



LinkedIn

Investigating the Security Issues of IoMT Attacks Using Machine Learning Techniques



Badeea Al Sukhni¹, Soumya K. Manna¹, Jugal Dave^{1,2}, Leishi Zhang¹

¹School of Engineering, Technology and Design, Canterbury Christ Church University, Canterbury, Kent CT1 1QU, UK

² Directorate of Research and Publications, Rashtriya Raksha University, India

INTRODUCTION

The Internet of Medical Things (IoMT) plays a significant role in the healthcare system as it improves effectiveness and efficiency of treatment by continuously monitoring patients using smart home sensor and wearables (Fig. 1). Using these information gathered from Internet of Medical Things (IoMT) devices, early disease diagnosis can be made, assisting doctors to choose the best course of action and acting promptly when necessary [1]. Additionally, it helps to reduce the number of hospital visits, limiting carbon footprint.

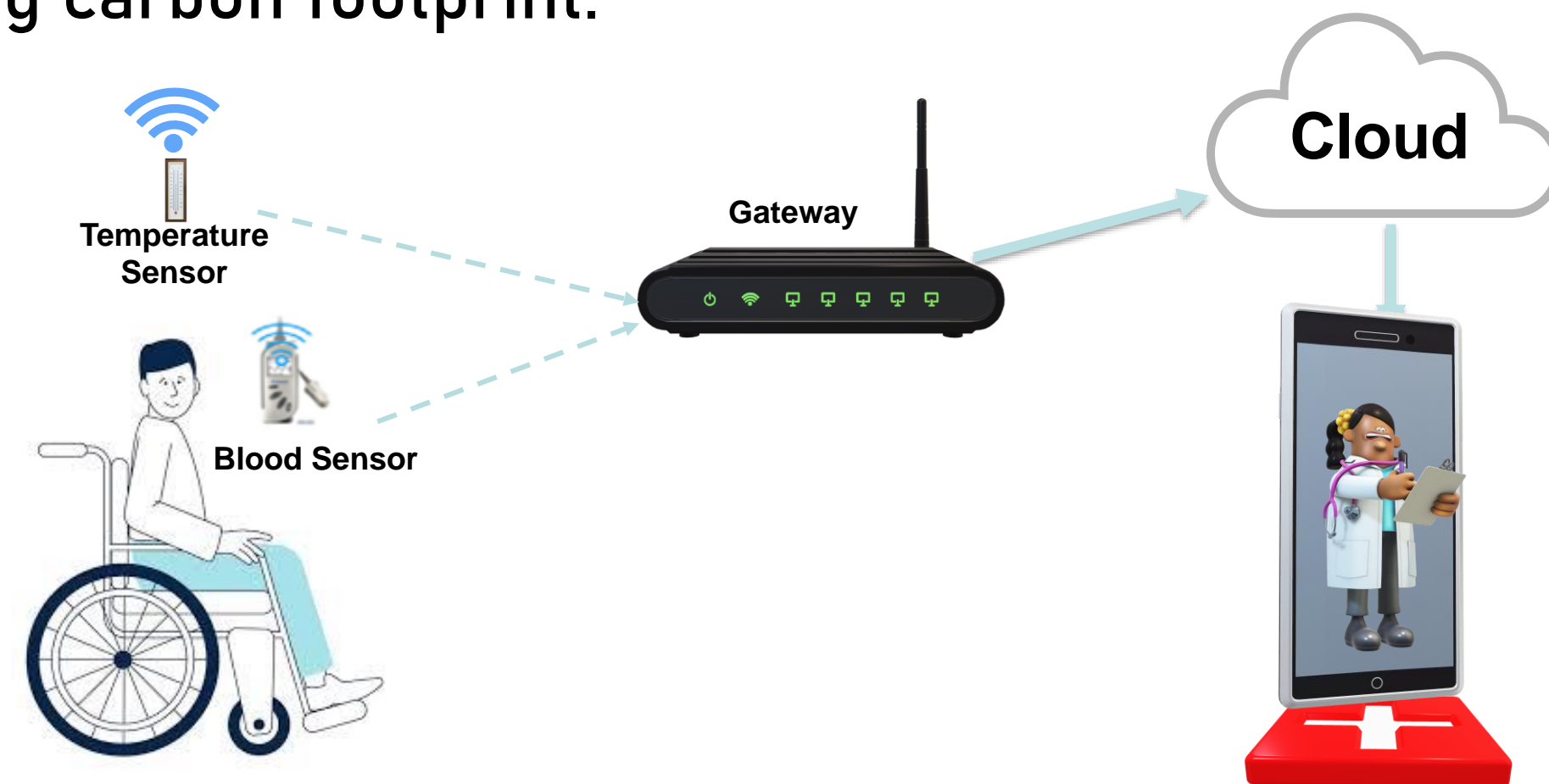


Figure 1: The IoMT Application

IoMT devices are vulnerable to Multi-layer attacks because most of these devices are resource-constrained and portable hence lack of security features in these devices making them a prime target for intruders to steal patients' sensitive information [1].

Multi-layer attacks are a group of attacks exploiting multiple layers of IoMT architecture (Fig. 2) for example DDoS and MITM attacks, for instance, can target the three layers of the IoMT system and lead to serious consequences [2].

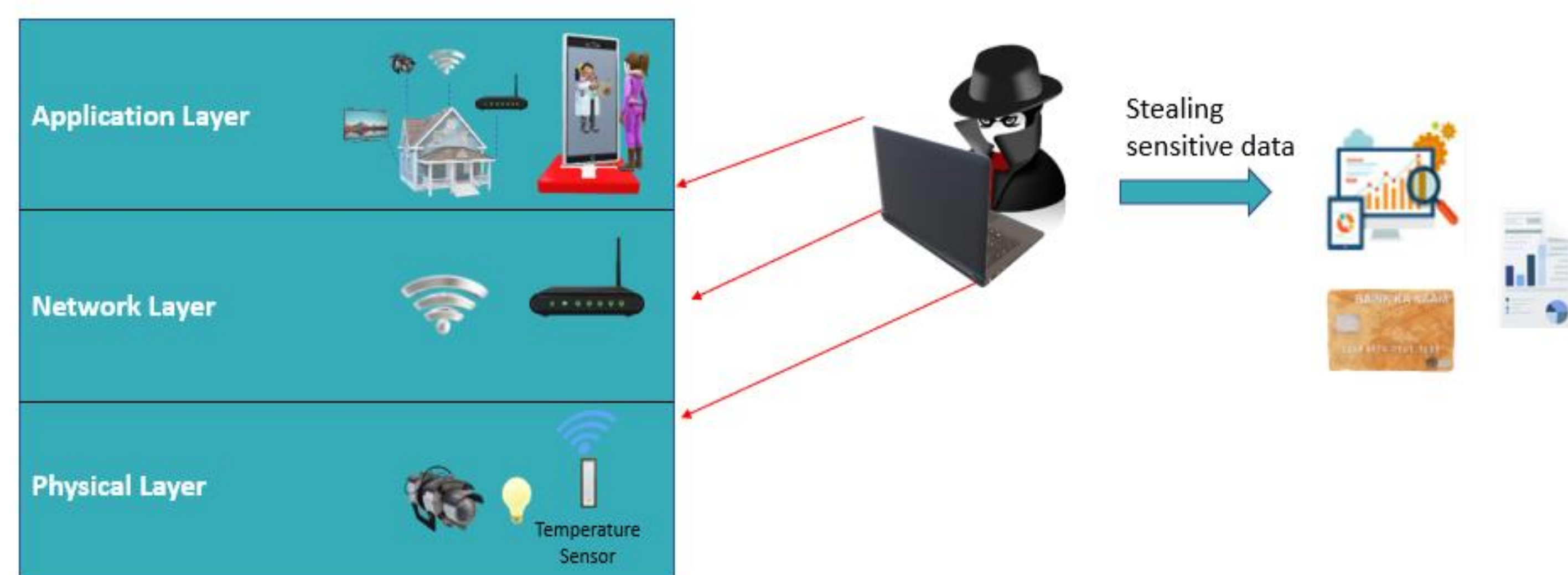


Figure 2: Multi-layer attacks on IoMT architecture

OBJECTIVES

The main aim of the project is to create a robust IDS for IoT devices. To achieve this aim, we have focused on these objectives:

- Understanding the IoMT architecture and its structural loopholes.
- Identifying MultiLayer security attacks and their behavioral patterns.
- Investigating different types of machine learning (ML) techniques with the associated datasets to secure IoMT devices against multilayer attacks.

FINDINGS

After reviewing the existing surveys on multilayer IoT attacks, our research (Fig. 3) is focused on distinguishing the multilayer attacks from single layer attacks.

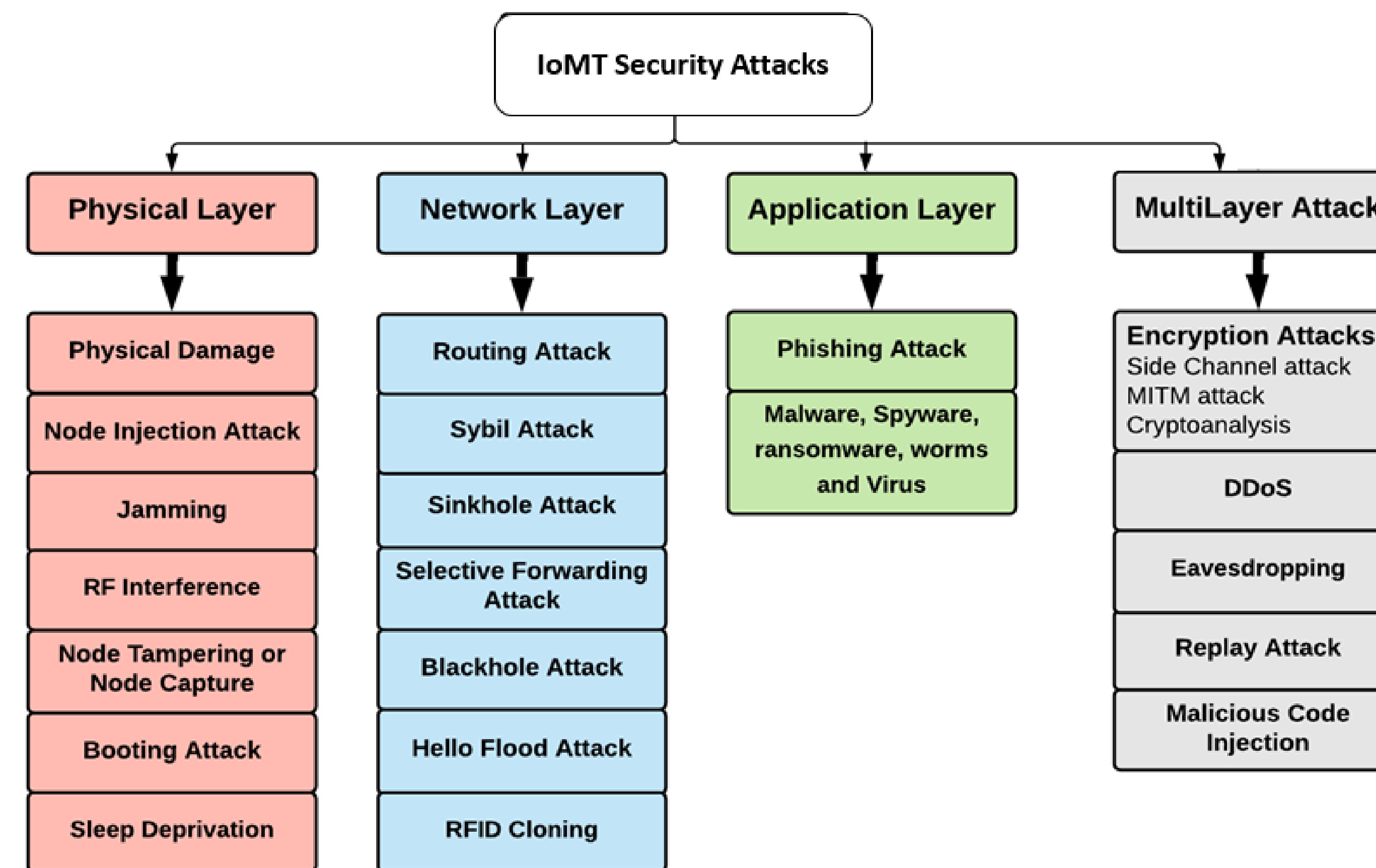


Figure 3: The IoMT Security attacks including multi-layer attacks.

Machine learning models use adaptive algorithms to discover complex patterns from dataset, and can be utilized to develop effective Intrusion Detection Systems for IoT devices and services (Fig. 4).

Ref.	Attacks and Layers	Dataset	ML Algorithm	Features	Accuracy
Doshi et al. [3]	DDoS attacks on the network layer	own dataset	KNN, SVM, DT, RF, and DNN	5	99%
Moustafa et al. [4]	Botnet attacks on the application layer	UNSW-NB15 and NIMS botnet	NB, DT and ANN	36	98.29% - 99.54%
Shafiq et al. [5]	DDoS attacks on the network layer	Bot-IoT	NB, RF, DT, BN, and RF	44	99.79%
Liang et al. [6]	DDoS attacks on the network layer	NSL-KDD	DNN	41	98%
Hady et al. [7]	MITM on the network layer	own dataset	RF, DNN, SVM, and ANN	34	92%

Figure 4: Attacks, layers, datasets, ml, features and the number of features considered in some of the reviewed studies

The researchers generated their own testbed datasets or deployed publicly available datasets however not all of these datasets such as Bot-IoT, ToN-IoT, Edge-IIoT etc are related to IoT environments.

METHODOLOGY

Currently, we investigate the existing IoT datasets to find the significant features of multi-layer attacks. We aim to develop a novel computational framework by investigating the similarities in the features of multi-layer attacks for training ML models that would help us to detect multi-layer attacks efficiently (Fig. 5).

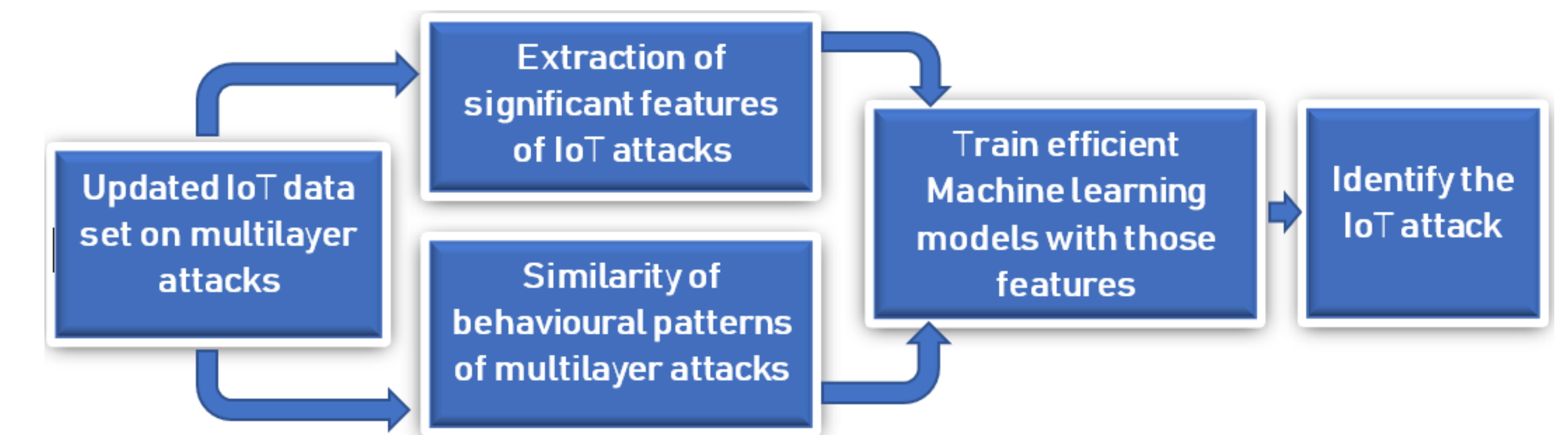


Figure 5: The research methodology

DISCUSSION and CONCLUSION

Despite the advantages of many of the recent ML approaches and the high detection accuracy in identifying and detecting Multi-layer attacks, there are gaps and challenges still exist.

- For instance, some of the ML models are less flexible in detecting new types of attacks or attacks that are targeting new devices.
- It is essential to obtain up-to-date datasets with traffic produced by IoMT devices in order to develop anomaly detection systems that will be able to profile the legitimate traffic for IoMT devices.

Future Work:

- Investigating and comprehending existing ML models and IoMT datasets in order to identify key aspects of multi-layer attacks
- Developing a novel computational algorithm capable of detecting multilayer attacks by identifying similarities in IoT attack features.

REFERENCES

- [1] Rasool, R.U., Ahmad, H.F., Rafique, W., Qayyum, A. and Qadir, J., 2022. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications*, p.103332.
- [2] Khanam, S., Ahmedy, I.B., Idris, M.Y.I., Jaward, M.H. and Sabri, A.Q.B.M., 2020. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE access*, 8, pp.219709-219743.
- [3] Doshi, R., Aporthe, N. and Feamster, N. (2018) "Machine learning DDoS detection for consumer internet of things devices," in *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*. doi:10.1109/SPW.2018.00013.
- [4] Moustafa, N., Turnbull, B. and Choo, K.K.R., 2018. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, 6(3), pp.4815-4830.
- [5] Shafiq, M. et al. (2020) "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, 107. doi:10.1016/j.future.2020.02.017.
- [6] Liang, C. et al. (2019) "Intrusion Detection System for Internet of Things based on a Machine Learning approach," in *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, VITECoN 2019*. doi:10.1109/VITECoN.2019.8899448.
- [7] Hady, A.A. et al. (2020) "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," *IEEE Access*, 8. doi:10.1109/ACCESS.2020.3000421.