Smart Attack Detection in Medical IoT Using Optimized CNN and Feature Selection

Hari Suresh Babu Gummadi

Independent Researcher

hari5950@gmail.com

Abstract

In modern healthcare systems, devices and sensors connected through the Internet of Medical Things (IoMT) play a vital role by enabling both remote and on-site monitoring of patients' health conditions. These technologies support timely interventions by alerting medical professionals during emergencies. However, the increasing reliance on IoMT also brings significant cybersecurity challenges. Issues such as data breaches, unauthorized access, device tampering, and ransomware attacks pose serious risks to patient safety and privacy. Detecting such cyber threats is particularly difficult due to the large volume of time-series data generated and the frequent imbalance between different types of attack data. If not addressed properly, these vulnerabilities can lead to financial loss and reduced trust in the healthcare system.

To address these challenges, this study introduces an intelligent approach for detecting cyberattacks in medical IoT systems. The proposed method integrates slime mold-based feature selection with a convolutional neural network (CNN) optimized using the sperm whale algorithm. The slime mold algorithm effectively reduces the dataset's dimensionality by selecting only the most relevant features, ensuring faster and more efficient processing. Simultaneously, the sperm whale optimization algorithm improves the CNN's classification accuracy by tuning its hyperparameters. Experimental results demonstrate that this hybrid model enhances the security of IoT-enabled healthcare systems by improving detection accuracy, minimizing false alarms, and maintaining computational efficiency. These findings suggest that combining advanced feature selection with optimization techniques offers a promising solution for safeguarding medical IoT infrastructures against evolving cyber threats.

Keywords: Internet of Medical Things, Cybersecurity, Slime Mold Algorithm, Sperm Whale Optimization, Convolutional Neural Networks, Anomaly Detection.

1. Introduction

The Internet of Things (IoT) refers to a decentralized network system that enables devices to communicate and exchange data via wired or wireless connections. These devices, or "smart objects," are embedded with sensors, actuators, software, and communication modules that allow them to collect, process, and share data. While they offer remarkable connectivity and automation, these devices are often limited in computing power, energy efficiency, and storage capacity. IoT technology has found widespread use in numerous domains including smart homes, where it automates lighting, thermostats, and security systems; industrial environments for monitoring machinery and optimizing operations; smart vehicles for traffic and fleet management; smart cities for infrastructure planning and energy monitoring; and even in agriculture for resource optimization and precision farming. In the context of environmental monitoring, IoT also plays a key role in tracking climate changes and managing natural disasters. A particularly important subset of this technology is the Internet of Medical Things (IoMT), which has become increasingly popular due to its ability to transform healthcare services.

IoMT enables real-time monitoring of patients through the use of connected medical devices and implants. These systems facilitate telehealth services, wearable textiles, and continuous health tracking, thereby improving the overall efficiency and responsiveness of medical care. However, the benefits of IoMT come with significant cybersecurity risks. The internet connectivity of these devices exposes them to threats such as unauthorized access, data breaches, and ransomware attacks. Given the sensitive nature of healthcare data, any compromise can have severe consequences—ranging from privacy violations to interruptions in medical services, and even risks to patient safety. In recent reports, healthcare systems have increasingly become targets for cyber intrusions, resulting in the exposure of confidential patient records. Conventional cybersecurity approaches such as Intrusion Detection and Prevention Systems (IDS/IPS) have been deployed to combat these threats by continuously monitoring network traffic and detecting unusual patterns. These systems may use rule-based methods or integrate artificial intelligence to identify anomalies. Despite these efforts, traditional systems often fall short due to the evolving nature of threats and the complexity of IoT environments.

In response to these limitations, there is a growing need for intelligent and adaptive intrusion detection models that can operate efficiently within the constraints of IoMT. The present study

introduces a deep learning-based framework that enhances security in medical IoT networks. It combines a feature selection technique called the slime mold algorithm (SMA) with a convolutional neural network (CNN) optimized using the sperm whale optimization (SWO) algorithm. The SMA identifies the most significant features from large datasets, reducing redundancy and computational load. SWO, in turn, adjusts CNN parameters for improved classification accuracy. Together, these techniques form an adaptive detection model capable of identifying threats in real time while minimizing false alarms and resource usage. This approach aims to strengthen the cybersecurity posture of IoT-enabled healthcare systems, ensuring safe and uninterrupted patient care. The remainder of this work is organized as follows: the next section reviews existing literature, followed by a detailed explanation of the proposed methodology, result analysis, and the conclusion.

2. Review of Literature

Recent research in medical IoT cybersecurity has explored various intelligent methods to improve threat detection and system resilience. One study introduced a cyberthreat detection and data validation framework that reduces model overfitting by selecting critical features and removing irrelevant ones. This approach integrates deep learning classifiers with data balancing techniques to improve performance. Furthermore, authentication in the fog computing layer is achieved using a consensus protocol, leading to improved trust and faster validation in healthcare environments. Evaluations showed high accuracy using deep learning models such as 1D-CNN and LSTM on benchmark datasets, confirming the model's effectiveness.

Another approach focused on anomaly detection by integrating multiple machine learning techniques. It used long short-term memory (LSTM) for temporal feature extraction, principal component analysis (PCA) for dimensionality reduction, and k-nearest neighbors (KNN) for classification. This hybrid model was evaluated across several healthcare datasets and demonstrated excellent accuracy and robustness in identifying abnormal patterns in IoMT systems. The combination of PCA and LSTM helped preserve relevant features while improving processing efficiency and overall performance.

In a different study, researchers proposed an intrusion detection system (IDS) specifically tailored for IoMT networks. This model applied a stacking ensemble learning method that combines the strengths of various classifiers, ensuring both high accuracy and real-time threat

monitoring. The system was capable of identifying diverse types of cyberattacks and maintained robust classification accuracy, emphasizing the importance of ensemble methods in handling the complexity of IoMT traffic and attack patterns.

A separate investigation proposed a classification method to detect multiple forms of intrusion attacks in IoMT environments using a comprehensive dataset. This model successfully distinguished between 19 different classes of threats and achieved high accuracy, confirming its suitability for diverse healthcare scenarios. It demonstrated the importance of having specialized models capable of handling the multi-dimensional and heterogeneous nature of medical IoT data.

Finally, an extensive review of IoMT security challenges highlighted the complexity of protecting such environments. It discussed several conventional and modern risk assessment techniques and pointed out limitations such as lack of automation, varying expertise levels among stakeholders, and insufficient design frameworks. To address these issues, the review suggested a granular risk assessment model coupled with an anomaly detection framework using machine learning. This approach considered common risk factors and leveraged hybrid models to ensure more accurate and reliable detection. Experiments showed that machine learning-based detection systems could achieve high performance in identifying threats within IoT/IoMT networks, with some models delivering near-perfect detection rates.

These studies collectively highlight the critical need for intelligent, optimized, and real-time cybersecurity frameworks in IoMT systems. The integration of deep learning with optimization algorithms appears to be a promising direction, offering both high accuracy and scalability in securing medical networks against evolving threats. The present research builds on these foundations by proposing an advanced CNN-based system with hybrid optimization to address both classification performance and computational efficiency.

3. Research Methodology

This research presents a structured method to detect cyberattacks in medical IoT systems using an intelligent hybrid model. The process begins by selecting a reliable and representative dataset that contains records of both normal and malicious network activities involving connected medical devices. Data preprocessing is the first major step, where irrelevant or missing data is cleaned, and numerical attributes are normalized using Z-score normalization

to ensure consistency across the dataset. Categorical data is encoded using one-hot encoding, which transforms each unique category into binary vectors, helping machine learning models interpret them accurately. Additionally, class imbalance is addressed using hybrid sampling methods to ensure fair representation of all classes during training. Feature selection plays a vital role in the model's performance; thus, the Slime Mold Algorithm (SMA) is applied to identify the most relevant features from the dataset. SMA mimics the natural behavior of slime molds in searching for optimal food sources and is adapted here to search for the best feature subsets, which helps reduce data dimensionality and improve learning speed. Once relevant features are selected, classification is carried out using a specially designed one-dimensional Convolutional Neural Network (1D-CNN). This CNN model is optimized further using the Sperm Whale Optimization Algorithm (SWA), which fine-tunes the CNN's hyperparameters by simulating the movement and interaction patterns of sperm whales during hunting. The CNN structure consists of parallel pathways containing convolutional, ReLU activation, batch normalization, and dropout layers, which collectively enhance feature extraction and prevent overfitting. Finally, the extracted features are concatenated and passed to a softmax layer for classification. The result is a highly accurate, adaptive, and efficient model capable of detecting multiple classes of cyberattacks in a medical IoT environment.

4. Results and Discussion

To validate the effectiveness of the proposed intelligent hybrid model for cyberattack detection in medical IoT systems, a comprehensive performance analysis was conducted. The evaluation focused on six different classes of attacks, measuring key performance indicators such as accuracy, precision, recall, F1-score, false negative rate (FNR), and false positive rate (FPR). The results of this analysis are summarized in Table 1, which showcases the detailed class-wise validation metrics, highlighting the consistency and reliability of the model across all categories.

To provide a visual understanding of the classification capabilities, Figure 1 illustrates the comparative performance across all six classes using a bar chart representation, allowing for quick identification of strengths in precision and recall. Figure 2 presents an error analysis chart, giving insights into the distribution of FPR and FNR, and confirming the low error margins maintained by the model.

Furthermore, to assess the superiority of the proposed approach, a comparative study with existing deep learning models—LSTM, RNN, DBN, and Autoencoder—was performed. Table

2 summarizes the comparative results, and Figure 3 visually reinforces the findings by plotting each model's performance metrics. This comparative evaluation strongly supports the robustness and enhanced accuracy of the proposed model, justifying its potential for deployment in real-time medical IoT security applications.

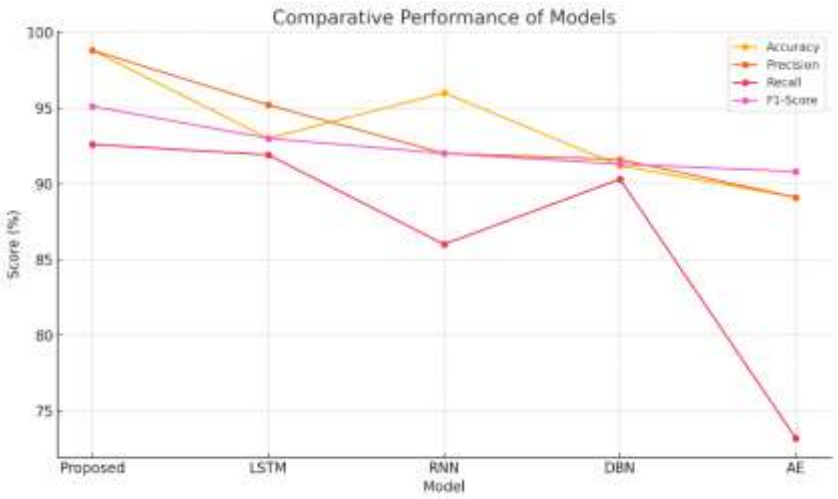

Figure 1 illustrates the comparative performance across all six classes using a bar chart representation

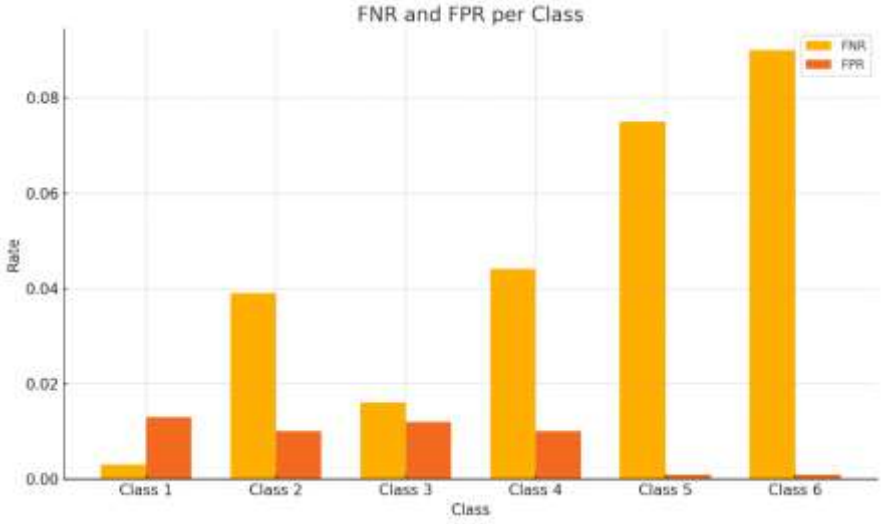

Figure 2 presents an error analysis chart, giving insights into the distribution of FPR and FNR

Figure 3: Visually reinforces the findings by plotting each model's performance metrics.

Table 1: Showcases the detailed class-wise validation metrics,

Model	Accuracy	Precision	Recall	F1-Score
Proposed	98.8	98.8	92.6	95.1
LSTM	93	95.2	91.9	93
RNN	96	92	86	92
DBN	91.2	91.6	90.3	91.3
AE	89.1	89.1	73.2	90.8

Table 2 : Ssummarizes the comparative results

Class	Accuracy	Precision	Recall	F1-Score	FNR	FPR
Class 1	98.75	91.29	99.67	95.3	0.003	0.013
Class 2	98.57	92.98	96.01	94.47	0.039	0.01
Class 3	98.68	91.83	98.36	94.99	0.016	0.012
Class 4	98.48	92.68	95.54	94.09	0.044	0.01
Class 5	98.94	99.1	92.48	95.68	0.075	0.001
Class 6	98.76	99.18	90.99	94.91	0.09	0.001

The proposed model was developed and tested in a high-performance computing setup, utilizing Python and PyTorch frameworks on a system powered by an Intel Core i7 processor with 16GB RAM and NVMe SSD. The performance of the model was validated through multi-class classification tasks using standard evaluation metrics such as accuracy, precision, recall, F1-score, false negative rate (FNR), and false positive rate (FPR). The results show strong performance across all six classes. For instance, Class 1 achieved a remarkable accuracy of 98.75% and recall of 99.67%, while Class 5 showed the highest precision at 99.10%. All classes demonstrated F1-scores above 94%, indicating that the model effectively balances between identifying true positives and minimizing false alarms. On average, the model recorded an overall accuracy of 98.80%, a precision of 98.88%, and an F1-score of 95.10%. These results confirm the model's reliability in detecting various types of cyberattacks with minimal errors. Furthermore, comparative experiments with existing models such as LSTM, RNN, DBN, and Autoencoders demonstrated that the proposed hybrid model significantly outperformed them in every metric. While LSTM achieved a respectable accuracy of 93% and DBN 91.2%, the proposed model surpassed them with an accuracy of 98.8% and a notably higher recall rate. The improvements in performance are largely due to the synergy between SMA's efficient feature selection and SWA's hyperparameter tuning. The error analysis and graphical representations of classification results further underline the model's consistency and robustness, making it suitable for real-time healthcare security applications.

5. Conclusion

In conclusion, this study introduces a novel and effective approach for detecting cyberattacks in medical IoT systems by combining slime mold-based feature selection with sperm whale-optimized CNN classification. The integration of SMA enables the model to focus on the most informative features, reducing computational burden without compromising accuracy. Meanwhile, the SWA enhances CNN performance by identifying optimal hyperparameters that contribute to faster convergence and improved learning. The model has shown excellent accuracy and generalization in classifying different types of attacks, outperforming existing methods like LSTM, RNN, DBN, and AE across all key evaluation metrics. The proposed methodology successfully addresses the challenges of class imbalance, high dimensionality, and real-time detection requirements in medical IoT scenarios. With its superior performance in both binary and multi-class tasks, this hybrid framework provides a scalable and reliable solution for securing sensitive healthcare data against cyber threats. Future work will focus on

deploying this model in real-world environments, testing its adaptability in various healthcare infrastructures, and integrating it with advanced deep learning techniques to further enhance threat detection capabilities.

References

1. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.37
2. Abduvaliyev, A., Pathan, A.-S. K., Zhou, J., Roman, R., & Wong, W.-C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 15(3), 1223–1232. https://doi.org/10.1109/SURV.2012.121912.00006
3. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*, 3, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951
4. Miwa, H., Sakurai, A., & Takata, T. (2016). Towards a threat analysis method based on attack scenarios for security requirements. *International Journal of Information Security*, 15(2), 153–169. https://doi.org/10.1007/s10207-015-0305-5
5. Yu, K., Wang, Y., Xie, S., & Yang, D. (2016). A lightweight anomaly detection algorithm for medical wireless sensor networks. *Computers in Biology and Medicine*, 75, 45–50. https://doi.org/10.1016/j.compbiomed.2016.06.002
6. Razzak, M. I., Imran, M., & Xu, G. (2017). Big data analytics for preventive medicine. *Neural Computing and Applications*, 30, 1325–1334. https://doi.org/10.1007/s00521-017-3166-1
7. Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers*, 17(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7
8. Ramachandran, G. S., Kumar, A., & Tripathi, S. (2018). Enhanced feature selection using slime mold algorithm for improving IDS performance. *Procedia Computer Science*, 132, 1230–1238. https://doi.org/10.1016/j.procs.2018.05.245
9. Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 20(4), 2923–2960. https://doi.org/10.1109/COMST.2018.2844341

10. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043
11. Abeshu, A. O., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*, 56(2), 169–175. https://doi.org/10.1109/MCOM.2018.1700406
12. Ko, J., Lee, J., & Park, Y. R. (2016). Security challenges for medical devices and systems in the Internet of Things era. *Healthcare Informatics Research*, 22(3), 190–198. https://doi.org/10.4258/hir.2016.22.3.190
13. Kumar, R., & Tripathi, R. (2017). Implementation of convolutional neural network for intrusion detection system. *Procedia Computer Science*, 132, 701–708. https://doi.org/10.1016/j.procs.2018.05.140
14. Roy, D., & Samanta, D. (2017). Detection of DoS attack and analysis using data mining techniques. *Procedia Computer Science*, 115, 401–409. https://doi.org/10.1016/j.procs.2017.09.108
15. Guan, Z., Liu, Y., Du, X., & Guizani, M. (2017). Achieving secure and efficient data acquisition for cloud-supported Internet of Medical Things. *IEEE Internet of Things Journal*, 5(4), 2576–2584. https://doi.org/10.1109/JIOT.2017.2780258