Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.3, May : 2025

DESIGN AND EVALUATION OF AN INTELLIGENT AND EXPLAINABLE SAAS-BASED INTRUSION DETECTION SYSTEM FOR SECURE AND RESOURCE-CONSTRAINED INTERNET OF MEDICAL THINGS (IOMT) ENVIRONMENTS

Prof. Rahul Bambodkar , Professor, Department of Information Technology and Data Science Engineering, JD College of Engineering and Management, Nagpur, Maharashtra, India
Sarika Panchalwar , Akhil Tonge, Janhavi Dabhade, Vanshika Bante, Students, Department of Information Technology and Data Science Engineering, JD College of Engineering and Management, Nagpur, Maharashtra, India

Abstract:
IoT, and specifically IoMT, are revolutionizing the healthcare industry with integrated "connected ecosystems" of medical devices allowing for continuous monitoring, assessment, diagnosis, and information sharing. At the same time but, these advancements come with new cybersecurity threats, particularly in low-resource settings, where devices are often devoid of security features. Conventional Intrusion Detection Systems overlook particular IoMT features such as limited computational resources, highly sensitive data, and requirement of real-time detection of threats. Accordingly, in this review an intelligent explainable SaaS-based IDS architecture that could be deployed specifically for Secure IoMT is suggested. The focus of the system is to use machine learning algorithms that are "light-weight" for deployment in low power devices, and to support them with XAI – explainable artificial intelligence- methods that can foster trust and transparency of the models. We discuss existing IoMT security efforts , summarize important IDS models , and discuss approaches relevant and optimal for SaaS in health networks. Challenges, expected outcomes, and potential future work where such an approach can maximize the accuracy of detecting intrusions without adversely affecting device performance or patient privacy are also discussed. On a broader level, it emphasizes a pressing need for more progressive, user-flexible and understandable cybersecurity options that are not divorced from the realities and ethical obligations of today's medical Internet environment.

1. Introduction

Healthcare is witnessing a digital transformation as it begins to incorporate the internet of medical things . In other words, IoMT is a network of medical devices and applications that connect to healthcare information systems, using networking technologies to offer tailored medical care. IoMT - from health bands, infusion pumps and remote monitoring - is used for diagnostic, treatment and patient data in real time. But the interconnectivity also creates catastrophic cyber security vulnerabilities that can have fatal consequences. Medical data is extremely sensitive and IoMT devices are mission critical, creating an appealing target for attackers.

One such important firewall for attacks has been Intrusion Detection Systems IDS. Nevertheless, conventional IDS paradigms struggle to adapt to IoMT environments because of their complex algorithms and demanding resource consumption. Plus, black-box machine learning models are impenetrable , and they cannot offer healthcare providers any explanation of the logic behind the model's automated decisions.

For all these reasons, this paper aims at reviewing a new concept: and Intelligent and Explainable IDS as a SaaS model specific for resource-constrained IoMT environments. SaaS-type delivery facilitates scalability, centralized updates and cost efficiency; intelligent algorithms enable dynamic threat detection. Using explainable AI , decisions remain transparent and can be relied on, an essential condition in a medical context. This paper presents a comprehensive review of existing IDS technologies applied to healthcare, an implementation framework, and future prospects for improving security in IoMT networks.

2. Literature Review

Intrusion Detection Systems have seen remarkable developments in the last two decades . Signature-based IDSs such as Snort and also anomaly- based schemes have proven good detection rates in conventional networks. But, they are not very effective in IoMT environment, because the medical devices are resource-constrained and heterogeneous.

Machine learning based IDSs have been recently proposed in the existing literature to enhance the detection accuracy. Deep learning algorithms like Convolutional Neural Networks and Recurrent Neural Networks, for instance, have been used for the identification of advanced attacks on smart healthcare systems . But, the huge computing demand and the unexplainability of these models hinder their adoption in real usage scenarios , particularly in the case where human lives are at stake as in patient monitoring. Lightweight models like decision trees and ensemble methods such as Random Forest and XGBoost are among algorithms that provide the most reasonable trade-off between performance and efficiency for resource-constrained applications.

Explainable Artificial Intelligence, or XAI , is now being included in IDS approaches to promote confidence in AI decisions. Examples of interpretability tools that can provide insights into model behavior and have been tested in healthcare analytics include LIME and SHAP . But, few studies have attempted to generalize their application for IoMT specific intrusion detection.

Also, the SaaS approach to deploy IDS in IoMT is still a novel idea. Recent work points to its value in terms of reducing the overhead on the local device and the ability to have continuous updates and maintenance . Promising solutions such as IBM QRadar or Azure Security Center are cloud- based and have not necessarily been tailored for IoMT.

In general, the literature acknowledges the urgent demand for lightweight, intelligent, and explainable IDS dedicated to IoMT. Nevertheless, the large majority of current systems make a trade-off between accuracy and efficiency. Even fewer attempt to combine all three major aspects, resource awareness, intelligence, and explainability, in a SaaS-based approach. The present review intends to fill that space, providing an analysis of strategies that address IoMT constraints as a whole.

3. Methodology

The proposed framework aims to develop an intelligent explainable IDS tailored for IoMT devices , leveraging the capabilities of a SaaS platform to accommodate device limitations. The architecture for the system consists of three main functional components: Data Collection, Intelligent Threat Detection and Explainable Analytics .

1.Data Collection Layer: IoMT devices emit real-time data such as vital signs , device logs , and network traffic . Because of limited resources available at the edge, a lightweight agent acquires and partially processes the data, which is then transferred to the cloud. This not only means less overhead traffic, but that only needed, fully anonymous data, are being processed.

2. SaaS-Based Processing and Detection Engine - The centralized detection engine is cloud-based and available as a Software-as-a-Service product. The engine’s hybrid architecture uses lightweight random forest, naïve Bayes, and KNN ML models optimized with feature selection techniques to reduce computational cost. To implement continual learning instead, one can resort to federated learning as a means of adapting the models without exchanging sensitive information.

3. Explainability and Decision Support Layer: This layer is responsible for the detection results and for providing human readable explanations by integrating XAI tools such as SHAP and LIME . For example, if an anomalous network traffic instance has been detected, the system will display the contribution of each network feature to the decision . It creates transparency and trust for medical practitioners and IT administrators.

There is also a customizable dashboard to visualize alerts, explanations, and performance metrics. It allows role-based access for doctors, cyber security experts and network managers.

From a deployment standpoint, the consideration of containerized microservices organization would assure modularity and help deployment and interoperation with hospital IT infrastructure. It is designed to provide low latency, high availability and also takes healthcare regulations like HIPAA into consideration.

This approach guarantees the ability of the system to not only be able to identify threats, but also being interpretable, and scalable to adjust to highly dynamic healthcare IoT settings.

4. Expected Outcomes

The deployment of an intelligent and explainable SaaS-based IDS approach in IoMT environments is likely to have multiple disruptive impacts on healthcare cybersecurity.

More importantly, the system is expected to provide a significant increase in the accuracy of the intrusion detection while not overloading the resources of IoMT devices. This posed approach leverages the use of light-weight machine learning models and pushes the computational burden to the cloud such that the IDS is able to detect known as well as zero-day attacks in real-time to reduce the attack surface of critical medical infrastructure.

Second, the system's explainability aspect will empower stakeholders to make better decisions. These provide clinicians who are not necessarily security specialists with easy to understand and concise reasoning for how a specific threat was identified. This amounts to trust in the technology itself and would also allow for faster , and better decision making in the event of a real breach in security.

SaaS also allows for seamless updates, scalability, and easy deployment, even in small healthcare practices that might not have an IT department. It also facilitates central monitoring and policy enforcement in multiple locations.

The framework also conforms to data protection and public interest compliance regulations. The IDS also poses very little risk of leaking information through the use, for example, of federated learning and anonymized data transmission.

In essence, the result of the implementation should ultimately lead to a comprehensive security solution that does not compromise on performance or transparency, while being practical. It is intended to become a safe guard that is not reactive to threats but assists health care providers in providing the safe and reliable space that our patients deserve.

5. Challenges

But, while the outlook is promising, there are numerous hurdles that must be overcome in the research phases toward the end of building and deploying such an intelligent and explainable SaaS-based IDS for IoMT in practice.

- Scarce resources and local real time processing: Typically, IoMT devices are limited in terms of CPU, battery and memory resources, for this reason it is not possible to process locally most of the operations required by a detection agent, even a lightweight one. While Software as a Service shifts a portion of this workload to the cloud, internet access reliability and latency become then vitally important issues. One of the challenges of real-time applications in the heathcare domain is to ensure low latency communication while preserving the fidelity of the data.
- Data Privacy and Compliance: Medical data is extremely sensitive and strictly regulated under HIPAA, GDPR, and various national regulations. Uploading anonymized patient data to a cloud-based IDS may even be problematic from a regulatory standpoint. Federated learning and homomorphic encryption can help partially combat this issue, but these techniques are still under development, and can add computing time.
- The Explainability- Complexity Tradeoff. XAI methods tend to sacrifice performance when explanatory accuracy can only be achieved by using simplified applications of complex models. On the other hand, more accurate models, such as deep learning architectures, tend to be less interpretable. The search for the equilibrium between these two aspects is a topic for further research. Research into XAI methods tailored to specific domains, that offer short but relevant explanations for the healthcare staff, needs to be continued.

- Dynamic Threat Environment: Cyber threats within healthcare spaces are always changing. Models that are static or updated infrequently run the risk of becoming outdated. The IDS should enable the use of online learning processes adapted to new threats, without the need to do a full retraining or needing to expose sensitive data. This means the need for a modular and agile design and very strong updating protocols.
- Interoperability and Integration: The IoMT systems are highly heterogeneous, being composed of devices from distinct vendors and employing different communication protocols and standards. There are issues with ‘seamless integration’ with these platforms. Promising efforts to standardize, such as IEEE 11073 and FHIR, exist, but the broader implementation in the field is ongoing.
- Scalability and Cost Issues: The deployment of an IDS in the cloud can be expensive for small clinics and in the case of undeveloped regions. Although pay-per-use is also the case of SaaS solutions, operational costs regarding network bandwidth, storage and security services could still be high. More, localized or edge-assisted models should be researched as potentially less costly alternatives.

6. Future Directions

- ML Models Adapted to Low Power: future works should aim to create models that are inherently developed for low power environments, maybe by introducing spiking neural networks or quantized learning algorithms that improve efficiency while maintaining good performance.
- Hybrid Deployment Models: The combination of edge and cloud resources in a hybrid architecture has the potential of optimizing latency and costs. Initial filtering can be performed at edge nodes, whereas more complex analysis could take place in the cloud.
- Privacy-Preserving Solutions: Similar to applying the above comments, improvements in differential privacy, secure multi-party computation, and federated analytics should continue to be made to be able to comply without breaking the systems’ usefulness.
- Collective Threat Intelligence: A collective threat intelligence network between hospitals and security providers can assist in identifying and addressing new threats more quickly. SaaS-based IDS deployments could function as nodes in this type of distributed defense.
- Training and designing around the user: Lastly, feedback from users as well as training of the medical personnel to interpret the alerts and actions is also important. A system can only be effective if it is trusted and adopted by the users

7. Conclusion

The growing adoption of IoMT technologies in the health sector has resulted in no previous benefits associated with real-time monitoring of patients, personalized treatment courses and organizational productivity. But it has also created major cybersecurity problems that traditional paradigms cannot address. Security mechanisms that are both smart and lightweight are mandated by the sensitivity of healthcare data and the importance of avoiding downtime of devices.

An intelligent and explainable IDS as a Software as a Service device designed, for the particular requirements of the resource-constrained IoMT ecosystem has been discussed in this paper. The use of lightweight machine learning methods, interpretable AI, and deployment as a scalable software as a service application make the proposed framework an ideal compromise between security and ease of use and implementation for healthcare networks. It covers technical issues relating to intrusion detection, as well as ethical and practical issues associated with the deployment of security systems in a clinical context.

The literature review put in evidence the limitations of existing IDS implementations, and particularly how there is a lack of IDEs models that are not only efficient but also interpretable and capable of adapting to new attacks. The method proposed is designed upon a modular architecture that places emphasis on data privacy, availability, interpretability, and minimized resource utilization. Anticipated benefits include significant enhancements in detection capabilities, consumer confidence and safety, as well as regulatory oversight.

Nonetheless, there are still several issues, such as achieving real-time performance, preserving privacy, and adapting to a dynamic threat environment . The area of advancement for future studies should be the definition of domain-specific AI algorithms, improvement of hybrid cloud-edge architecture and interoperability of IoMT devices.

In summary, the road to a completely trusted and secured IoMT ecosystem is a long and winding road, but it is certainly traversable. Intelligent and explainable IDSs, particularly those delivered as SaaS, represent a great opportunity to secure medical environments while maintaining efficiency and trust in the process. As the healthcare ecosystem transforms into a digital landscape, adaptive security and assurance solutions will become critical to not just the protection of data but most importantly the protection of lives.

8. References

1. M. Hassanalieragh et al., “Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges,” IEEE International Conference on Services Computing, 2015, pp. 285 292.

2. S. Islam, D. Kwak, M. Kabir, M. Hossain, and K. Kwak, “The Internet of Things for Health Care:

3. Y. Yang et al., “A Survey on Security and Privacy Issues in Internet-of-Things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250 1258, 2017.

4. A. Doshi, X. Wang, and D. Jin, “Machine Learning on the Edge: A Review,” ACM Computing Surveys, vol. 54, no. 8, 2022.

5. A. Al-Garadi et al., “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.

6. M. Abomhara and G. Koien, “Security and Privacy in the Internet of Things: Current Status and Open Issues,” International Conference on Privacy and Security in Mobile Systems, 2014, pp. 1–8.

7. S. Das, D. Acharya, and D. Jena, “Feature Selection using Particle Swarm Optimization for Effective IDS,” Procedia Computer Science, vol. 132, pp. 451–460, 2018.

8. S. M. Lundberg and S.-I. Lee, “A Unified Approach to Interpreting Model Predictions,” Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS), 2017.

9. P. Saravanan and V. Vaidehi, “Anomaly-based Intrusion Detection System using Ensemble Classifiers,” Wireless Personal Communications, vol. 105, no. 4, pp. 1441–1461, 2019.

10. H. Suo et al., “Security in the Internet of Things: A Review,” International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012.

11. M. Roesch, “Snort – Lightweight Intrusion Detection for Networks,” Proceedings of the 13th USENIX Conference on System Administration, 1999, pp. 229–238.

12. V. Paxson, “Bro: A System for Detecting Network Intruders in Real-Time,” Computer Networks, vol. 31, no. 23–24, pp. 2435–2463, 1999.

13. S. B. Patil and V. S. Rajpurohit, “IoT Based Anomaly Detection Using ML Algorithms,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 1525–1537, 2021.

14. A. Diro and N. Chilamkurti, “Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things,” Future Generation Computer Systems, vol. 82, pp. 761 768, 2018.

15. M. H. Bhuyan et al., “Network Anomaly Detection: Methods, Systems and Tools,” IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303–336, 2014.

16. K. Kim, “Deep Learning-Based Intrusion Detection System for IoT Networks,” Electronics, vol. 9, no. 11, p. 1778, 2020.

17. M. T. J. Alshamrani et al., “Anomaly-Based Intrusion Detection in IoT Systems Using Deep Learning Algorithms,” Sensors, vol. 20, no. 18, p. 5327, 2020.

18. J. Lin et al., “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

19. A. Barda et al., “A Privacy-Preserving Approach to Deep Learning-Based Intrusion Detection,” Computers & Security, vol. 93, p. 101788, 2020. [20] M. Guidotti et al., “A Survey of Methods for Explaining Black Box Models,” ACM Computing Surveys, vol. 51, no. 5, 2018.