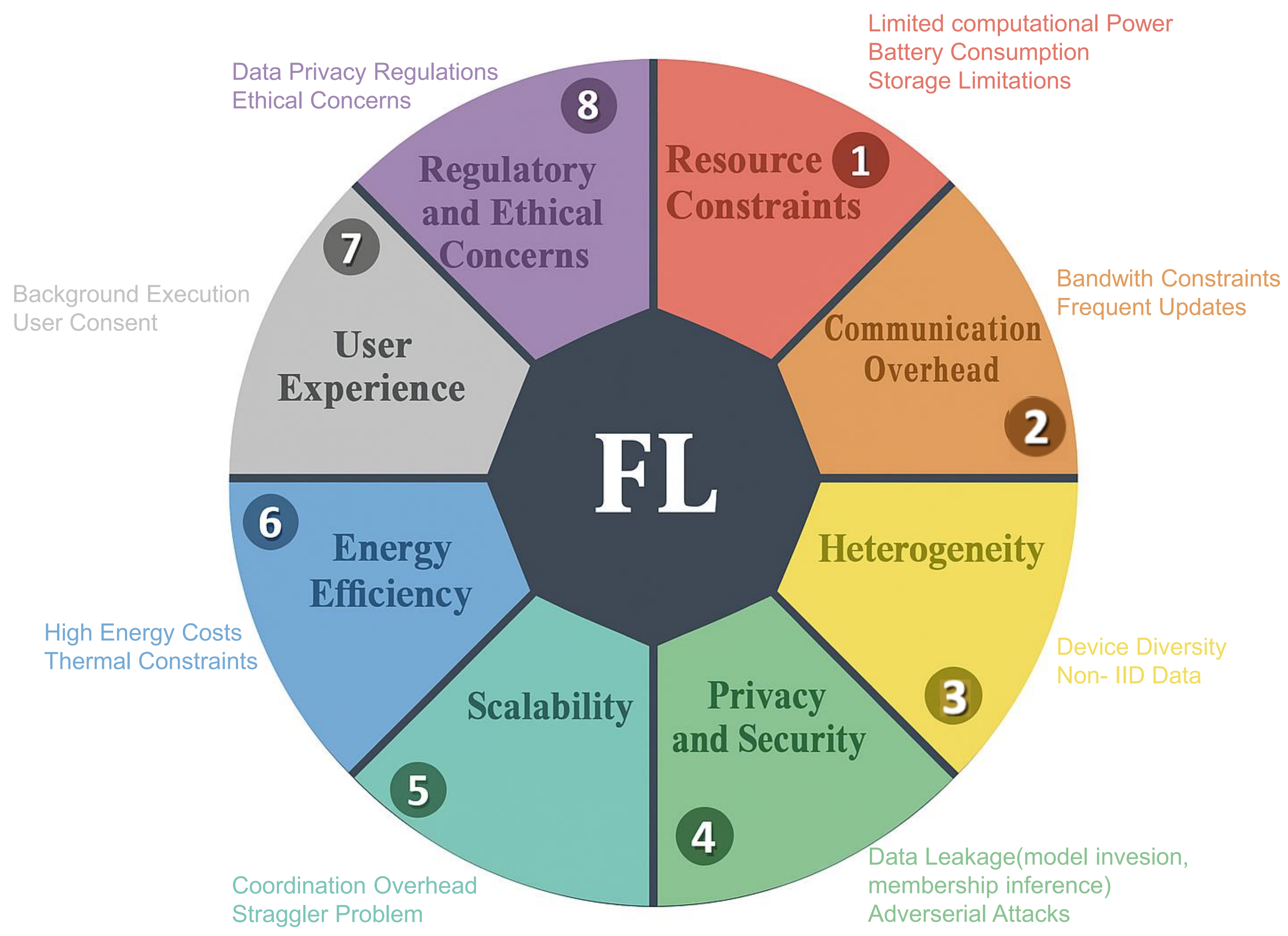
II. Federated Learning Architecture

FL is a distributed machine learning approach that enables multiple devices to train a shared model collaboratively without exchanging raw data. The process involves five principal steps repeated until the model converges or reaches a desired level of accuracy. [2]



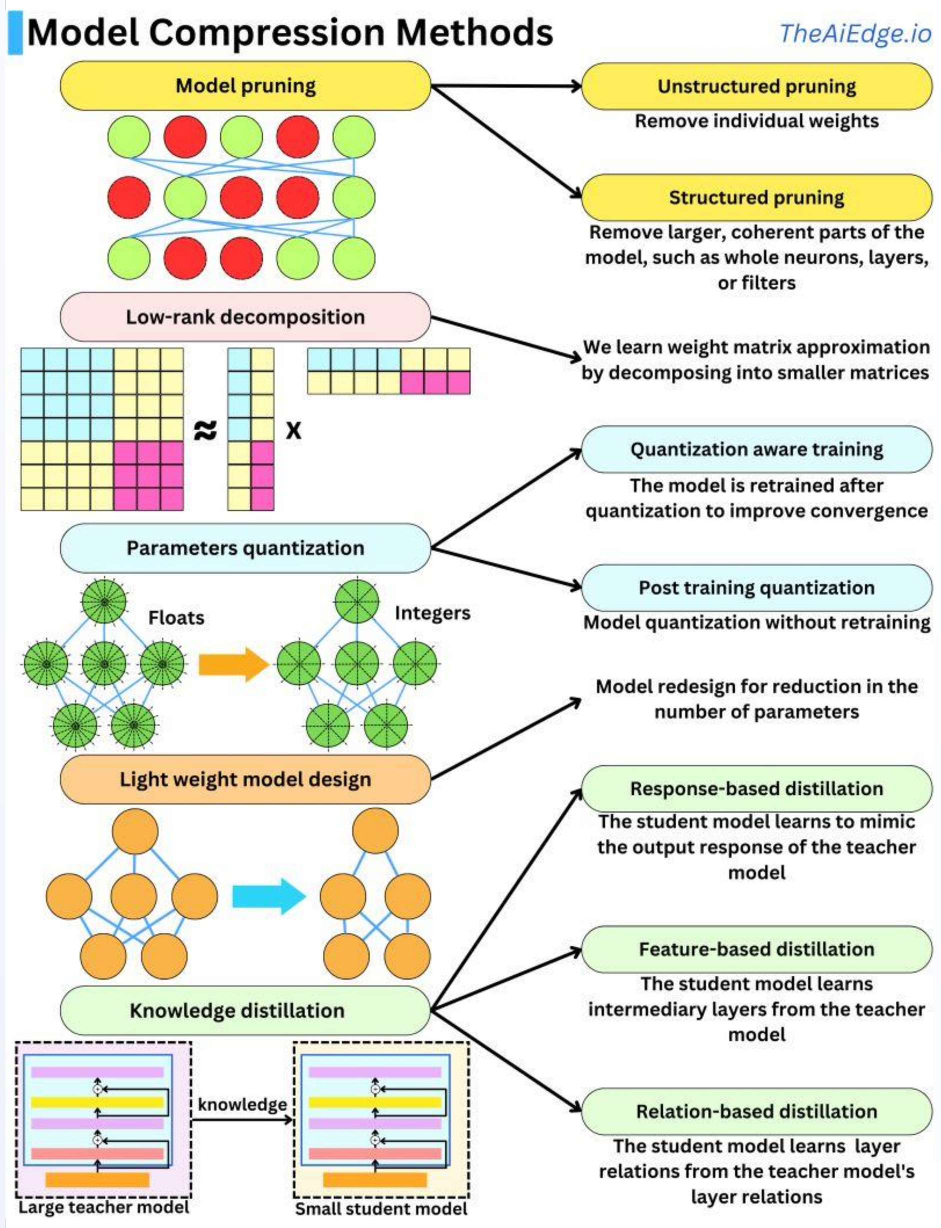
III. Challenges in implementing Federated Learning on Mobile Devices

While FL offers significant advantages, its implementation on mobile devices presents several challenges [3,4]



IV. Opportunities and Solutions

1. Efficient Model Training with Model Compression



2. Communication Efficiency

- Sparse Updates: Transmit only significant model updates to lower Communication overhead.
- Asynchronous Aggregation: Allow devices to submit updates at different times to address the straggler problem.
- Edge Caching: Use edge servers to cache and preprocess data, reducing mobile device load. [3]

3. Handling Heterogeneity

- Adaptative Sampling: Select devices with similar capabilities per training round for consistency
- Federated Transfer Learning: Use pre-trained models to minimize on-device training needs. [3]

4. Privacy and Security Enhancements

- Differential Privacy : Add noise to model updates to prevent data leakage while preserving accuracy.
- Secure Aggregation: Apply homomorphic encryption and secure multi-party computation to protect updates
- Robust Aggregation: Detect and filter malicious updates to enhance model robustness. [3]

V. Real-World Applications

Real-Life Example	Description	FL Type(s)
Apple's Siri Voice Recognition	Apple uses federated learning to improve Siri's speaker recognition, training models on local audio data from iPhones/iPads to recognize "Hey Siri" commands. Only model updates are sent to a central server, keeping raw audio private. Differential privacy adds noise for extra protection.	Horizontal FL, Cross-Device FL
HealthCare Rare Disease Diagnosis [5]	Google Health uses federated learning to combine insights from multiple healthcare providers' datasets (e.g., different medical records for the same conditions) to improve rare disease diagnosis without centralizing sensitive data.	Vertical FL, Cross-Silo FL
Google Gboard Next-Word Prediction	Google's Gboard keyboard app trains local models on users' typing data to enhance predictive text and autocorrect features. Model updates are shared with a central server, preserving user privacy by keeping raw keystrokes on-device.	Horizontal FL, Cross-Device FL

Conclusion

Getting FL to work on mobile devices isn't without its obstacles, yet it's a breakthrough when it comes to keeping data private while still building smart AI. By tackling issues like limited resources, communication costs, and difference between devices, FL opens up lots of exciting possibilities from customizing your keyboard to helping diagnose health conditions. As research keeps progressing, FL could really change the way we develop and use machine learning, making AI more available, faster, and safer for everyone.

References

[1] Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. ACM Computing Surveys (CSUR), 54(2), 1-36.

[2] Duan, Qiang & Hu, Shijing & Deng, Ruijun & Lu, Zhihui & Yu, Shui. (2022). Combining Federated Learning and Edge Computing toward Ubiquitous Intelligence: Challenges, Recent Advances, and Future Directions. 10.36227/techrxiv.21788450.

[3] Duggirala, Jagadeesh. (2024). Federated Learning on Mobile Devices: Challenges, Opportunities, and Future Directions. International Scientific Journal of Engineering and Management. 03. 1-7. 10.55041/ISJEM02079.

[4] Zhang, Tuo & Gao, Lei & He, Chaoyang & Zhang, Mi & Krishnamachari, Bhaskar & Avestimehr, Salman. (2021). Federated Learning for Internet of Things: Applications, Challenges, and Opportunities. 10.48550/arXiv.2111.07494.

[5] Hudaib, A., Obeid, N., Albashayreh, A., Mosleh, H., Tashtoush, Y., & Hristov, G. (2025). Exploring the implementation of federated learning in healthcare: a comprehensive review. *Cluster Computing*, *28*(5), 1-21.