Mykyta Luzan[1]

Secure Data Sharing in the Internet of Vehicles Using Blockchain-based Federated Learning

Master's Thesis (30 ECTS)

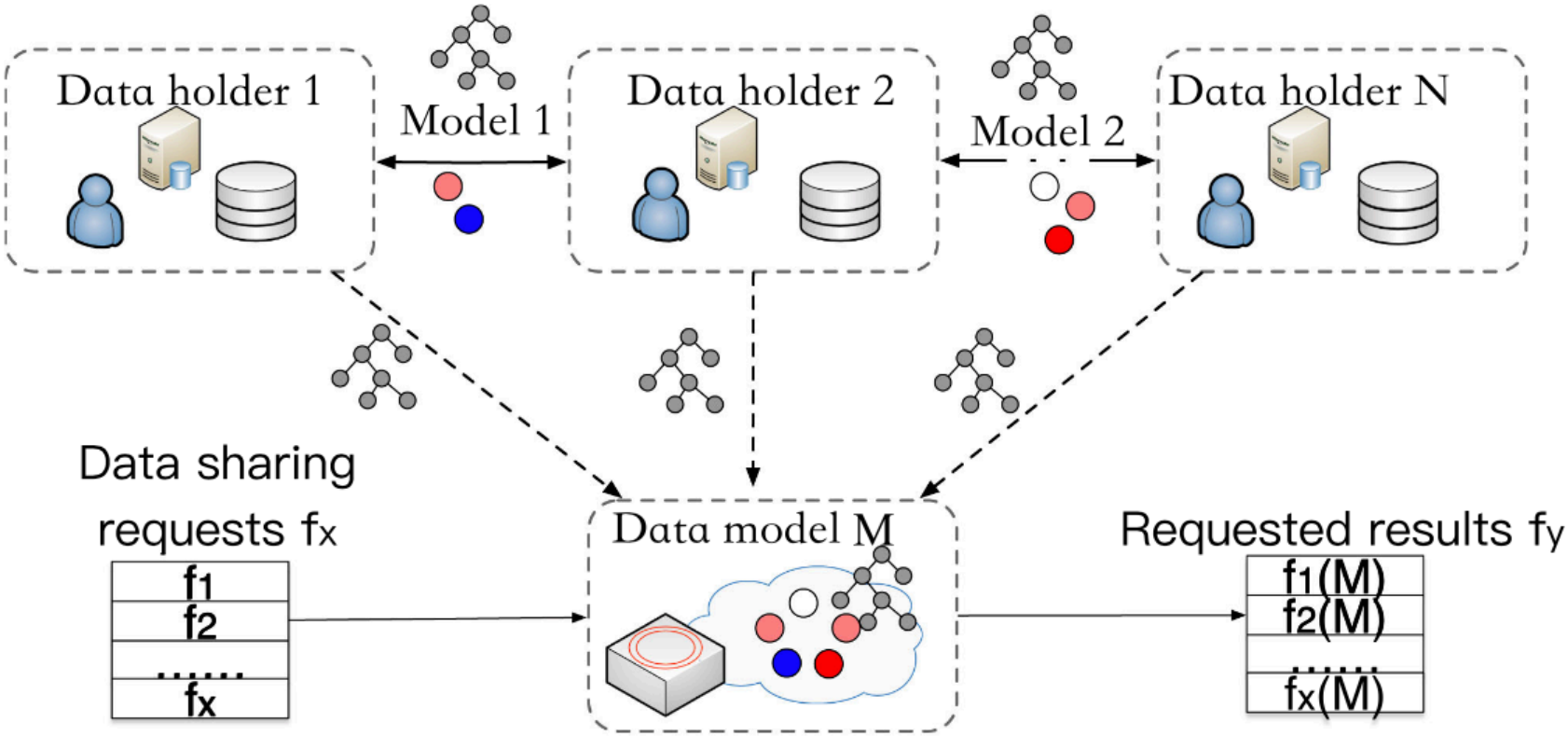
University of Tartu

23.01.2025

[1]Supervisors: Dr. Mubashar Iqbal and Dr. Raimundas Matulevičius

Data Sharing Using Federated Learning

During FL, data providers share trained ML models instead of exchanging their raw data.



IoV Use Case

Example: **Traffic trajectory prediction**

Actors:

- Vehicles - data holders
- Road Side Units (RSUs) - aggregators, curators

Assets:

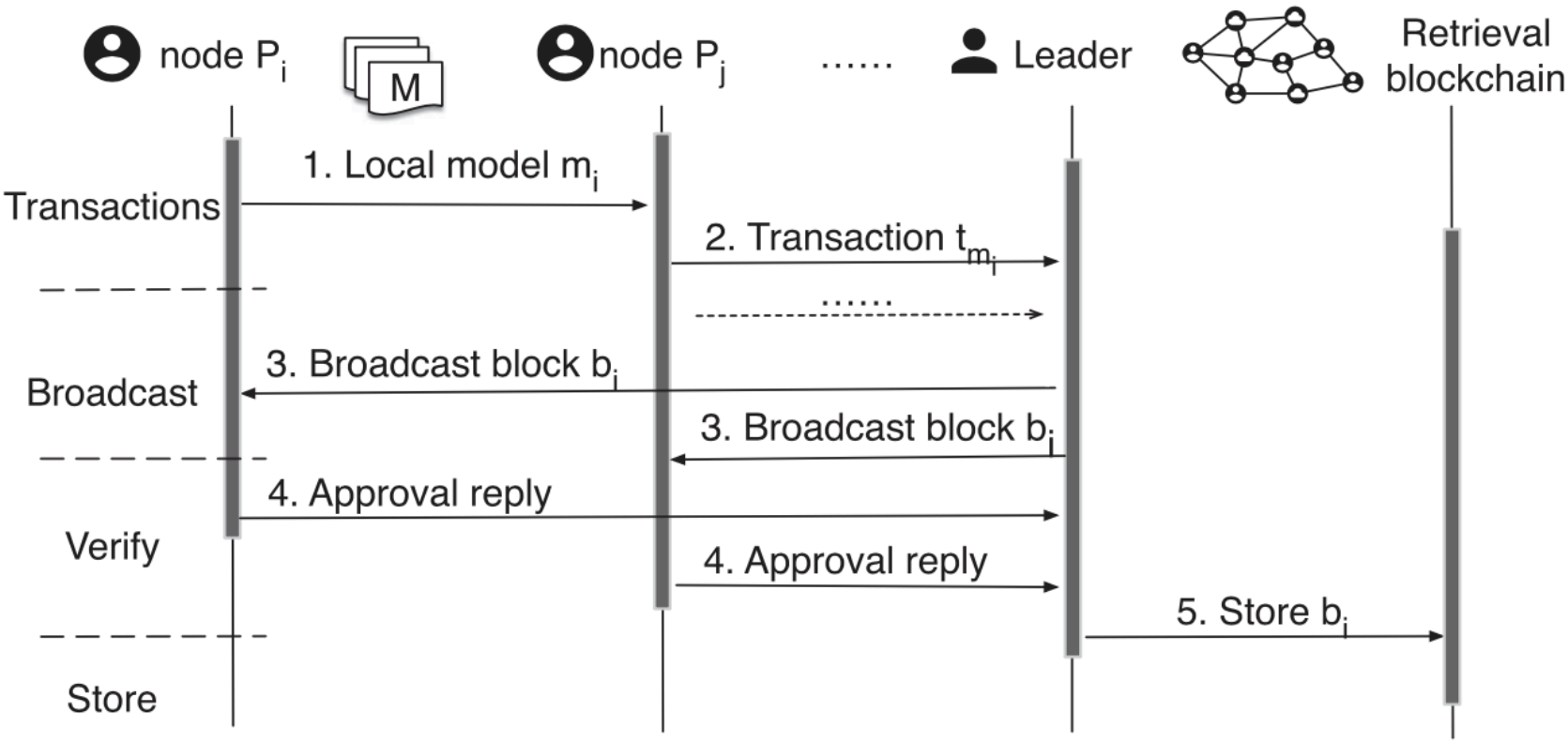
- Raw traffic data - confidentiality
- Local and global models - integrity & availability

Centralization Challenge

Main obstacles with the presence of **a centralized curator**:

- a high volume of traffic data
- lack of trust
- increased risk of **data leakage** and **data tampering**

Blockchain


node P_i
M
node P_j
.....
Leader
Retrieval blockchain
Transactions
1. Local model m_i
2. Transaction t_{m_i}
.....
Broadcast
3. Broadcast block b_i
3. Broadcast block b_i
4. Approval reply
Verify
4. Approval reply
5. Store b_i
Store

Zero-knowledge Proof (ZKP)

ZKP verifies that a certain **public algorithm** (weighted FedAvg) produced **public outputs** (new global model weights) for certain **private inputs** (local ML weights)

Research Question

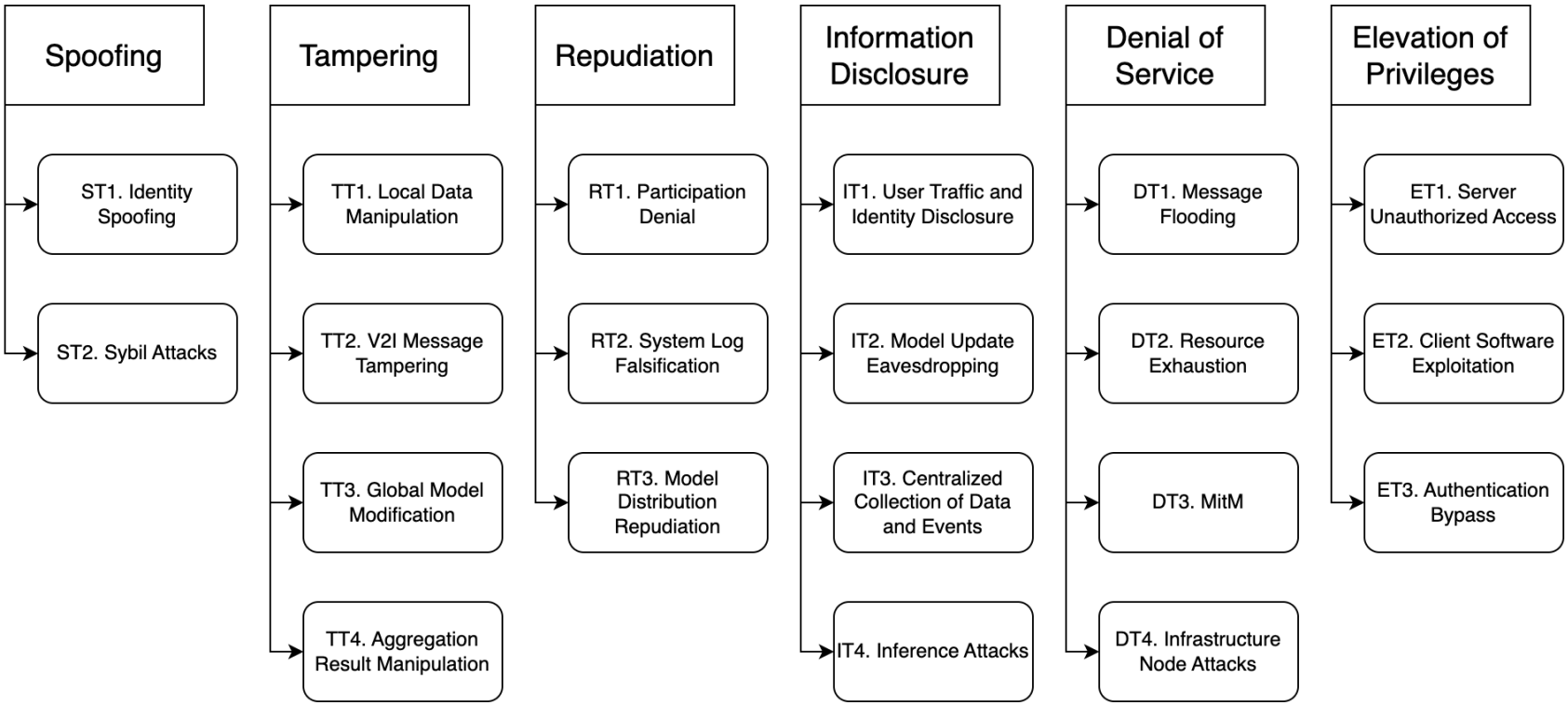
How **blockchain** and **ZKP** could mitigate the **security risks** in the centralized **FL** in the IoV?

Literature Review

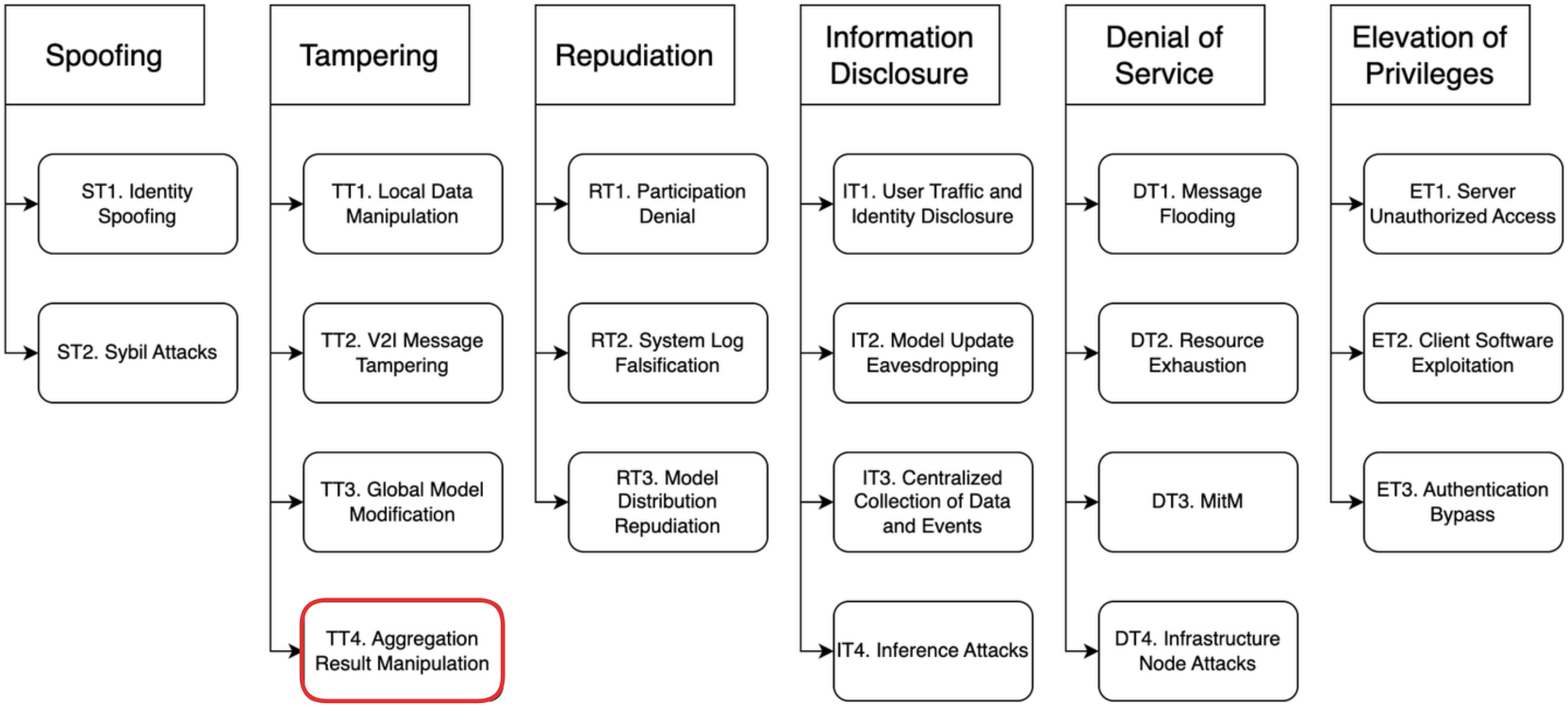
Snowball sampling technique:

- Started with 5 surveys
- Centralized FL attacks (24 papers)
- Defense mechanisms (30+ papers)

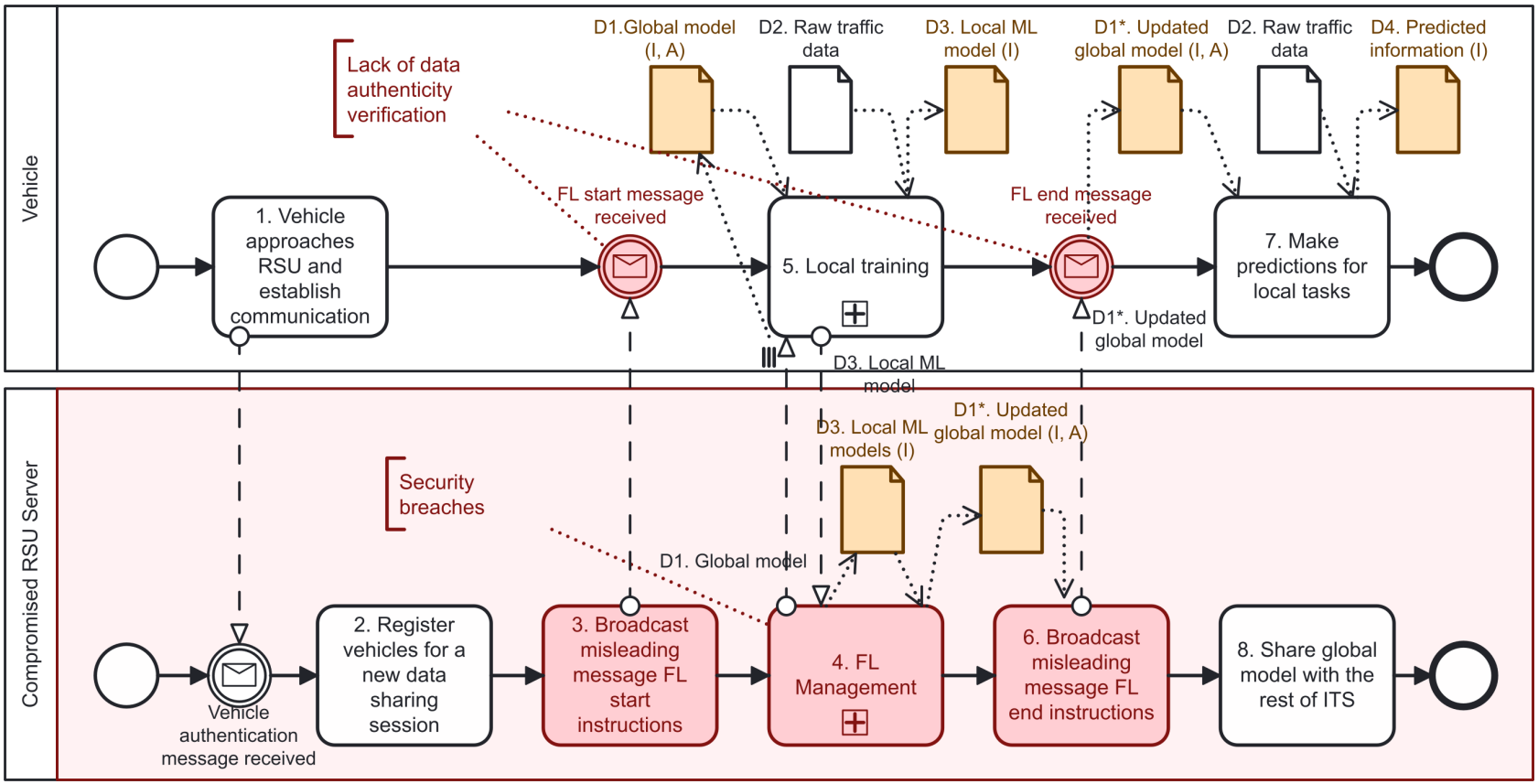
Threat Model. STRIDE



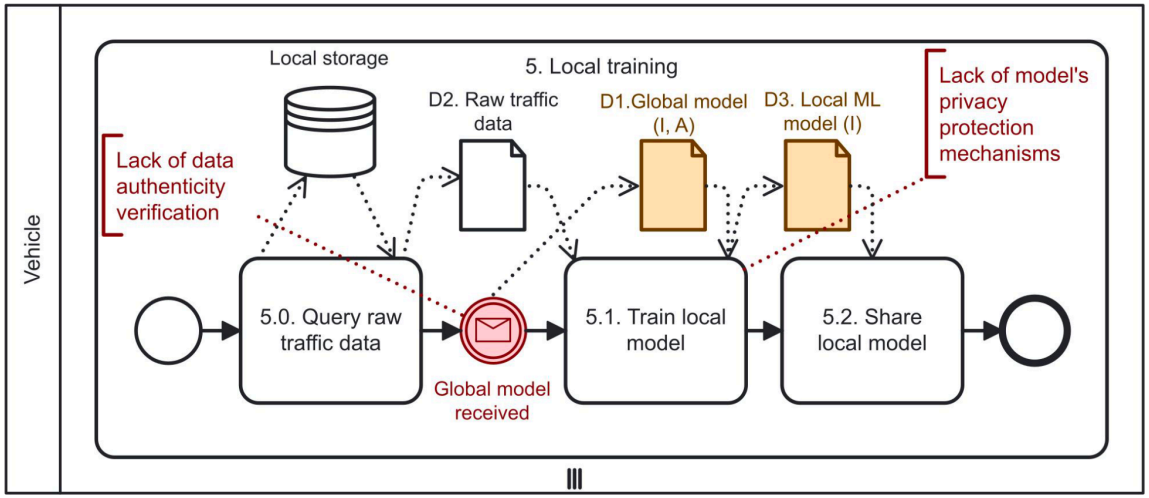
Threat Model. Tampering

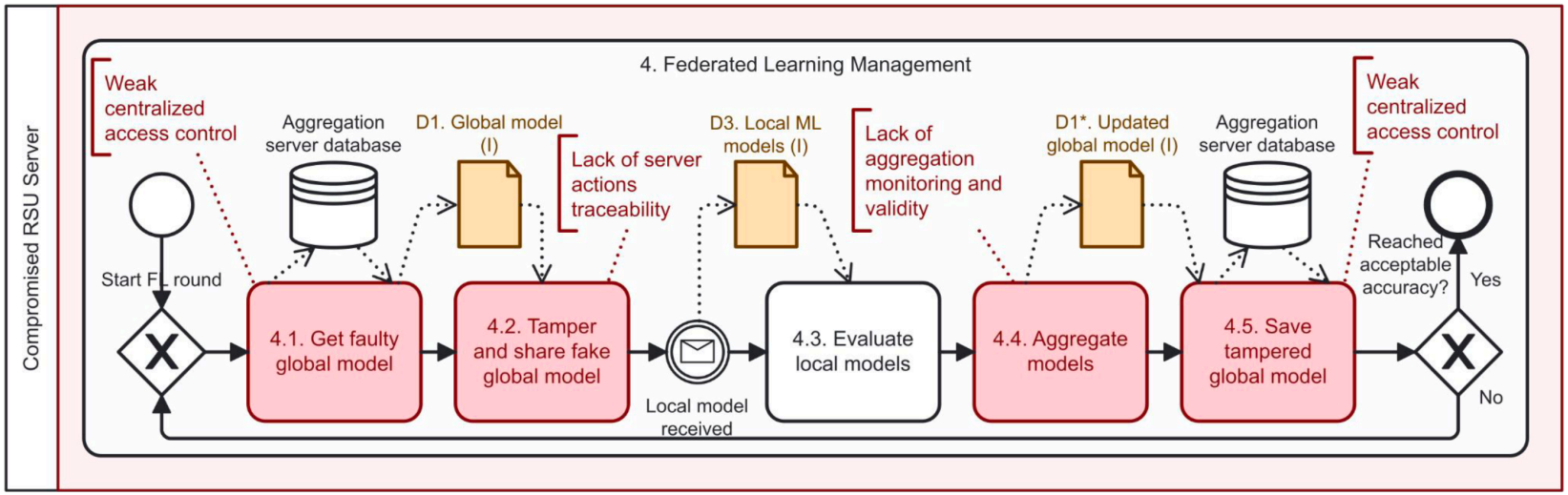


Model Aggregation Poisoning Attack



Model Aggregation Poisoning Attack (detailed)

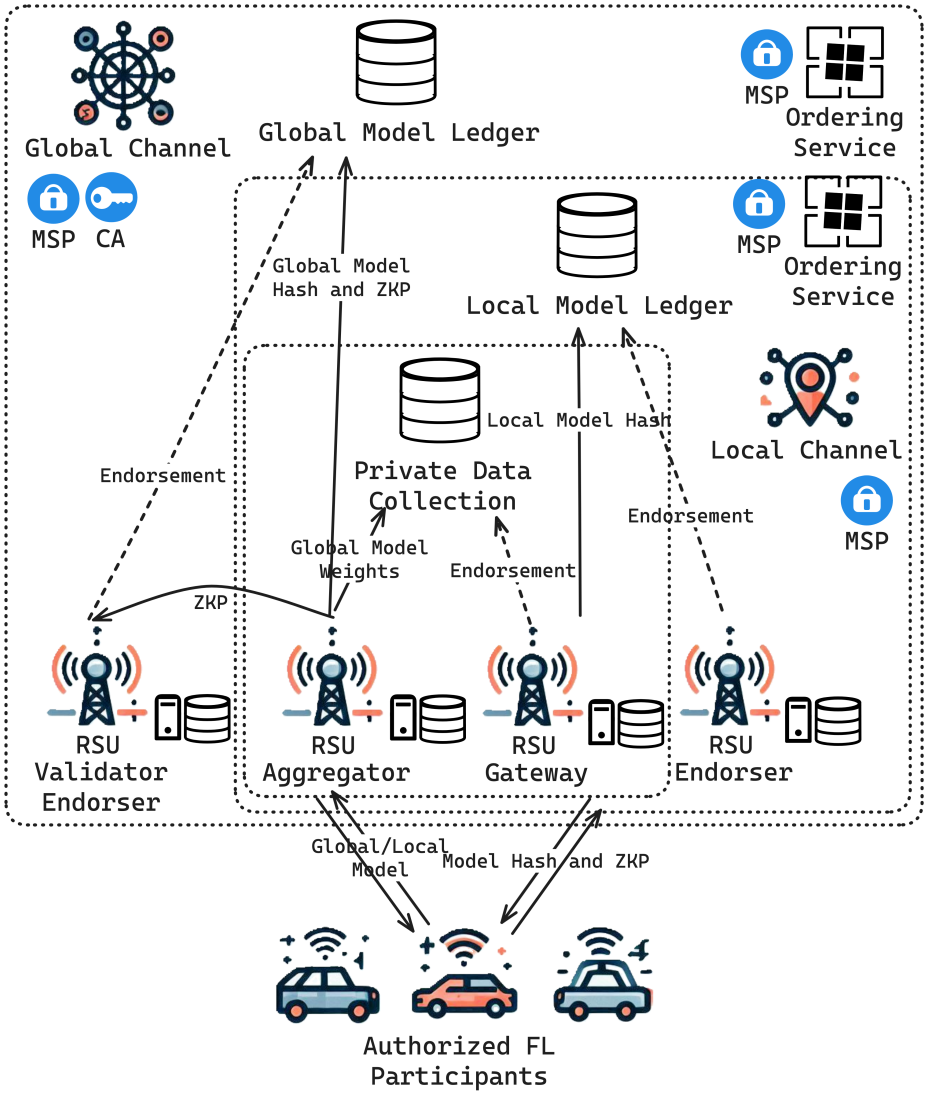




Blockchain-based Countermeasures

Hyperledger Fabric:

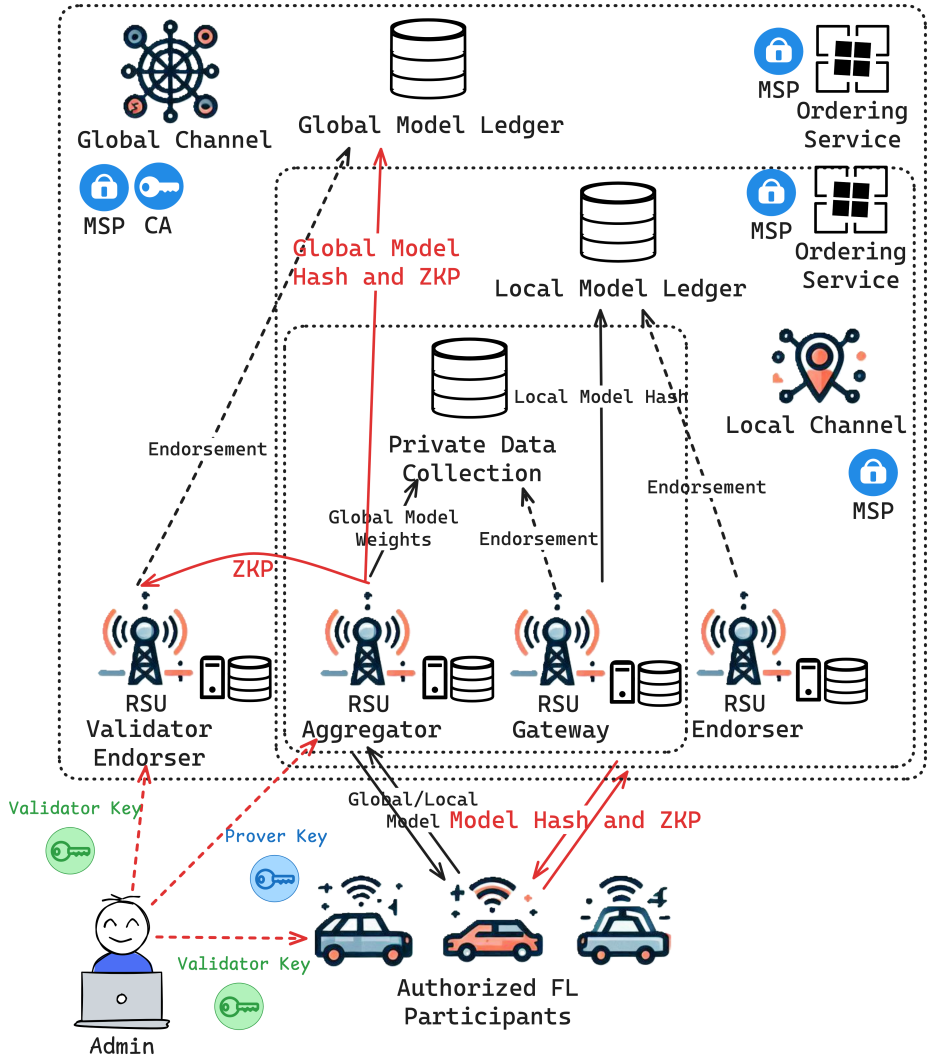
- Membership Service Provider (MSP)
- Endorsement Policies
- Channels
- Ordering Service



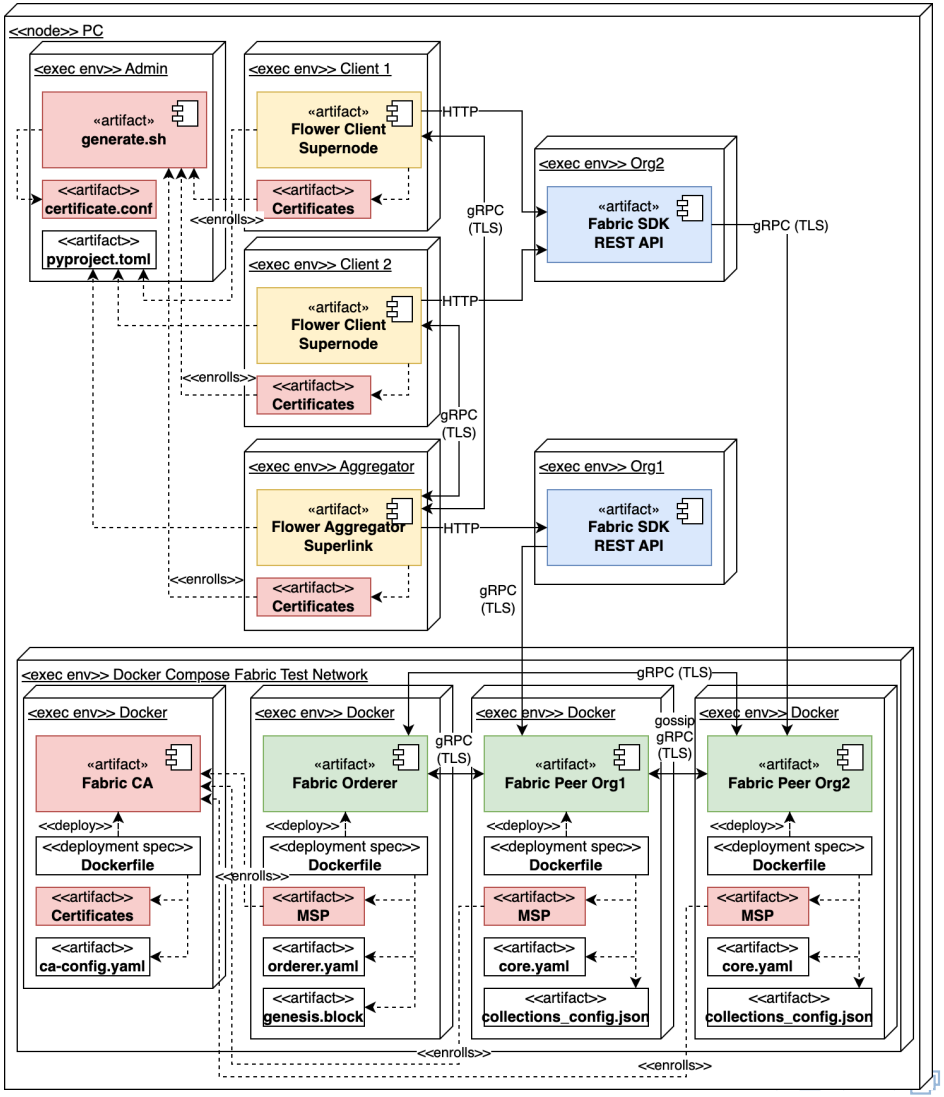
ZKP Countermeasures

ZKP process:

1. Setup by admin
2. Prove by RSU aggregator
3. Validate by vehicles or other RSUs



PoC Deployment + DEMO



Conclusions

Results:

- Security analysis of centralized FL in the IoV
- Blockchain-based solution with ZKP validation
- PoC implementation with open-source code

Further development:

- Security analysis of blockchain-based solution
- Scalability analysis