Machine Learning-based Techniques for Secure and Efficient IoT Data Management

Author: Tim Kramer
t.kramer-2@student.tudelft.nl

Supervisor: Chhagan Lal

Responsible Professor: Mauro Conti

TUDelft

1 - Background

Internet of Things (IoT) device number is growing to 30 billion by 2030 [1]

IoT in critical infrastructure: e.g. healthcare, energy, autonomous vehicles, government

Resource constraints, different protocols, etc. make traditional security methods less suitable. [2]

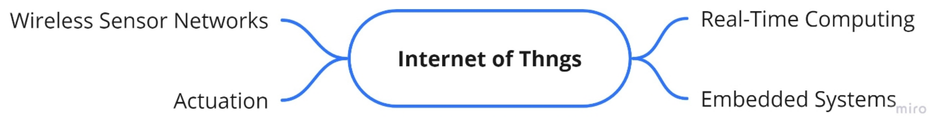

Figure 1: IoT convergence [2]

IoT Attack Vectors

layers: physical, mac, network, transport and application layer

passive: eavesdropping

active: (D)DoS, proxy, MitM, code/data injection, APT

Machine Learning

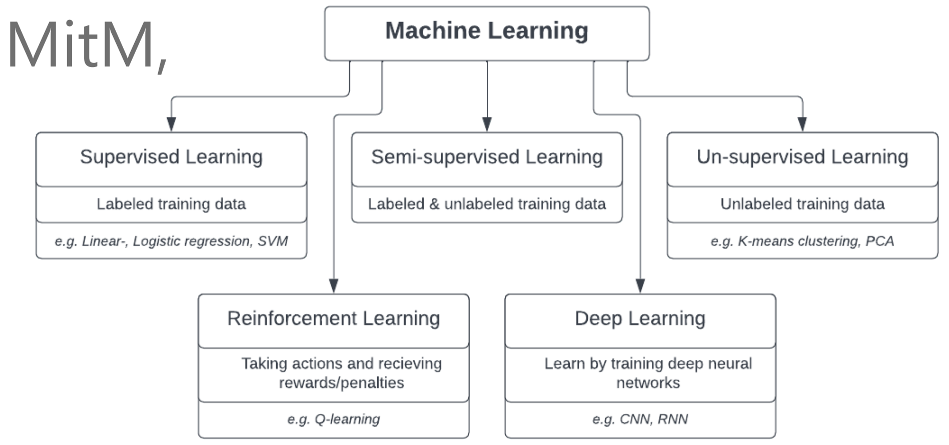

Figure 2: ML Algorithm Types

2 - Research Question

How does the use of Machine Learning methods support secure and efficient IoT data management?

3 - Methodology

Literature Review

Survey of Surveys

Study of SotA ML IoT Sec

Open Limitations

4 - Related Work

Survey, Year	Specialization	Security	Efficiency	Privacy
[3], 2020	General	●	●	●
[6], 2020	General	●	○	●
[7], 2022	APT	●	○	○
[8], 2022	RTS	○	●	○
[9], 2022	ML-based attacks	◑	○	●

Table 1: Survey of surveys

5 - State-of-the-art: ML-based IoT Security

Metrics for evaluation of IoT and ML: CIA, ML-Score, Scalability, ...

General Techniques for

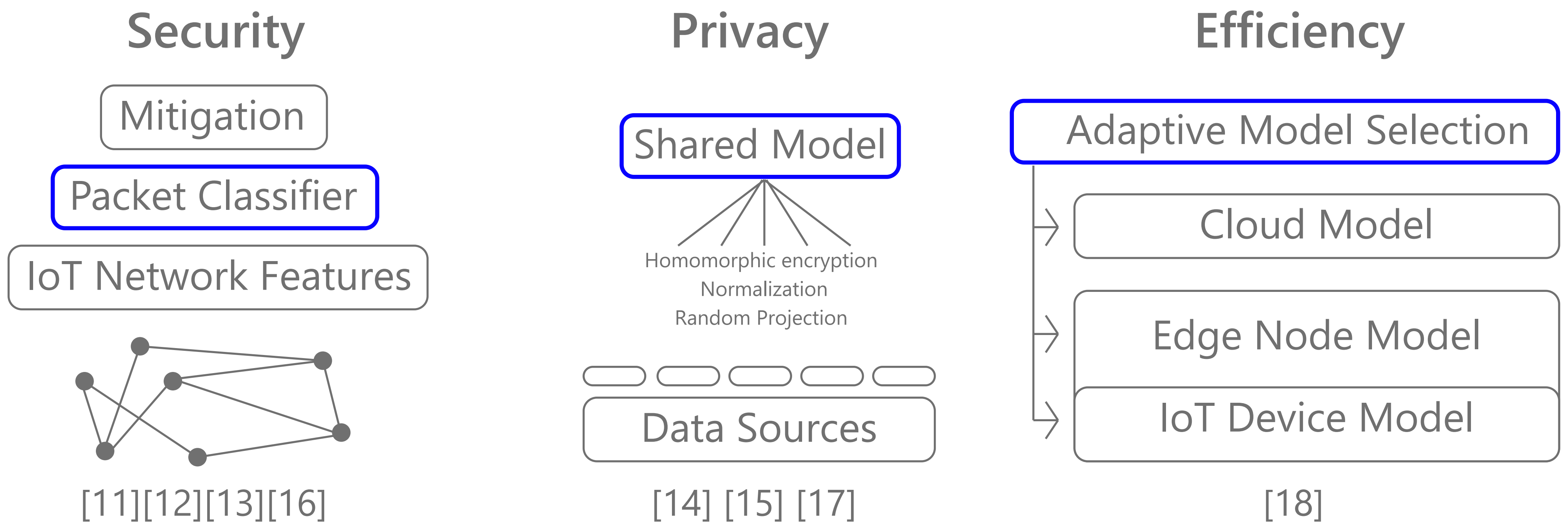

Figure 3: ML-based IoT Solution Structure

Paper, Year, Author	CIA	Likelihood	Damage	ML-Score	Scalability	Computational Cost
[11], 2018, Doshi	A	◕	◕	●	●	○
[12], 2019, Hamad	C, A, I	◑	●	●	◕	◑
[13], 2020, Kayode	C, I	○	●	●	◑	◑
[14], 2021, Zhu	C	◑	◑	●	●	●
[15], 2021, Jiang	C	◑	◑	◑	●	○
[16], 2021, Chowdhury	I, A, C	○	●	●	○	◑
[17], 2021, Jourdan	C	◑	◔	◕	◑	◑
[18], 2022, V. Ngo,	I, C	●	◔	●	●	◕

Table 2: Comparison of studied state-of-the-art methods

6 - Discussion

- High accuracy of ML detection methods
- Good scalability of most approaches
- Some work well in Real-Time Systems
- High resource consumption for privacy preserving methods
- Imbalanced and homogenous data sets used for some papers

7 - Future Work and Conclusion

- Dataset availability and balance
- Targeting multiple attack vectors
- Computational limitations
- Preserving privacy

Promising further use of ML for IoT security and efficiency

References

[1] Lionel Sujay Vailshery. Iot connected devices by use case 2030, Nov 2022.; [2] Ismail Butun, Patrik Osterberg, and Houbing Song. Security of the internet of things: Vulnerabilities, attacks,and countermeasures. IEEE Communications Surveys amp; Tutorials, 22(1):616–644, 2020; [4] Ismail Butun, Patrik Osterberg, and Houbing Song. Securityof the internet of things: Vulnerabilities, attacks,and countermeasures. IEEE Communications Surveysamp; Tutorials, 22(1):616–644, 2020.; [7] Zhiyan Chen, Jinxin Liu, Yu Shen, Murat Simsek, BurakKantarci, Hussein T. Mouftah, and Petar Djukic.Machine learning-enabled iot security: Open issues andchallenges under advanced persistent threats. ACMComputing Surveys, 55(5):1–37, 2022.; [8] Jiang Bian, Abdullah Al Arafat, Haoyi Xiong, Jing Li,Li Li, Hongyang Chen, Jun Wang, Dejing Dou, andZhishan Guo. Machine learning in real-time internet ofthings (iot) systems: A survey. IEEE Internet of ThingsJournal, 9(11):8364–8386, 2022.; [9] Emilie Bout, Valeria Loscri, and Antoine Gallais. Howmachine learning changes the nature of cyberattacks oniot networks: A survey. IEEE Communications Surveysamp; Tutorials, 24(1):248–279, 2022.; [11] Rohan Doshi, Noah Apthorpe, and Nick Feamster. Machinelearning ddos detection for consumer internet ofthings devices. 2018 IEEE Security and Privacy Workshops(SPW), 2018.; [12] Salma Abdalla Hamad, Wei Emma Zhang, Quan Z.Sheng, and Surya Nepal. Iot device identification vianetwork-flow based fingerprinting and learning. 201918th IEEE International Conference On Trust, SecurityAnd Privacy In Computing And Communications/13thIEEE International Conference On Big Data ScienceAnd Engineering (TrustCom/BigDataSE), 2019.; [13] Olumide Kayode and Ali Saman Tosun. Deep qnetworkfor enhanced data privacy and security of iottraffic. 2020 IEEE 6th World Forum on Internet ofThings (WF-IoT), 2020.; [14] Liehuang Zhu, Xiangyun Tang, Meng Shen, Feng Gao,Jie Zhang, and Xiaojiang Du. Privacy-preserving machinelearning training in iot aggregation scenarios.IEEE Internet of Things Journal, 8(15):12106–12118,2021.; [15] Linshan Jiang, Rui Tan, Xin Lou, and Guosheng Lin.On lightweight privacy-preserving collaborative learningfor internet of things by independent random projections.ACM Transactions on Internet of Things,2(2):1–32, 2021.; [16] Morshed Chowdhury, Biplob Ray, Sujan Chowdhury,and Sutharshan Rajasegarar. A novel insider attackand machine learning based detection for the internetof things. ACM Transactions on Internet of Things,2(4):1–23, 2021.; [17] Theo Jourdan, Antoine Boutet, Amine Bahi, and CaroleFrindel. Privacy-preserving iot framework for activityrecognition in personal healthcare monitoring. ACMTransactions on Computing forHealthcare, 2(1):1–22,2021.;[18] Mao V. Ngo, Tie Luo, and Tony Q. Quek. Adaptiveanomaly detection for internet of things in hierarchicaledge computing: A contextual-bandit approach. ACMTransactions on Internet of Things, 3(1):1–23, 2022.