Privacy protection and performance enhancement in IoT applications using Blockchain and machine learning techniques

How do the combination of machine learning and blockchain impact privacy and performance in IoT data management?

1 - Background

- Significant increase in data generated by Internet of Things (IoT) [1]
- Blockchain (BC) and Machine Learning (ML) have the potential to improve privacy in IoT data management [2]

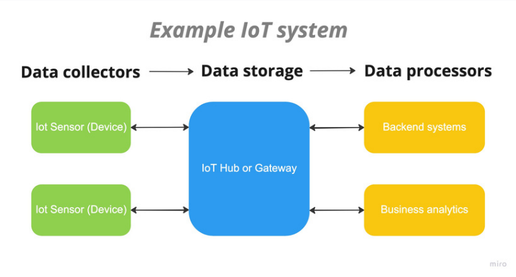

Figure 1. IoT data flow

2 - Related works

- Privacy leakage and pseudonymity risks when an adversary analyses data with DL
- Consensus mechanisms of BC have a high impact on the performance of an IoT application
- Potential solutions to various privacy threats have already been proposed using either BC or ML, fewer solutions with BC-ML integrations
- Proposed setup for Industrial IoT applications (Fig. 2)

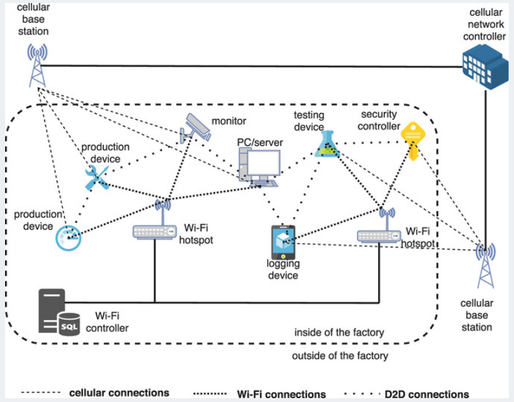

Figure 2. Proposed IIot network by Wu et al. [3]

3 - Review findings

- All solutions improve confidentiality and performance
- Transparency is hard in combination with confidentiality
- Frameworks lay a good privacy-preserving basis with performance improvements

Paper	Confidentiality	Anonymity	Transparency	Consent Management	Performance
PPDC [12]	●	●	●	○	◐
secureSVM [13]	●	◐	○	◐	◐
PPSF [6]	◐	◐	○	○	●
BC Federated Learning [14]	●	◐	○	●	◐
IoT healthcare FL + BC [15]	◐	○	○	○	◐

No: ○, Partially: ◐, Yes: ●

Table 1. Review of state-of-the-art solutions by metrics

4 - Future work

- Transparency in privacy-preserving solutions
- Full anonymity while an authority admits new nodes
- Impact of Consent Management on data quality for training ML models
- Implementing new applications on a BC-ML empowered IoT framework

5 - Conclusion

- State-of-the-art solutions on BC-ML IoT applications reviewed
- Integrations of BC and ML can improve privacy and performance in IoT networks
- Future research directions insightful for researchers to guide future work

References

1] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2020.
[2] N. Waheed, X. He, M. Ikram, M. Usman, and S. Hashmi, "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," ACM Computing Surveys, vol. 53, pp. 1–37, 12 2020.
[3] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial iot: A survey," Computer Networks, vol. 191, p. 108004, 2021. [Online].

Author Jeroen Janssen **Contact** J.D.Janssen@student.tudelft.nl

TU Delft

Supervisor Chhagan Lal **Responsible Professor** Mauro Conti