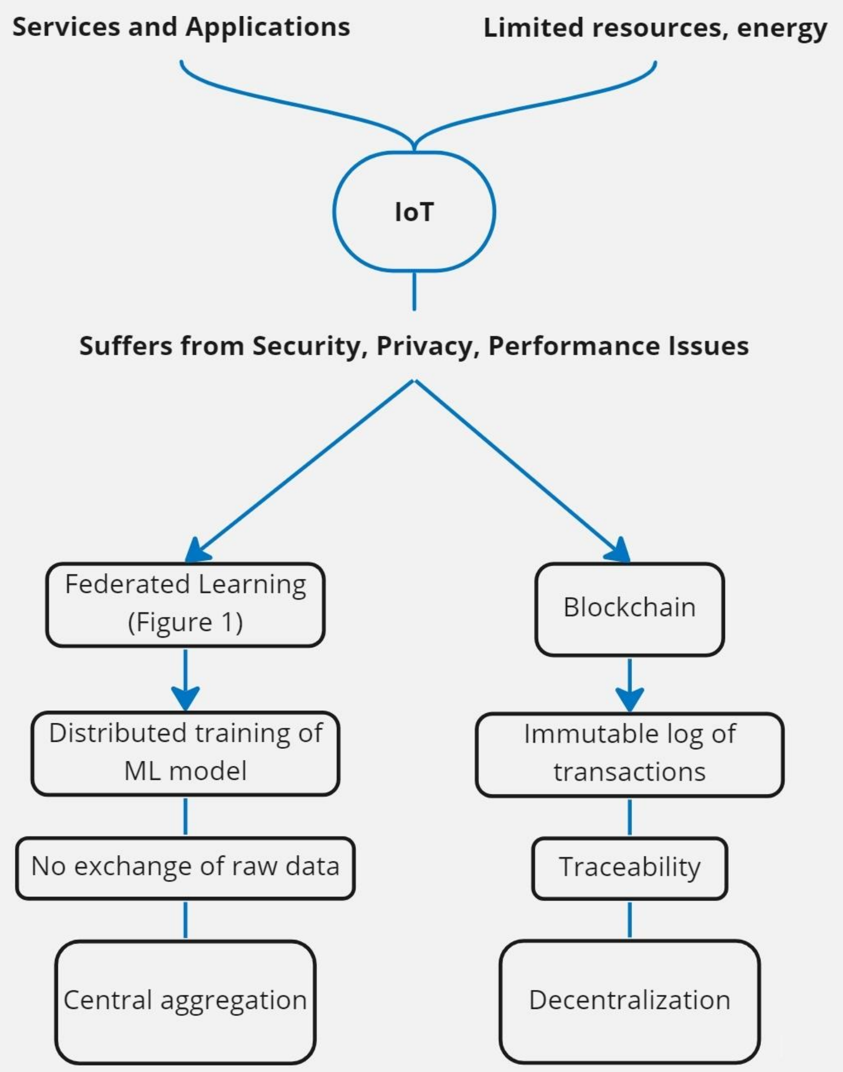
Blockchain-empowered federated learning based solutions for Internet of Things Security, Privacy, and Performance

Author: Panagiotis Papadopoulos

Supervisor: Chhagan Lal
Responsible Professor: Mauro Conti

TU Delft

1 BACKGROUND


Services and Applications
Limited resources, energy
IoT
Suffers from Security, Privacy, Performance Issues
Federated Learning (Figure 1)
Blockchain
Distributed training of ML model
Immutable log of transactions
No exchange of raw data
Traceability
Central aggregation
Decentralization

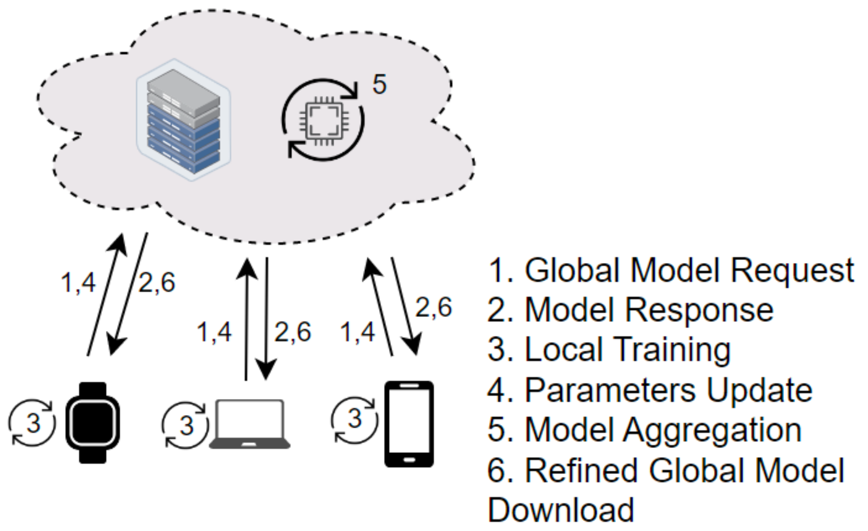


Figure 1: Federated Learning in IoT

2 MOTIVATION

- Federated Learning does not come without **setbacks**:
  - Requires a central authority
  - Communication overhead
  - No incentive for nodes to participate
- Interesting to explore how **Blockchain can be used to enhance Federated Learning**

3 RESEARCH QUESTION

- **Blockchain-empowered federated learning-based solutions for Internet of Things Security, Privacy, and Performance**
- **Study and review state-of-the-art solutions** that attempt to enhance IoT Security, Privacy, and Performance

4 ANALYSIS & DISCUSSION

- Strong **focus** on enhancing **security**
- **Privacy** is covered to a lesser extent
- Most solutions take **performance** into account
- **Blockchain not used** in most solutions
- **Reflect on challenges** of implementation

Papers	Security	Privacy	Performance	FL	BC	Testing	Application
IOTFLA [1]	●	●	○	●	○	○	Smart Home
FL IDS IoV [2]	●	○	●	●	○	◐	IoV
RAFeL [3]	●	○	●	●	○	●	Malware Detection for IoT
(POSTER) Decentralized FL Anomaly Detection [4]	◐	○	◐	●	○	◐	General IoT
Blockchain & Federated Learning Distributed Architecture for IoT [5]	●	●	◐	●	●	●	General IoT

Table 1: Comparison of state-of-the-art solutions for IoT using Blockchain and Federated Learning

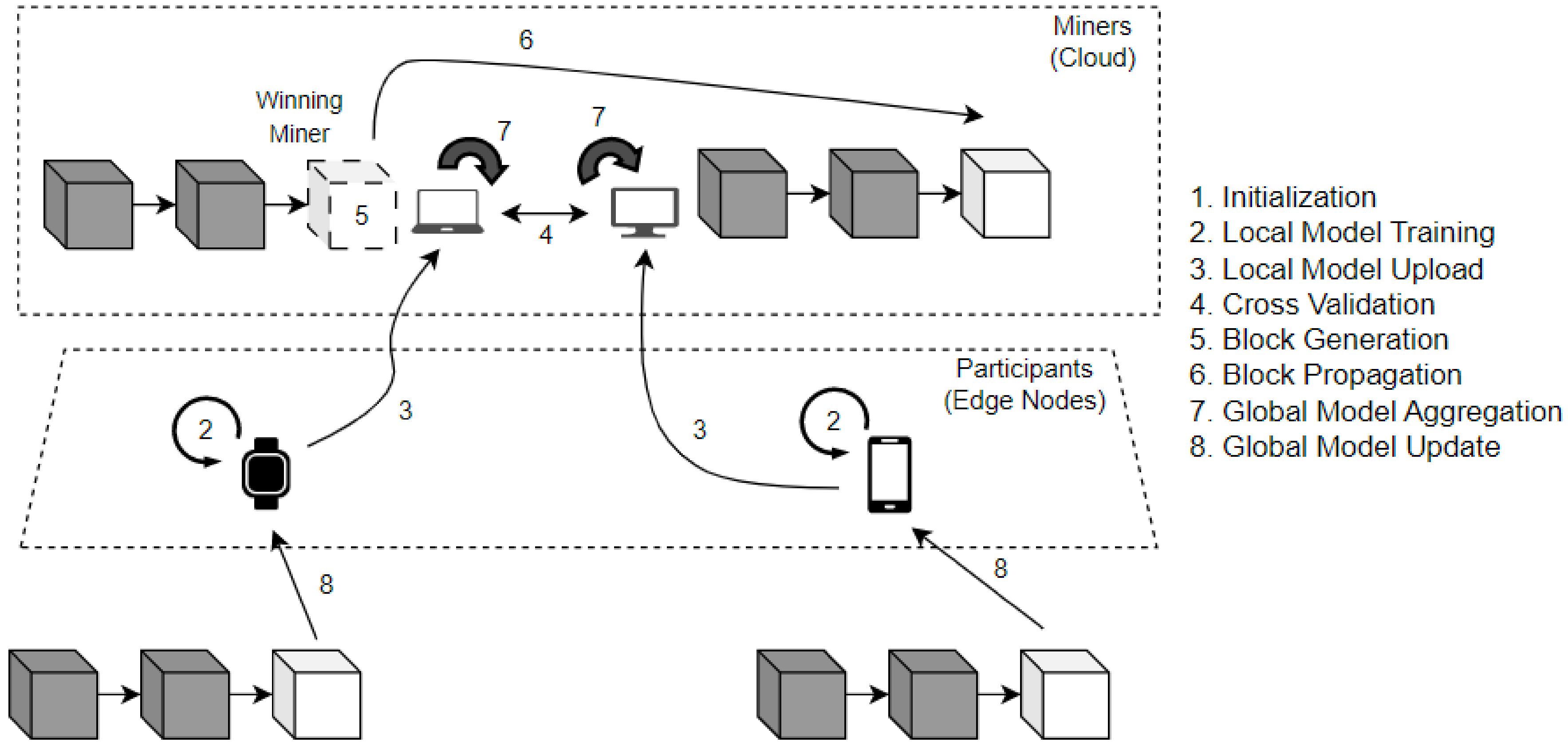


Figure 2: Integration Architecture of blockchain-enabled FL

5 FUTURE RESEARCH

Integration of Blockchain with FL

- Research shows the potential, but further studying is required
- Federated Learning itself is a complicated technology
- A possible direction is towards the generic architecture shown in Figure 2:
  - Using Blockchain to verify local results and store the global model
  - Using Blockchain to incentivize nodes with a reward scheme or smart contracts

Simulations & real-world implementation

- Crucial to design the models such that they can be implemented to the real-world
- Important to properly test them too
- Most of the proposed solutions provide experimental setups
  - Small scale
  - With assumptions

Security, Privacy, and Performance

- Easy for a malicious party to gain access to end nodes
- Research focuses on anomaly detection
- The existence of central aggregation servers hinders security
- Decentralized solutions are preferable
- Develop novel security solutions to shield the central server
- Communication overhead
  - Compression algorithms

6 CONCLUSIONS

- Federated Learning is a **promising technology** to enhance security, privacy, and performance of IoT
- Federated Learning **presents some challenges**
- **Blockchain** is deemed a **good fit** to integrate with federated learning and mitigate those issues
- There is still **research needed** until blockchain-enhanced federated learning can be **efficiently applied** in large scale real-world scenarios

[1] U. M. Aïvodji, S. Gambs, and A. Martin, "Iotfla : A secured and privacy-preserving smart home architecture implementing federated learning," in 2019 IEEE Security and Privacy Workshops (SPW), 2019, pp. 175–180.
[2] Hbaieb, S. Ayed, and L. Chaari, "Federated learning based ids approach for the iov," ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3538969.3544422
[3] S. Shukla, G. Kolhe, H. Homayoun, S. Rafatirad, and S. M. P D, "Rafel - robust and data-aware federated learning-inspired malware detection in internet-of-things (iot) networks," in Proceedings of the Great Lakes Symposium on VLSI 2022, ser. GLSVLSI '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 153–157. [Online]. Available: https://doi.org/10.1145/3526241.3530378
[4] Lian and C. Su, "Decentralized federated learning for internet of things anomaly detection," in Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, ser. ASIA CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 1249–1251. [Online]. Available: https://doi.org/10.1145/3488932.3527285
[5] P. Kumar Sharma, P. Gope, and D. Puthal, "Blockchain and federated learning-enabled distributed secure and privacy-preserving computing architecture for iot net- work," in 2022 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), 2022, pp. 1–9.