Securing the FL Landscape:

A Comparative Analysis of Attacks in Centralized and Decentralized Models

By: Alberte Krogh Hansen, Alexis Donato Calin, and Kimika Uehara

Table of contents

What is Federated Learning?

Advantages of FL

- **Privacy**: Data remains on local devices; only model updates are shared.
- **Communication Efficiency**: Only small parameter updates are exchanged.
- **Scalability**: Ideal for distributed systems requiring privacy-preserving collaboration.

Challenges in FL

- **Single Point of Failure (SPoF)**: Dependency on a central server creates vulnerabilities.
- **Server Vulnerabilities**: Risks of data breaches and model corruption.
- **Fairness & Scalability**: Aggregated models may not perform equally well across diverse clients.

What is Decentralized Federated Learning?

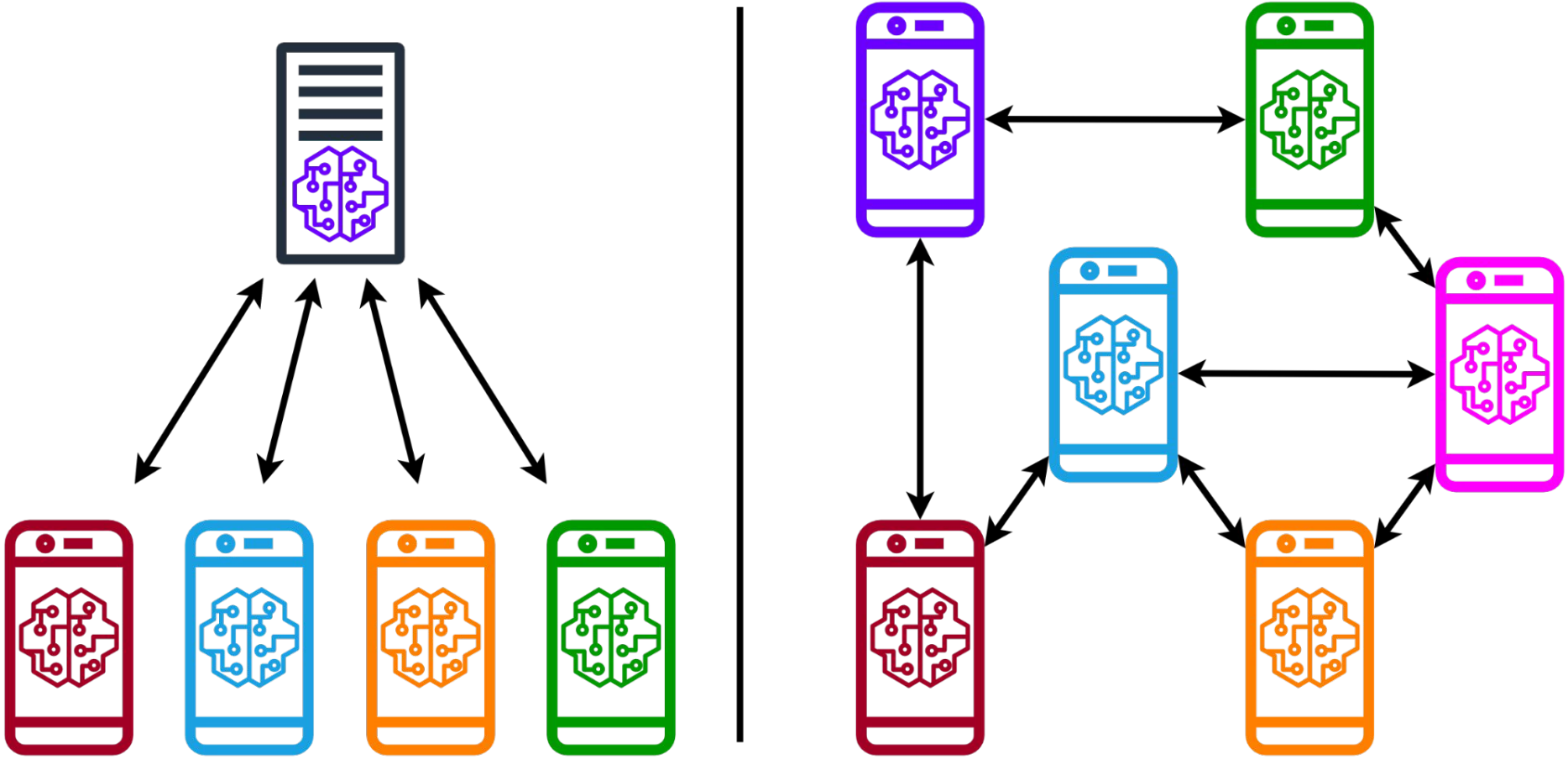
Advantages of DFL

- **Scalability:** Handles many participants effectively.
- **Fairness:** Reduces bias from centralized aggregation.
- **Robustness:** Resilient to central server failures.

Challenges in DFL

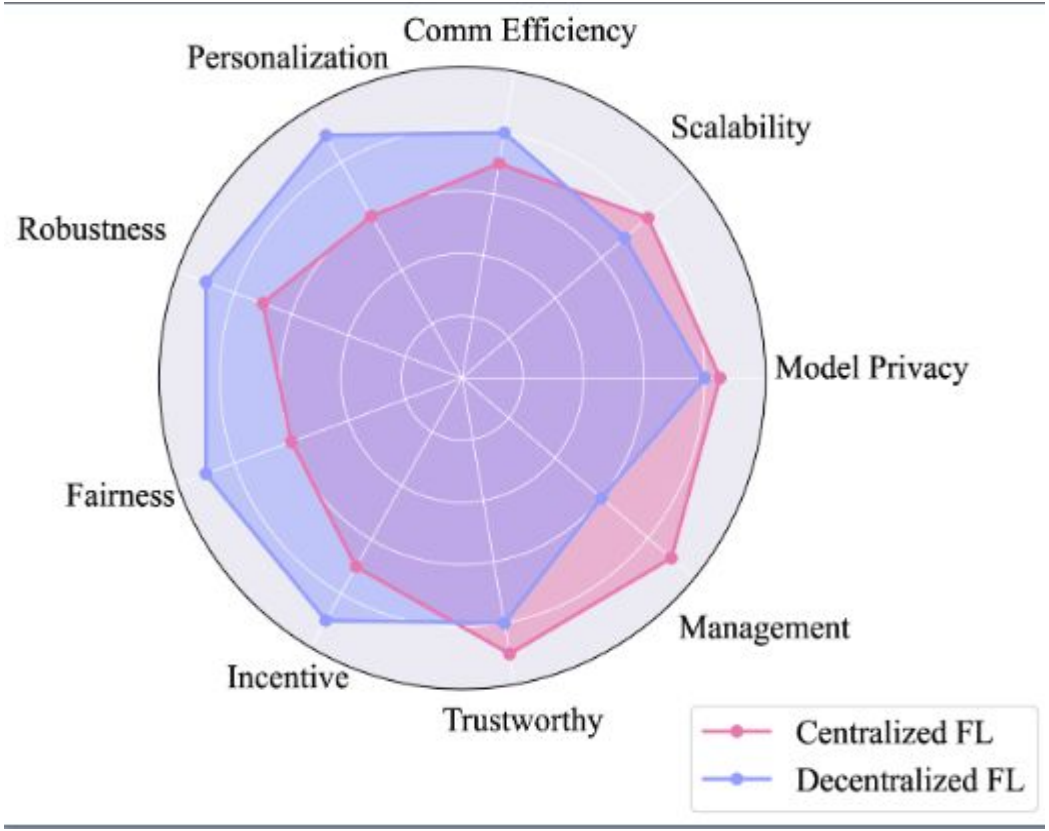
- **Higher Complexity:** More difficult to implement and manage.
- **Consistency Issues:** Requires advanced synchronization mechanisms.
- **Lack of central managemen**t: No central server to aggregate and update = adds to higher complexity.

FL VS DFL

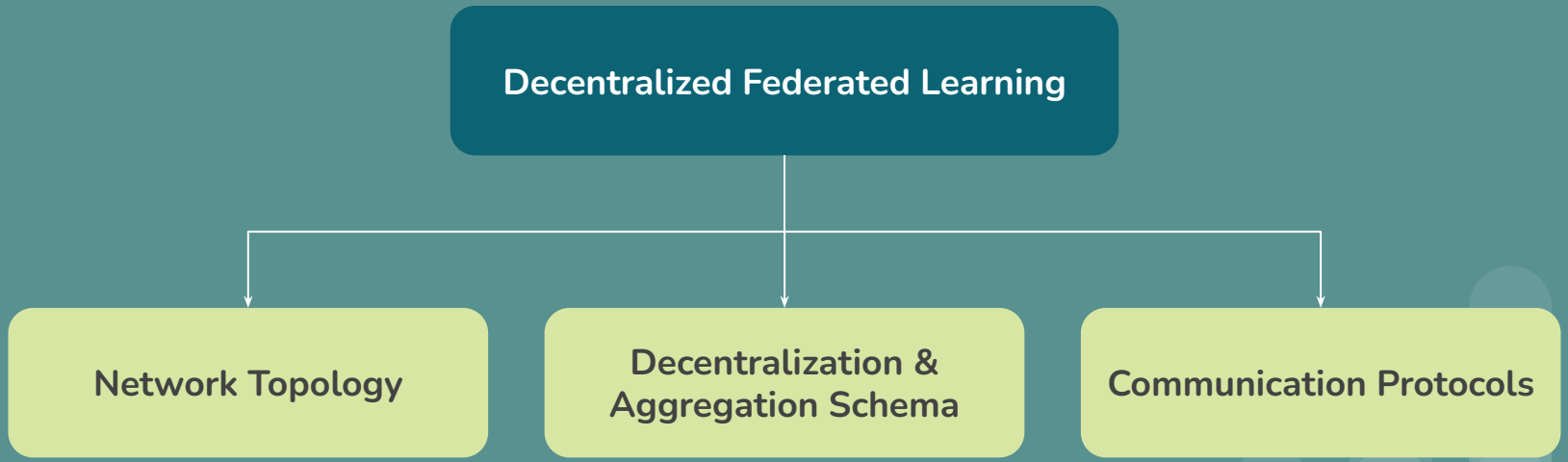


Key Trade-off

- FL: Simplicity vs. Vulnerability.
- DFL: Robustness vs. Complexity.

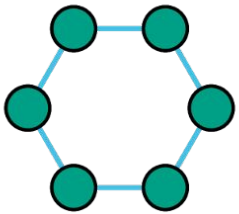


Components of DFL & Security Implications

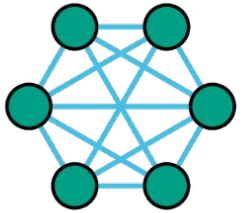


Network Topology pt. 1

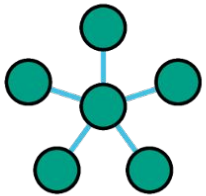
(a) Line



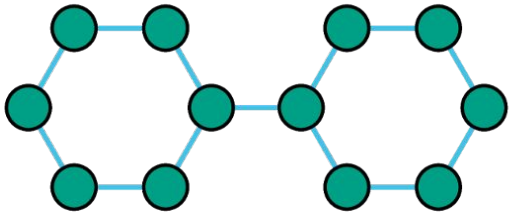
(b) Ring



(c) Mesh



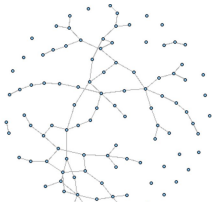
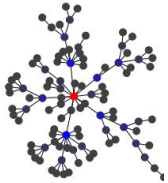
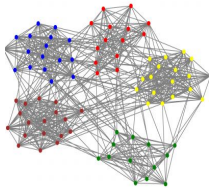
(d) Star



(g) Hybrid

Source: Liangqi Yuan, Ziran Wang, Lichao Sun, Philip S. Yu, and Christopher G. Brinton. Decentralized federated learning: A survey and perspective, 2024.

Network Topology pt. 2

Model	Characteristics	Security Implications
Erdos-Renyi (ER)	Random graphs with homogeneous structure 	**PROS:** More uniform, better local data retention, less targeted attacks **CONS:** Limited knowledge diffusion
Barabasi-Albert (BA)	Random scale-free networks (power law) 	**PROS:** High-degree hubs enhance connectivity **CONS:** Potential SPoF
Stochastic Block Model (SBM)	Community-like network 	**PROS:** Distinct communities with limited external data access **CONS:** Limited learning efficiency and knowledge sharing

Decentralization & Aggregation Schema

Fully Decentralized

Model updates aggregated through direct exchanges among clients

✔️No SPoF
✔️Fault Tolerance
❌No central oversight
❌Data leakage

Partial Aggregation

Intermediate nodes perform some aggregation

✔️Intermediate nodes act as filters
❌Trusted nodes become target

Blockchain

Blockchain stores the global model
Aggregation via miner code / smart contract

✔️Tamper-proof
✔️Traceable
✔️Consensus mechanisms
❌Blockchain-based vulnerabilities

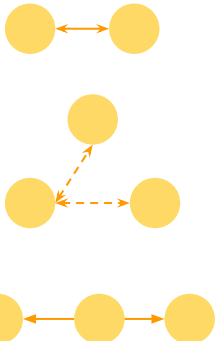
Communication Protocols

Parameter Sharing

- **Synchronous**
  - ✔ Reliability
  - ✘ Slow or idle participants, SPoF
- **Asynchronous**
  - ✔ Faster convergence
  - ✘ Delayed/duplicate updates
- **Semi-synchronous**
  - ✔ Speed and resource efficiency
  - ✘ Vulnerable aggregation

Protocols

- **Pointing**
  - ✔ Limits data exposure
  - ✘ Eavesdropping/interception
- **Gossip**
  - ✔ Fault tolerance & robustness
  - ✘ Less traceability
- **Broadcast**
  - ✔ High transparency & robustness
  - ✘ DoS & malicious broadcast



Common Attacks and Defenses on FL

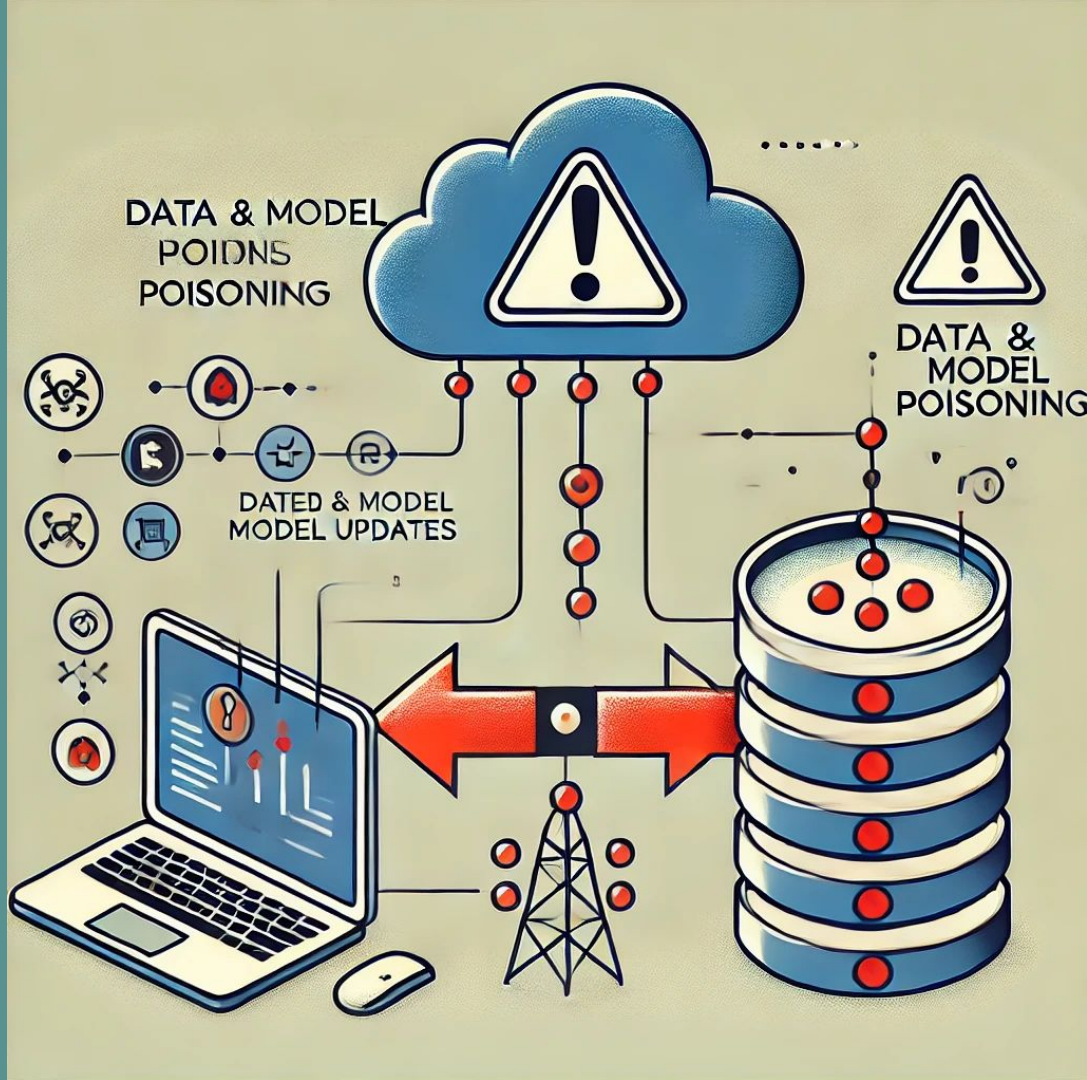
3. Poisoning Attacks

Data Poisoning: Manipulating client datasets to mislead model training.

Model Poisoning: Uploading malicious model updates to the server.

Impact: Reduces model accuracy, introduces biased or incorrect predictions.

Defence: E.g. Anomaly Detection



1. Byzantine Attack

Attack:

- Collusion by multiple malicious clients (Byzantine users).
- Fake updates disrupt global model convergence or degrade accuracy.
- Hard to detect in large-scale systems.

Defence:

Credibility-Based detection

Blockchain-Based FL framework

2. Server Exploitation

- Centralized server is a high-value target for attackers.
- Exploits can lead to model corruption or extraction of sensitive data.

Common Attacks and Defenses on DFL

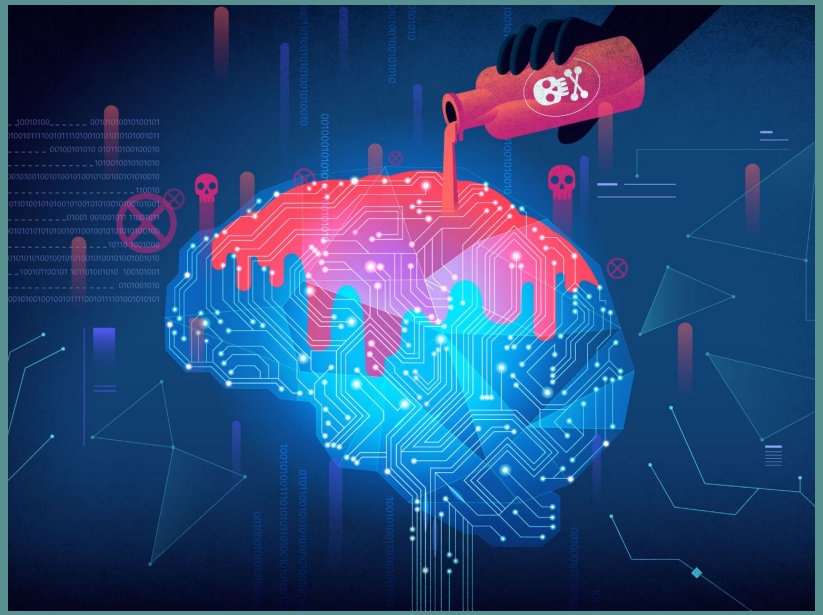
1. Poisoning Attacks and Defenses in DFL

Data Poisoning: aim to poison the global model by sending model updates derived from mislabeled data

Model Poisoning: manipulates the model's parameters to cause it to behave in an undesirable way

Defences:

- **Anomaly Detection**
- **Pruning**
- **Federated distillation**



2. Privacy Breach Attacks on DFL

Model Inversion: Exploit shared model parameters to reconstruct private data.

Membership Interference: Aim to infer whether a data record was used to train a target model or not.

Defence:

- **Secure Multi-Party Computing**
- **Differential Privacy**
- **Homomorphic Encryption**

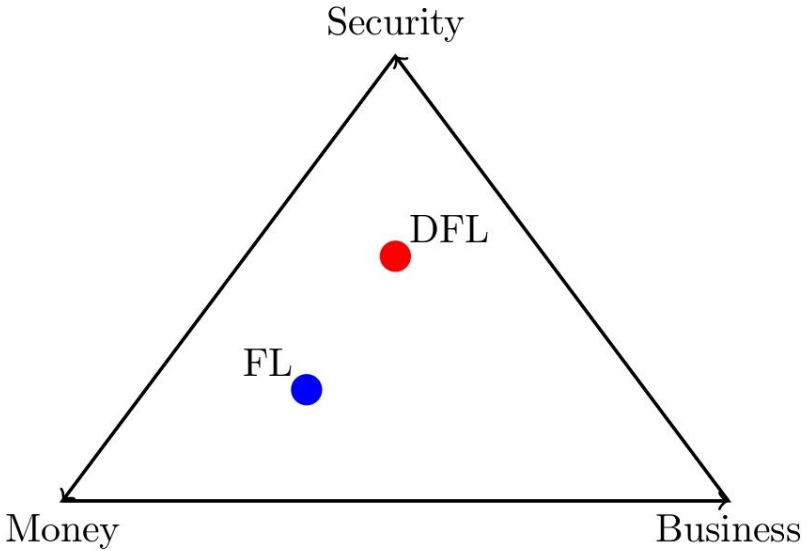
3. Blockchain-based Attacks and Defenses in DFL

Attack	Characteristics
Consensus/Sybil	Majority control with fake nodes
Privacy Poisoning	Inject personal data
Routing Attacks	Tamper with packet routing
Private Key Hijacking	Flaws in key-signing mechanisms
DDoS	Fill the buffer with spam data

Discussion

Interplay between Money, Business, and Security for both FL and DF

- FL: Cheaper to implement at the cost of security
- DFL: Better security at the cost of a more expensive implementation
- Neither are better or worse for facilitating the business



Challenges and Future Directions

Challenges:

- Communication overhead & scalability
- Processing power & energy usage

Future Directions:

- Network dynamics & model aggregation strategies
- Blockchain integration
- Empirical studies & tailored solutions