


Enhancing Cybersecurity in Healthcare: Machine Learning and Deep Learning Strategies for Intrusion Detection on the Internet of Medical Things

Baohan Mo^{a}

Mathematics, Kean University, 1000 Morris Ave., Union, New Jersey, U.S.A.

Keywords: Internet of Things, Internet of Medical Things, Intrusion Detection Systems.


Abstract: The Internet of Things is increasingly being used in healthcare, leading to rapid growth on the Internet of Medical Things. This technology helps greatly with monitoring patients and collecting data for treatment. However, this combination of technology also introduces significant security threats, especially the risk of intrusions into the Internet of Medical Things (IoMT) systems. This paper evaluates how machine learning and deep learning can improve intrusion detection systems for IoMT. This paper reviewed the current use of Machine Learning (ML) and Deep Learning (DL) in Intrusion Detection Systems (IDS), focusing on systems that detect unusual activities and their effectiveness within the IoMT. By comparing traditional and newer models, such as the PCA-GWO hybrid model, this study highlighted the importance of designing and improving models to identify security threats. The study finds that while ML and DL offer powerful and efficient solutions for detecting intrusions, they also come with challenges in computational demands, data collection and privacy, and making the models easy to explain. Further research can help improve these areas, including optimal algorithms, legal ways to gather data, and using advanced encryption and federated learning to balance efficiency with privacy. The paper concludes that optimized ML and DL techniques can greatly enhance the security of IoMT, ensuring that critical medical data remains intact and private.

1 INTRODUCTION

In the realm of modern healthcare, the proliferation of Internet of Things (IoT) devices has initiated a digital revolution. Patient monitoring and medical data collection have become sophisticated, thanks to this paradigm shift prompted by Kevin Ashton's concept of the IoT in 1999. The IoT is not merely a network of interconnected devices; it is a robust infrastructure integral to the information society. It leverages identification, data capture, processing, and communication capabilities, facilitating an array of services across diverse applications (International Telecommunication Union, n.d.). However, this digital metamorphosis brings with it a plethora of challenges. The heterogeneous nature of the internet, a dearth of comprehensive security solutions, and the manufacturers' sometimes lax approach to security pose significant risks. Despite advancements in IoT technology and the implementation of intrusion

prevention systems, the security of the Internet of Medical Things (IoMT) networks remains jeopardized. Cyber attackers have demonstrated a disturbing proficiency in exploiting vulnerabilities to compromise devices and exfiltrate sensitive patient data. They can remotely disable medical devices, potentially paralyzing entire hospital networks, compromising patient care, and endangering lives (Zhang et al., 2024).

The burgeoning field of IoMT, a subset of IoT applied specifically to healthcare, promises enhanced patient monitoring through its real-time, continuous data collection capabilities (Si-Ahmed et al., 2023). Yet, as the deployment of IoMT devices surges, so too do the security risks. The methods and motives of cyber-attacks are evolving, with attackers now capable of manipulating medical devices and illicitly accessing health records. The inherent lack of robust security measures in these devices — the oversight of essential authentication, trust models, and anomaly detection techniques — provides a gateway for

^a <https://orcid.org/0009-0009-3413-2486>

unauthorized interventions. One of the more insidious forms of cyber aggression faced by healthcare networks is the Distributed Denial of Service (DDoS) attack, which denies service to legitimate users (Gupta et al., 2022). It underscores the urgency for effective intrusion detection systems (IDS). This also reflects the significant impact of vulnerabilities on IoMT networks that transmit critical patient data (Ioannou et al., 2021).

While traditional IDS can be energy-intensive, the advent of machine learning offers a beacon of hope. ML techniques not only conserve energy but also excel in processing vast datasets. The challenge, however, is that big data processing with traditional ML often entails laborious manual feature extraction and data labeling, which is not only time-consuming but can also compromise accuracy (Kocher et al., 2021). In contrast, deep learning, a more sophisticated incarnation of machine learning, thrives on large datasets. It excels at autonomously learning features, which is invaluable when managing complex and high-dimensional data streams common in medical applications. DL algorithms, through their intricate neural network structures, are adept at discerning intricate patterns and anomalies in data that would typically elude traditional ML models. Saheed et al. create capable and streamlined Intrusion Detection Systems (IDS) within the IoMT framework to identify and anticipate unforeseen network threats (Saheed et al., 2021). Common IDS strategies split into two types: signature-based and anomaly-based. The anomaly-based IDS utilizes machine learning to generate models of reliable activities. It then assesses incoming data against these models, flagging any deviations as potentially suspicious. This method retains effectiveness within the IoMT sphere, employing various algorithms like random forests, decision trees, and Convolutional Neural Networks (CNNs), all of which demonstrate robust performance.

This article delves into the transformative impact of ML and DL in fortifying the IoMT against cyber threats. By scrutinizing the latest research contributions, comparing outcomes from existing literature, and evaluating the advantages and drawbacks, this paper aims to provide a comprehensive survey of the field. This paper outlines the methods in Section 2, explaining the steps and analysis used. Section 3 discusses the empirical results and relates them to previous work in the field. Finally, Section 4 summarizes the research's contributions and explores their implications for future work in this area.

2 METHODS

2.1 Framework of IoMT

In the structural configuration of the IoT framework, a quintet segmentation is conventionally proposed (Khan et al., 2012), whereas the Internet of IoMT specifically is delineated into a three-tiered hierarchy (Si-Ahmed et al., 2023). This tailored tripartite demarcation within IoMT is characterized by a things layer, an intermediate layer, and a back-end computing, each serving distinct yet interlinked functions in the network's ecosystem.

The things layer shown in Figure 1 residing at the IoMT's interface, is engineered for data acquisition, channelling the raw sensory input derived from a myriad of devices and actors within the healthcare milieu. This includes an array of instruments and equipment, integrated and wearable technology, as well as human agents - nurses, physicians, and patients - all embedded within the clinical infrastructure. Each entity is endowed with communicative capacities, typically leveraging RFID and EPC technologies, to broadcast pertinent data such as physiological metrics and operational statuses. This echelon of the architecture is meticulously tuned to harness and relay information, embodying a complex mesh of nodes that bridge the corporeal and the digital realms (Irfan et al., 2018).

The intermediate layer, or the gateway layer, assumes a pivotal role as the processing and transit hub within the IoMT schema. It encapsulates the technological sophistication of multi-agent systems, leveraging the distributed prowess of fog computing to furnish prompt and localized data analytics. Through a versatile suite of communication protocols - spanning HTML, SMS, MMS, Bluetooth, and Wi-Fi - this stratum orchestrates the dialogue between the diverse array of devices and the overarching IoMT infrastructure. It is within this tier that the crucial functions of encryption and security protocols are executed, ensuring that all transmitted data uphold the rigorous standards of confidentiality and integrity. Moreover, it confers a degree of contextual intelligence upon the data, tagging it with spatial and temporal metadata to enhance subsequent analytic endeavors and anomaly detection algorithms (Irfan et al., 2018).

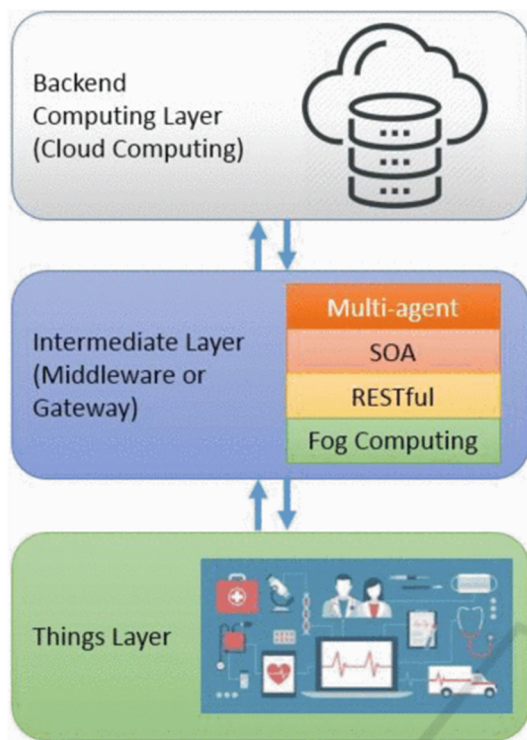


Figure 1: IoMT Architecture (Irfan et al., 2018).

2.2 IoMT IDS Approaches

As previously delineated, conventional Intrusion Detection System (IDS) strategies bifurcate into two quintessential types: signature-based IDS and anomaly-based IDS. This treatise concentrates on the latter, undertaking a scrutinizing survey and analysis of extant models. Through this lens, the discourse endeavours to dissect and appraise the nuanced mechanisms that define anomaly-based IDS, emphasizing the integration and optimization of such systems within the increasingly complex tapestry of cybersecurity.

2.2.1 Machine Learning Algorithms-Based IoMT IDS

In (Gao et al., 2017), the Author et al. describes a norm-based intrusion detection system employing decision tree algorithms. The decision tree model utilizes observational data to project outcomes. The research developed decision tree classifiers to ascertain if network conduct aligns with specific attributes correlated with the security of medical apparatuses. These attributes, forming the crux of the machine learning model input, encompass the type of operation executed, the timing of the operation, the frequency of the operation, the interval elapsed since

the last operation, the signal strength indicator received, the day type, and the location. The proposed scheme issues alerts when observed behaviours diverge from the established profile of normal device operations. Ultimately, the decision tree algorithm was juxtaposed with Support Vector Machine (SVM) and K-means algorithms, revealing that decision-tree-based algorithms yield superior detection precision, diminished false positive rates, and accelerated training and prediction velocities in contrast to other algorithms scrutinized. Nonetheless, the proffered method might falter in instances where the assailant possesses insider knowledge of the data access paradigms to and from the medical device.

2.2.2 Deep Learning Algorithms-Based IoMT IDS

Ismail et al. in (Ismail et al., 2020), an exploration of CNN-based monitoring within the IoMT milieu is undertaken, spotlighting the role of Convolutional Neural Networks (CNN) in the domain. The researchers proffer a novel CNN-regular target detection and recognition model, predicated on the Pearson Correlation Coefficient and regular pattern behaviour, crafted to surmount the challenges spawned by the substantial memory requisites and intricate model complexity analysis associated with CNN deployment. This model is calibrated to discern regularities or consistent patterns within health parameters that typically manifest in contexts characterized by minimal variability. The quintessential health-related factors are sifted through in the initial hidden layer of the CNN, while the ensuing layer executes a correlation coefficient analysis, categorizing health factors into either positively or negatively correlated. Regular pattern behaviours are unearthed via mining the frequency of these patterns within the classified health factors. The model's outputs are then stratified into parameters linked to maladies such as obesity, hypertension, and diabetes. The efficacy of the model was corroborated by leveraging two distinct datasets, demonstrating an enhancement in accuracy and computational efficiency vis-à-vis a triad of alternative machine learning methodologies. This CNN model leverages deep learning's intrinsic capability for feature extraction and pattern recognition, enabling the processing of unstructured medical health records and the identification of consistent health parameter patterns.

Ioannou et al. in (Ioannou et al., 2021) introduce a hybrid model specifically designed for IDS within the IoMT framework, synergizing Principal

Component Analysis (PCA) and Grey Wolf Optimization (GWO) as pivotal feature engineering steps for Deep Neural Networks (DNN). The machine learning workflow commences with data pre-processing, incorporating PCA for dimensionality reduction to curtail the feature set within the dataset, thereby augmenting computational efficiency and model performance. Classification tasks are executed employing a DNN, structured with an input layer, multiple hidden layers, and an output layer. The optimization process within GWO emulates the hierarchical leadership and hunting strategies of wolves to identify optimal solutions in feature selection space, culminating in a PCA-GWO hybrid model that ensures only the most pertinent features are utilized for training, enhancing the accuracy and efficiency of the DNN classifier. Upon comparison with traditional machine learning classifiers, such as K-Nearest Neighbours, Naive Bayes, Random Forest, and Support Vector Machines, the proposed PCA-GWO-DNN model demonstrates superior accuracy and reduced training times.

3 DISCUSSIONS

Machine learning and deep learning are widely used in the medical field of the Internet of Things and are constantly innovating. Facing different problems in the medical field, different methods can be used to adjust to resist different intrusions and protect the privacy of medical data. and patient safety. Machine learning performs better than traditional methods when dealing with long rule problems. Zero-day attacks and new vulnerabilities in IDS can be effectively detected through machine learning (Si-Ahmed et al., 2023). However, machine learning relies on manual feature selection and model tuning, while structuring the data results in faster training and prediction times, along with accuracy and lower false positive rates when the system is trained with easy-to-understand features. Deep learning further improves the inherent capabilities of feature extraction, reduces the need for manual feature engineering, and is better at processing unstructured data common in medical records, improving computational efficiency while maintaining or enhancing accuracy (Qiu, 2022). At the same time, some hybrid model attempts, such as PCA and GWO hybrid model optimization feature selection, have improved the performance of problem solving to varying degrees. While the medical IoMT is constantly innovated upon through the application of machine learning and deep learning, addressing

numerous issues within the medical field, there are noteworthy limitations and challenges to consider. First, IoMT devices are unaffordable because most methods require high computational overhead to train models, which consumes limited energy of IoMT devices (Rbah et al., 2022). Besides, collecting large data sets in an IoMT environment may be difficult due to privacy concerns or practical limitations. Additionally, the offline environment of the model cannot consider the real Internet of Things environment, and most models have poor interpretability (Rbah et al., 2022). On the other hands, privacy issues will always need to be taken into consideration, and more sophisticated privacy-preserving technologies may be integrated into IoT devices and systems. Advanced encryption methods are divided into symmetric, asymmetric, keyless algorithms, and implementations such as homomorphic encryption or federated learning, where data only remains on the local device and only model updates are shared (Ghubaish et al., 2021). To tackle the issue of high computational overhead and energy consumption for training IoMT device models, optimization algorithms such as Particle Swarm Optimization (PSO) can streamline computing demands, and efficient model architectures can minimize energy use while maintaining high accuracy. Furthermore, the collection and utilization of data can be conducted legally and ethically through cooperation and sharing agreements, safeguarding private information. In terms of model interpretability, tools like LIME enhance model transparency, making them more comprehensible. Shafiq et al. have demonstrated improvements in the accuracy of machine learning predictions by employing a blend of PSO, machine learning classifiers, and LIME-based explanations to facilitate human interpretability (Memon et al., 2023). Moreover, the adoption of advanced encryption techniques, including symmetric, asymmetric, and keyless algorithms, alongside methods like homomorphic encryption or federated learning, ensures that private data remains on local devices. Only model updates are shared, which not only preserves user privacy but also mitigates energy consumption (Ghubaish et al., 2021).

4 CONCLUSIONS

This article explores how the IoMT can leverage ML and DL technologies to improve the performance of IDS in the context of increasing cybersecurity threats. Although the deployment of IoMT devices comes

with challenges and security risks, proper application of ML and DL technologies offers promising solutions to these problems. The article introduces various IDS strategies using machine learning algorithms e.g. decision trees and deep learning methods e.g. CNN) and evaluates the performance of these algorithms in real-time monitoring and anomaly detection. In addition, the paper also focuses on the use of a hybrid model combining PCA and GWO to achieve the optimization of feature engineering in DNN. These methods provide more accurate, efficient, and energy-efficient ways to detect and prevent cyber threats, ensuring the integrity and confidentiality of sensitive medical data. Although the integration of IoT with machine learning and deep learning provides efficient solutions and IDS performance can be enhanced in the face of increasing cybersecurity threats, it also brings some challenges such as device energy consumption, data collection, models explain ability and privacy security. These challenges are being addressed through advances such as algorithm optimization, establishing legal frameworks for data use, implementing explainable models, and employing cutting-edge encryption and federated learning technologies. These measures are critical to improve the effectiveness, accuracy, and energy efficiency of cyber threat detection and prevention, which is critical to protecting the sensitive medical data at the heart of IoMT.

REFERENCES

- Gao, S., & Thamilarasu, G. 2017. Machine-learning classifiers for security in connected medical devices. 2017 26th International Conference on Computer Communication and Networks (ICCCN), pp. 1-5.
- Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. 2021. Recent advances in the internet-of-Medical-Things (IoMT) systems security. *IEEE Internet of Things Journal*, 8(11), pp. 8707-8718.
- Gupta, K., Sharma, D. K., Gupta, K. D., & Kumar, A. 2022. A tree classifier based network intrusion detection model for Internet of Medical Things. *Computers and Electrical Engineering*, 102, 108158.
- Internet of things global standards initiative. (n.d.). ITU. <https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx>
- Ioannou, I., Nagaradjane, P., Angin, P., Balasubramanian, P., Kavitha, K. J., Murugan, P., & Vassiliou, V. 2024. GEMLIDS-MIOT: A green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening. *Computer Communications*, 218, pp. 209-239.
- Irfan, M., & Ahmad, N. 2018. Internet of Medical Things: Architectural model, motivational factors and impediments. 2018 15th Learning and Technology Conference (L&T), pp. 6-13.
- Ismail, W. N., Hassan, M. M., Alsalamah, H. A., & Fortino, G. 2020. CNN-based health model for regular health factors analysis in internet-of-Medical things environment. *IEEE Access*, 8, pp. 52541-52549.
- Khan, R., Khan, S. U., Zaheer, R., & Khan, S. 2012. Future internet: The Internet of things architecture, possible applications and key challenges. 2012 10th International Conference on Frontiers of Information Technology, pp. 257-260.
- Kocher, G., & Kumar, G. 2021. Machine learning and deep learning methods for intrusion detection systems: Recent developments and challenges. *Soft Computing*, 25(15), pp. 9731-9763.
- Memon, S. A., Wiil, U. K., & Shaikh, M. 2023. Explainable Intrusion Detection for Internet of Medical Things. In *Proceedings of the 15th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management-KMIS*, SCITEPRESS Digital Library, pp. 40-51.
- Qiu, Y., Wang, J., Jin, Z., Chen, H., Zhang, M., & Guo, L. 2022. Pose-guided matching based on deep learning for assessing quality of action on rehabilitation training. *Biomedical Signal Processing and Control*, 72, 103323.
- Rbah, Y., Mahfoudi, M., Balboul, Y., Fattah, M., Mazer, S., Elbekkali, M., & Bernoussi, B. 2022. Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey, 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1-9.
- Saheed, Y. K., & Arowolo, M. O. 2021. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms, *IEEE Access*, 9, pp. 161546-161554.
- Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. 2023. Survey of machine learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing*, 140, 110227.
- Zhang, Y., Zhu, D., Wang, M., Li, J., & Zhang, J. 2024. A comparative study of cyber security intrusion detection in healthcare systems. *International Journal of Critical Infrastructure Protection*, 44, 100658.
- Zhang, L., Shen, L., Ding, L., Tao, D., & Duan, L. Y. 2022. Fine-tuning global model via data-free knowledge distillation for non-iid federated learning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 10174-10183.