MITIGATING **IOT DATA MANAGEMENT SECURITY** CONCERNS THROUGH **BLOCKCHAIN** AND **MACHINE LEARNING** BASED SOLUTIONS: STUDY AND CONCEPTUAL DESIGN

Author: Lars van den Eeden, l.vandeneeden@student.tudelft.nl - Supervisor: Chhagan Lal, Responsible Professor: Mauro Conti

1 - INTRODUCTION

- Security breaches and advanced attacks on the internet of things (IoT)
- Confidentiality, Integrity, Availability (CIA)
- Blockchain and Machine Learning (ML)

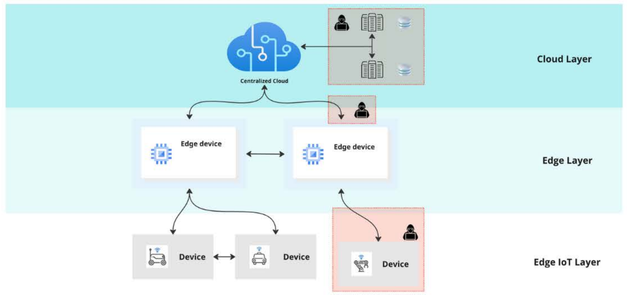

Figure 1. IoT Attack vectors

2 - BACKGROUND

Research Question:
How can we use Blockchain and machine learning (ML) based solutions to address security concerns in IoT data management?

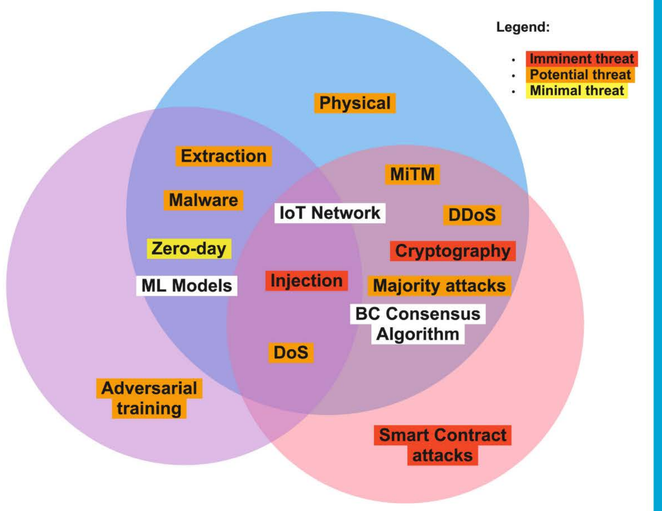

Figure 2. Different types of attacks, showcasing per domain

Findings
Many ML-based **IDS solutions**
Works **lack full analysis** on:
Security & Privacy
BC & ML

Future research
Storage and **Computation**
Specialized BC solutions
Focus on **privacy**

Figure 3. Reviewed surveys, findings and future research, summarized

3 - FINDINGS

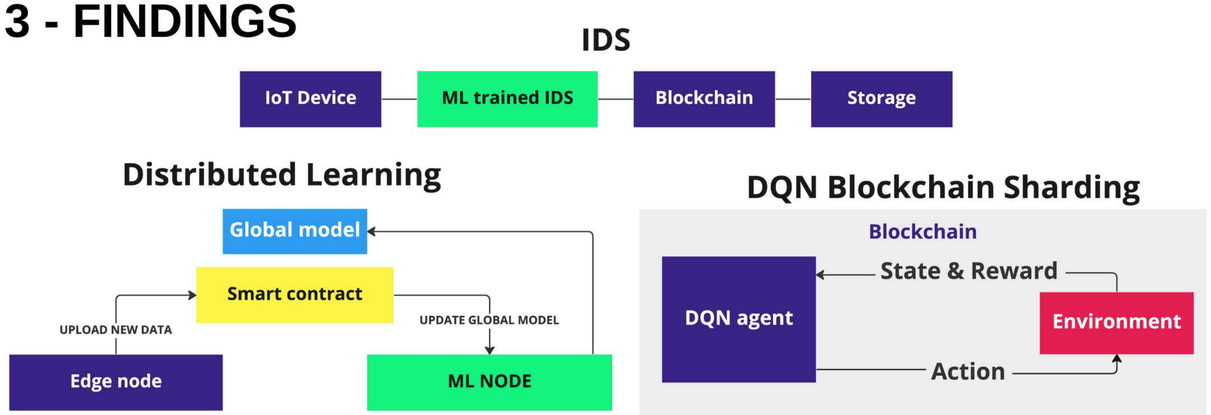

Figure 4. Different types of BCML integrations from surveyed papers

	Rahman et al.	Yun et al.	Rabienejad et al.	Rathore et al.	Alkadi et al.	Centralized IoT
Confidentiality	◑	●	○	◕	○	◔
Integrity	◑	◕	○	◕	○	◑
Availability	●	●	◕	◕	○	◕
Decentralization	◔	◑	●	◕	◕	○
Scalability	◔	◑	◕	●	◔	●
Latency	○	○	○	○	○	●
Energy Efficiency	◕	●	◕	●	◕	●
ML effectiveness	◕	●	◑	◑	◑	○

Table 1. Summarized analysis [1] [2] [3] [4] [5]

4 - PROPOSED DESIGN

DQNSB scheme with global IDS training and ML-based Smart Contract audits

DQNSB-based solution

IoT
- ✓ 1300 TPS minimum
- ✓ Energy efficient
- ✖ Unknown latency
- ✖ Limited scalability

Security
- ✓ Access control
- ✓ Global ML model training
  - Confidential IDS alerts
  - Smart contract audits
  - Model audits
- ✓ Secure to 21 / 24 attacks
- ~ Semi decentralized
- ~ Semi confidential

Future proof
- ✓ Modular
- ✖ Quantum resistance

Figure 5. Advantages and limitations of the proposed design

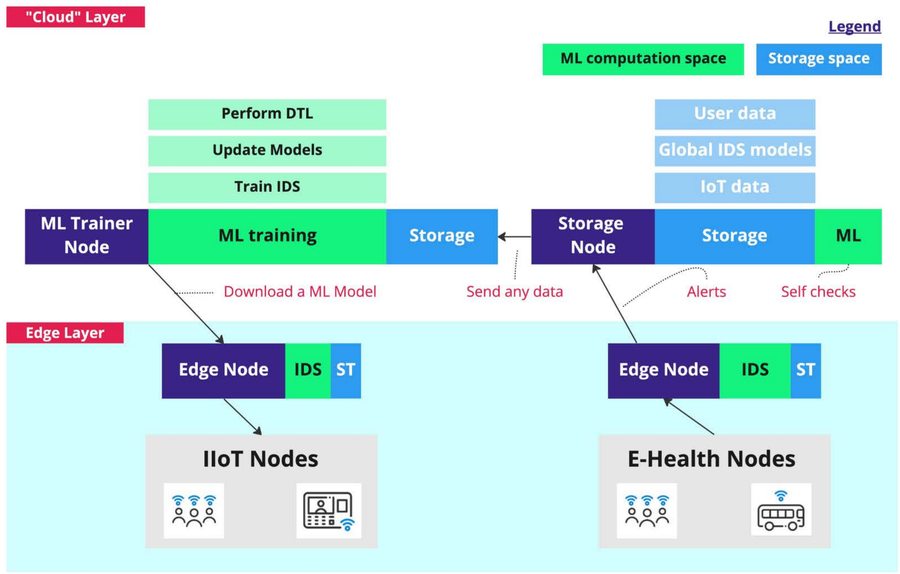

Figure 6. Proposed Design: four nodes assisting each other to collectively train IDS models.

5 - DISCUSSION

- Many IDS systems
  - DRL, DTL, DNN, Bi-LSTM
- Dataset use quality
- Some papers lack thorough analysis
- Problems for different sectors
- GDPR rules

6 - DIRECTIONS

- Multi-Domain ML
- Energy efficient system
- Zero Knowledge (zk) rollups
- (zk) Verifiable model inference
- Quantum technology
- Latency

7 - CONCLUSION

- Aim of the project
- IoT attack vectors
- Higher security with BCML
- Blockchain trilemma discussion
- Challenges in the field

REFERENCES

[1] Rahman, Ziaur & Yi, Xun & Khalil, Ibrahim. (2022). Blockchain-based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. IEEE Internet of Things Journal. 1-1. 10.1109/JIOT.2022.3147186.
[2] J. Yun, Y. Goh and J. -M. Chung, "DQN-Based Optimization Framework for Secure Sharded Blockchain Systems," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 708-722, 15 Jan.15, 2021, DOI: 10.1109/JIOT.2020.3006896.
[3] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Secure AI and Blockchain-enabled Framework in Smart Vehicular Networks," 2021 IEEE Globecom Workshops (GC Wkshps), 2021, pp. 1-6, DOI: 10.1109/GCWkshps52748.2021.9682140.
[4] S. Rathore and J. H. Park, "A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5522-5532, Aug. 2021, doi: 10.1109/TII.2020.3040968.
[5] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463–9472, 2021.