Canterbury Christ Church University

School of Engineering, Technology and Design

Safeguarding IoMT: Semi-automated Intrusion Detection System (SAIDS) for Detecting Multilayer Attacks

Badeea Al Sukhni, Soumya Manna, Jugal Dave, Leishi Zhang

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

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).

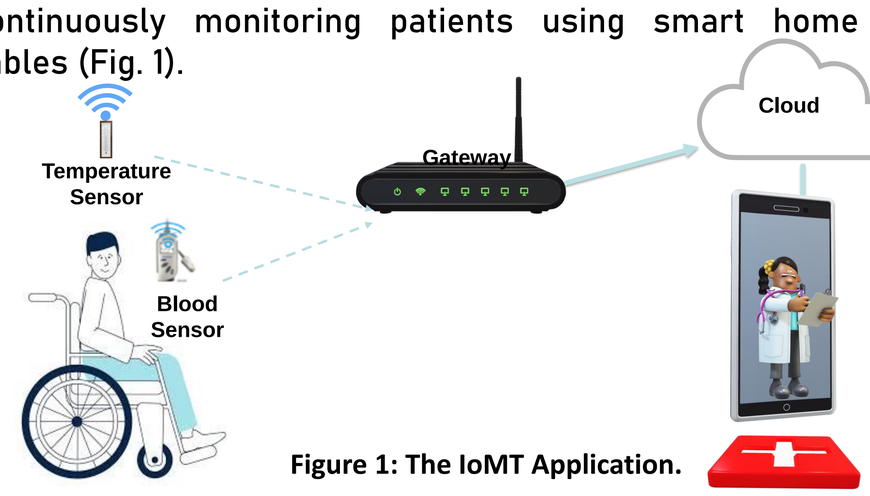

Figure 1: The IoMT Application.

- IoMT devices are vulnerable to Multi-layer attacks that are exploiting multiple layers of IoMT architecture (Fig. 2). Denial-of-service (DoS) and Man-In-The-Middle (MITM) attacks, for instance, can target the three layers of the IoMT system and lead to serious consequences, such as theft of patients' sensitive data and reputational damages [2].

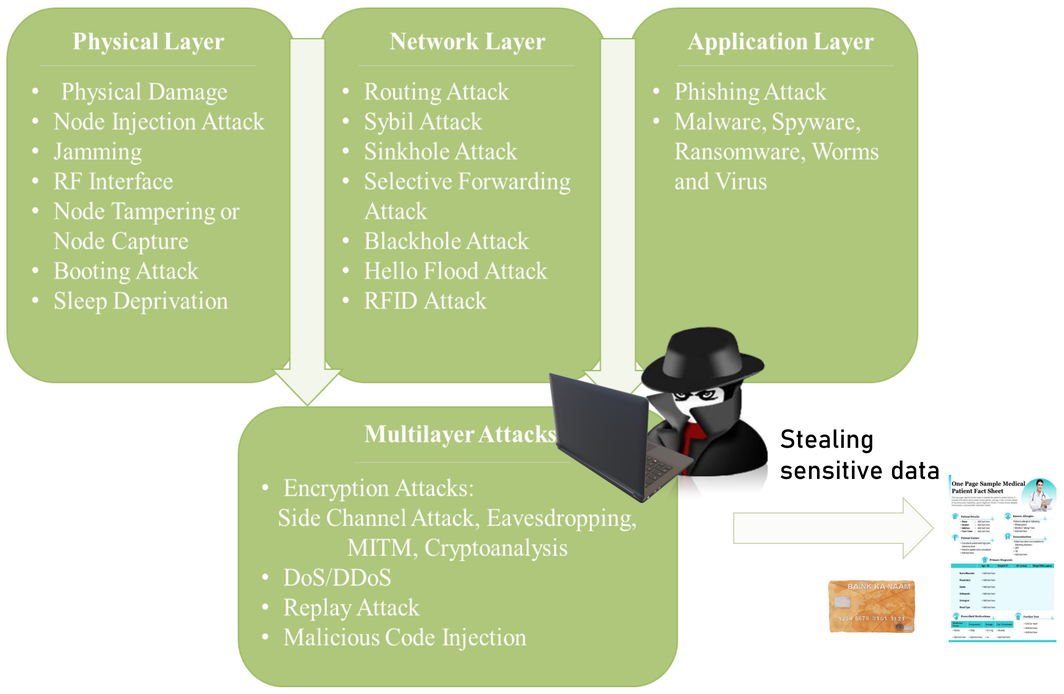

Figure 2: The IoMT Security attacks including multi-layer attacks.

OBJECTIVES

This project aims to create a robust detection system for multilayer attacks using a Semi-automated Intrusion Detection System (SAIDS) for IoT devices. To achieve this aim, we have focused on the following objectives:

- Explore a variety of feature selection algorithms.
- Apply feature weighting.
- Integrating human and machine learning approaches to work together.
- Increase detection efficiency by utilizing significant features.

METHODOLOGY

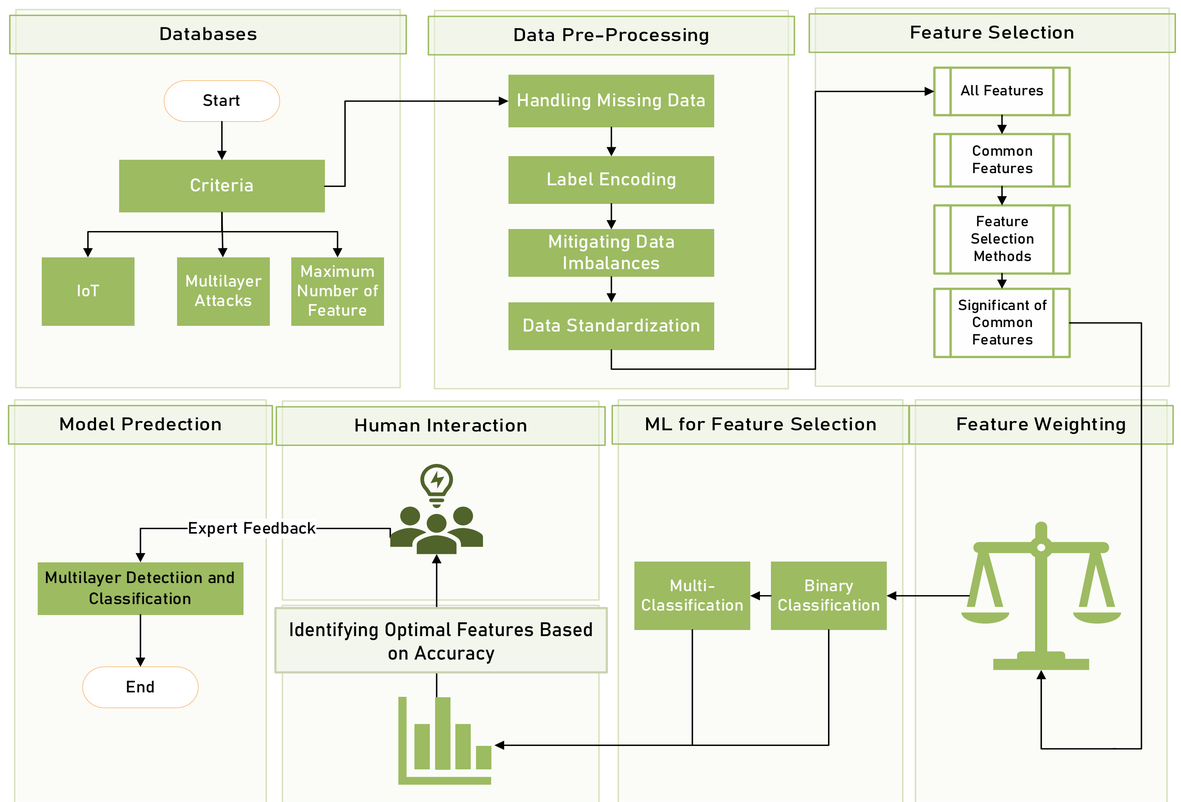

Figure 3: Semi-automated Intrusion Detection System (SAIDS).

FINDINGS

The proposed SAIDS is implemented by utilizing the Edge-IIoTset dataset. It managed to identify an optimal set of 13 significant features for the efficient detection and classification of multilayer attacks.

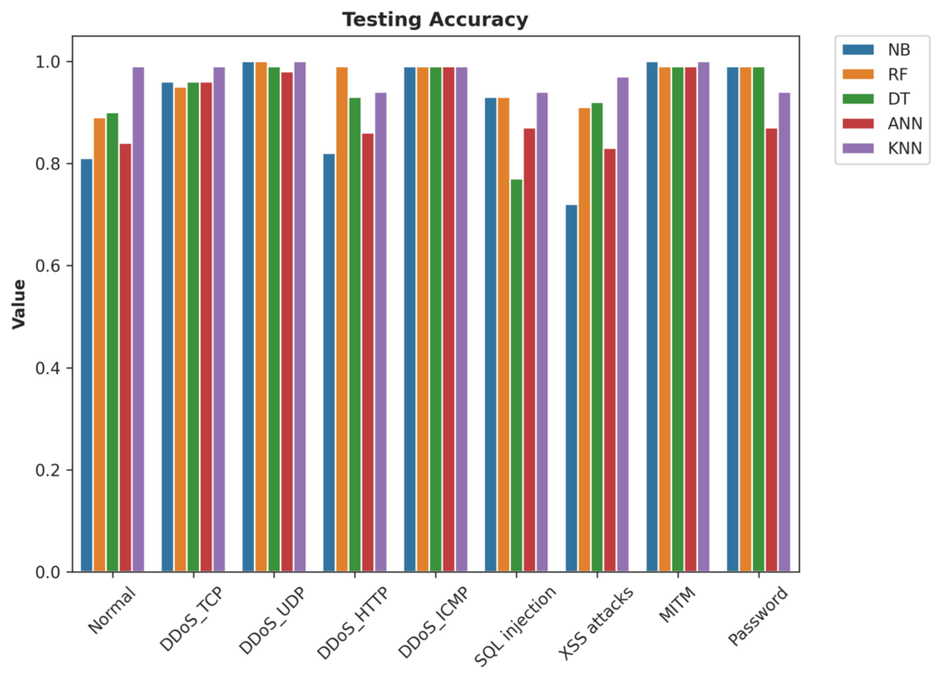

Figure 4: Testing Accuracy using KNN for the 13 Features Sets.

Using SAIDS, we managed to reduce the number of features in the dataset from 62 to 34, identifying those common across multilayer attacks. We then identified an optimal set of 13 significant features as critical for detecting and classifying multilayer attacks. This approach underscores the strengths of both human judgment and algorithmic precision, enhancing the overall efficacy of the IoT multilayer detection system.

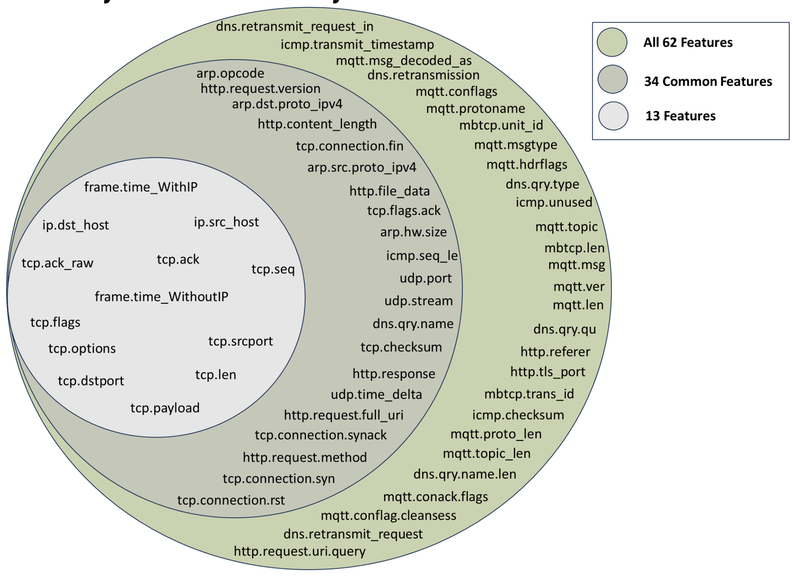

Figure 5: All features, 34 common features and 13 Features Sets.

Future Work:

- Exploring the integration of more advanced machine learning and artificial intelligence techniques, such as deep learning, reinforcement learning, federated learning, and transfer learning.
- Real-time implementation.

LEARN MORE ABOUT IOT MULTILAYER SECURITY

[1] Al Sukhni, B., Dave, J.M. and Zhang, L. (2022) Investigating the security issues of multi-layer IoT attacks using machine learning techniques. IEEE, pp. 1.

[2] Al Sukhni, B., Manna, S.K., Dave, J.M. and Zhang, L. (2022) Machine learning-based solutions for securing IoT systems against multilayer attacks. Springer, pp. 140.

Google Scholar

Contact: b.alsukhni331@canterbury.ac.uk