Meta-IDS: Meta-Learning-Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network-Key Insights

Abstract

- The IoMT enhances healthcare but poses security risks due to internet dependence.
- Meta-learning allows systems to adapt and learn from past experiences for better threat detection.
- Meta-IDS effectively detects zero-day attacks that lack known patterns.
- The system combines signature-based and anomaly-based detection for comprehensive security.
- Meta-IDS demonstrated high performance in accuracy and low error rates compared to existing models.

Introduction

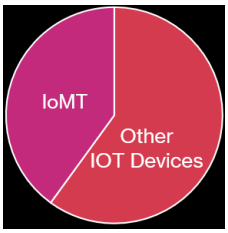
- The number of IoT devices is expected to exceed 27 billion by 2025, indicating rapid technological advancement.(However, upon reviewing the reference they cited, it actually states that the correct figure is **38.6 billion**.)

  according to "R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "A comprehensive deep learning benchmark for IoT IDS," *Comput. Secur.*, vol. 114, Mar. 2022, Art. no. 102588."

  A comprehensive deep learning benchmark for IoT IDS – ScienceDirect

  > The growth of IoT devices is unprecedented. The projected number of IoT devices in 2025 is 38.6 billion, reaching 50 billion by 2030 (Karieetal., 2020). IoT devices' ability to gather

- IoMT devices constitute a significant portion of IoT which makes up about 30% to 40% of all IoT devices, offering improved healthcare but also introducing security risks.



- Vulnerabilities in medical devices can lead to serious security breaches, highlighting the need for effective countermeasures.

- Traditional intrusion detection systems are inadequate against new and sophisticated cyber threats, necessitating innovative solutions.
- The proposed Meta-IDS aims to enhance security in IoMT by utilizing machine learning techniques for real-time threat detection and prevention

Related Work

- The IoMT network's vulnerability to cyberattacks can have dire consequences, including patient safety risks.
- Traditional IDS methods are insufficient against advanced persistent threats (APTs) and zero-day attacks.
- ML and DL approaches enhance detection capabilities but often face limitations in real-time applicability and complexity.
- Existing solutions frequently focus on narrow attack categories or specific data sets, reducing their generalizability.
- There is a critical need for hybrid IDS solutions that can effectively identify both known and unknown threats in diverse IoMT settings.

Proposed Methodology

This part details the proposed Intrusion Detection System (IDS) for the Internet of Medical Things (IoMT), employing machine learning (ML) and deep learning (DL) techniques to bolster cybersecurity. The system architecture integrates various health-monitoring sensors and uses messaging protocols such as MQTT and CoAP for effective data management. It encompasses a Meta-IDS architecture, which includes data collection, feature engineering using techniques like SMOTE, and a meta-learning process with hyperparameter optimization. The IDS employs both signature-based and anomaly detection methods, utilizing mean-shift clustering for adaptability. Performance optimization ensures real-time processing, and the system's design is resilient to attacks, safeguarding patient data and maintaining operational efficiency in healthcare settings.

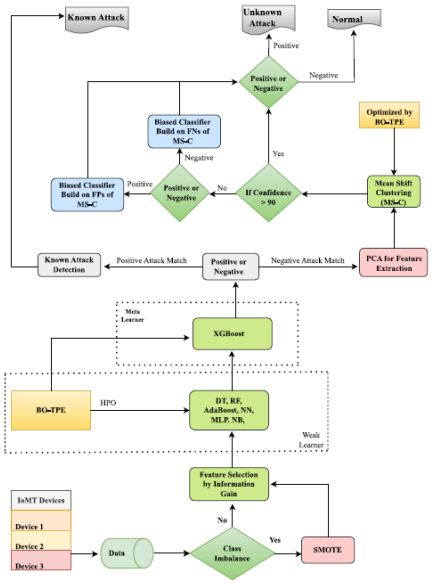


Fig. 2. Proposed framework of Meta-IDS.

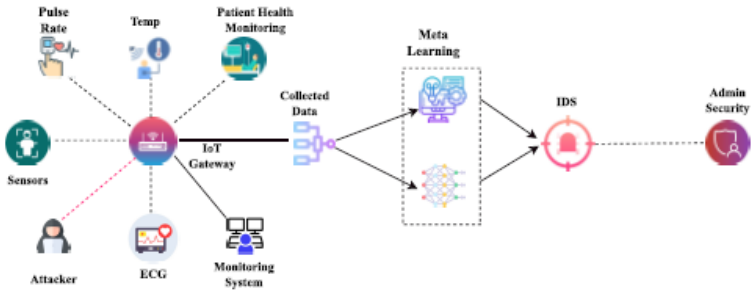


Fig. 1. IoMT-based IDS.

Data set Description

- The choice of data sets is critical for effectively evaluating IDS performance.
- WUSTL-EHMS-2020 emphasizes security within healthcare environments, focusing on patient and network data.
- IoTID20 addresses unique challenges faced in IoT networks, reflecting a variety of cyberattack patterns.
- WUSTL-IIOT-2021 simulates real-world industrial systems, highlighting threats relevant to critical infrastructure.
- The diverse nature of the data sets ensures a comprehensive assessment of the IDS across multiple domains.

Experiment and Performance Evaluation

- The Meta-IDS integrates feature engineering with machine learning algorithms for enhanced performance.
- Hyperparameter optimization significantly contributes to the model's effectiveness in intrusion detection.
- The evaluation metrics used (accuracy, precision, recall, F1-score) provide a comprehensive understanding of the model's performance.
- The methodology effectively mitigates overfitting risks through careful data splitting and cross-validation.
- The model demonstrates exceptional robustness in identifying both known and unknown attacks across diverse datasets.

Discussion

- Meta-IDS effectively combines signature-based and anomaly-based detection for robust security.
- The use of E-GraphSAGE significantly boosts model performance, showcasing the effectiveness of explainable AI.
- Meta-learners provide superior generalizability and help avoid overfitting compared to weak-learners.
- Performance improvements are achieved through the introduction of a biased classifier to enhance detection rates.
- Deployment in real-world scenarios faces challenges related to resource constraints, data privacy, and interoperability.

Conclusion

- The Meta-IDS model effectively detects known and zero-day attacks in IoMT networks.
- Data preprocessing and feature engineering are crucial for improving data quality.
- Hyperparameter optimization significantly boosts the performance of machine learning models.
- The MSCL algorithm helps in identifying zero-day attacks using unsupervised learning.
- The model faces challenges such as environmental sensitivity and evolving cyber threats, indicating the need for further enhancements.