Securing Smart Healthcare: Intrusion Detection in IoMT Networks Using Deep Learning

Mohammed Saidani[1*], Akram Ben Tabo[1]

[1] Department of Computer Science, University of Laghouat, 03000, Algeria

* mohammed.saidani@mail.com

https://doi.org/10.70695/10.70695/IAAI202503A6

Abstract

With the exponential growth of the Internet of Medical Things (IoMT), healthcare systems are increasingly vulnerable to a wide array of cyber threats that can jeopardize patient safety, data privacy, and operational integrity. Traditional security mechanisms often fall short in identifying sophisticated or novel attack patterns. To address this issue, we propose a deep learning-based intrusion detection system (IDS) that leverages Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNN) to detect malicious activity within IoMT network traffic. The system is evaluated using the CICIoMT2024 dataset, which simulates real-world IoMT environments. We conduct three levels of classification: binary (attack vs. normal), 6-class (category-level attacks), and 19-class (specific attack types). Each model is assessed using performance metrics including accuracy, precision, recall, and F1-score. Our results indicate that CNNs consistently outperform RNNs, particularly in binary and category-level classifications, achieving high accuracy and robustness. The study demonstrates the effectiveness of deep learning models in enhancing IoMT network security and provides a practical framework for deploying intelligent, real-time IDS solutions in healthcare infrastructures.

Keywords Intrusion Detection System; Deep Learning; Internet of Medical Things; Convolutional Neural Network; Recurrent Neural Network; Cybersecurity

1 Introduction

The integration of digital technologies into healthcare systems has given rise to a new and transformative paradigm: the IoMT [1]. IoMT refers to the networked ecosystem of medical devices, sensors, software applications, and healthcare systems that communicate and exchange data over the internet. These devices are designed to collect, monitor, and transmit critical patient data in real-time, enhancing clinical decision-making, patient outcomes, and operational efficiency. From remote patient monitoring and wearable health trackers to connected infusion pumps and diagnostic imaging systems, IoMT has revolutionized how healthcare services are delivered [2].

However, this increased connectivity comes at a significant cost in terms of cybersecurity. IoMT systems inherently possess several vulnerabilities: they often rely on resource-constrained devices, operate in open or semi-secure environments, use legacy protocols, and are required to maintain high availability [3]. As a result, IoMT infrastructures have become prime targets for cyberattacks such as denial-of-service (DoS), man-in-the-middle attacks, data exfiltration, ransomware, and malware infiltration. The implications of such attacks can be catastrophic—not only compromising the confidentiality and integrity of medical records but also disrupting vital clinical functions and potentially endangering patients' lives [4].

In this context, ensuring the security and resilience of IoMT networks is a pressing concern. Traditional security mechanisms, including firewalls, signature-based antivirus tools, and rule-based IDS, are increasingly inadequate in this dynamic threat landscape [5]. These systems typically rely on known attack signatures or predefined behavioral rules, which limits their ability to detect zero-day exploits, advanced persistent threats (APT), or rapidly evolving malware strains. Moreover, manually updating and tuning these systems for the ever-growing volume of network traffic is both time-consuming and error-prone [6].

To address these limitations, researchers have turned to artificial intelligence (AI) and, more specifically, deep learning (DL) techniques for building intelligent and adaptive IDS frameworks. Deep learning models are capable of learning intricate patterns and anomalies from raw data with minimal human intervention. By leveraging large-scale network traffic datasets, DL models can generalize beyond seen examples and detect novel threats in real time. Two of the most prominent deep learning architectures in the domain of network security are CNNs and RNNs [7-8].

CNNs, originally developed for image processing, are powerful feature extractors that can capture spatial correlations in structured input data. When applied to network traffic, CNNs can identify distinguishing patterns in packet sequences and flow statistics. RNNs, on the other hand, are well-suited for temporal data and are capable of modeling sequential dependencies across time—making them ideal for identifying persistent attack behaviors and event sequences in traffic logs [9]. Both models offer unique advantages and have been used independently or in combination to build robust IDS systems. Fig. 1. Shows an example of an IDS.

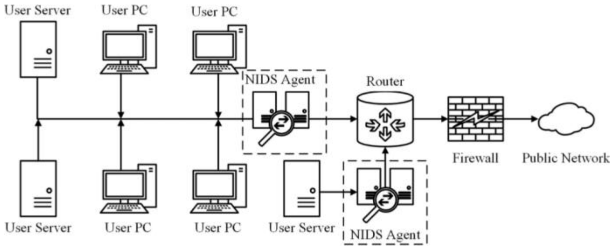

Fig. 1. An Example of IDS

This paper presents a comparative study of CNN and RNN-based deep learning models for intrusion detection in IoMT networks using the CICIoMT2024 dataset. Developed by the Canadian Institute for Cybersecurity, CICIoMT2024 is a comprehensive and realistic dataset that emulates real-world IoMT traffic under both normal and attack scenarios [10-11]. It includes a wide variety of attacks such as brute force, botnet, keylogging, DDoS, and privilege escalation, making it well-suited for evaluating intrusion detection techniques. The dataset also categorizes traffic into binary labels (normal vs. malicious), six attack categories, and nineteen specific attack types, providing multiple levels of classification granularity [12-13].

The key objectives of this research are as follows:

To investigate the applicability of CNN and RNN deep learning architectures for intrusion detection in IoMT environments.

To evaluate the performance of both models using three classification tasks: binary, 6-class (attack category), and 19-class (attack-specific).

To measure and compare the models using standard classification metrics such as accuracy, precision, recall, and F1-score.

To analyze the strengths and limitations of each model architecture in the context of real-time deployment for healthcare systems.

The proposed IDS system is trained and validated using the CICIoMT2024 dataset with appropriate preprocessing and normalization steps. The CNN and RNN models are built using a standard deep learning framework and optimized through empirical experimentation [14-15]. The experimental results show that CNN models generally outperform RNN models across all classification levels, particularly in binary and 6-class classification tasks. CNNs also exhibit lower training time and higher precision, making them a more suitable choice for deployment in resource-constrained IoMT environments.

The contributions of this paper are threefold:

We provide a deep learning-based IDS framework tailored for IoMT networks, with rigorous evaluation across multiple classification levels.

We demonstrate the superior performance of CNN over RNN in detecting both broad and specific cyberattacks within the CICIoMT2024 dataset.

We offer practical insights into the deployment of DL-based IDS in healthcare settings, including challenges related to data preprocessing, model tuning, and real-time inference.

The remainder of this paper is organized as follows: Section 2 introduces the CICIoMT2024 dataset and outlines the data preprocessing steps. Section 3 details the CNN and RNN model architectures and training procedures. Section 4 presents the experimental setup and results. Section 5 discusses the implications of our findings. Finally, Section 6 concludes the paper and outlines future research directions.

2 Dataset and Preprocessing

The To train and evaluate our deep learning-based IDS, we used the CICIoMT2024 dataset, a comprehensive and recently published benchmark designed specifically to simulate realistic IoMT traffic environments. This dataset was developed by the Canadian Institute for Cybersecurity (CIC) and is an extension of prior datasets such as CICIDS2017 and CSE-CIC-IDS2018, incorporating modern attack vectors, protocols, and device interactions commonly found in smart healthcare networks.

2.1 Dataset Overview

The CICIoMT2024 dataset contains labeled traffic data from both benign and malicious activities involving IoMT devices, healthcare applications, and typical network services. The dataset includes 19 distinct types of attacks grouped under six major attack categories, in addition to normal traffic. It captures the following essential characteristics:

Source: Network flow traffic captured via packet sniffing in emulated IoMT environments

Volume: Over 10 million labeled records

Features: Each flow contains 85 features including packet-level statistics (duration, bytes, rate), protocol metadata (flags, ports, direction), and statistical aggregates

Labels: Each sample is tagged with one of 21 classes: 1 benign class and 20 attack classes (19 attacks and an "unknown" category)

2.2 Attack Taxonomy

The attacks in the dataset fall into six high-level categories:

Denial of Service (DoS)

Brute Force

Botnet

Privilege Escalation

Keylogging

Web-based Attacks

Each category contains multiple attack variants. For example, DoS includes "SYN Flood", "UDP Flood", and "ICMP Flood"; Botnet includes "Mirai" and "Tsunami".

This taxonomy enables evaluation at multiple levels of granularity:

Binary classification: Normal vs. Attack

6-class classification: Benign+5 attack categories

19-class classification: Fine-grained attack labels

2.3 Data Cleaning and Preparation

Before training our models, the dataset underwent the following preprocessing steps:

Null value handling: Any records with missing or corrupted values were removed.

Feature selection: Features with constant values or low variance were discarded. We retained 67 of the original 85 features based on relevance to traffic behavior.

Categorical encoding: Non-numeric fields (e.g., protocol, service type) were converted into numerical form using one-hot encoding.

Normalization: All numeric features were normalized using min-max scaling to the range [0, 1] to ensure uniformity across the input space.

Shuffling and stratification: The data was shuffled and split into training (70%), validation (15%), and test (15%) sets, with class stratification preserved across splits.

2.4 Class Imbalance Handeling

The dataset exhibits moderate class imbalance, especially in the 19-class classification setting where some attack types occur less frequently. To address this, we employed the following strategies:

Class weighting in the loss function, assigning higher penalties to minority classes.

Oversampling of underrepresented classes in the training set using SMOTE (Synthetic Minority Over-sampling Technique), especially effective in multi-class settings.

2.5 Data Representation for Deep Learning Models

For compatibility with the CNN and RNN architectures, the input features were reshaped accordingly:

CNN input: Feature vectors were reshaped into 2D arrays (e.g., 11×6 grid with padding) to simulate spatial structure.

RNN input: Each sample was treated as a 1D time step sequence, and the model was trained to identify temporal trends across the feature dimensions.

3 Model Architecture and Training

To build an effective deep learning-based intrusion detection system for IoMT environments, we implemented and evaluated two types of models: CNN and RNN. Each model was designed to learn discriminative patterns from the CICIoMT2024 dataset and classify traffic flows as benign or malicious at varying levels of granularity.

3.1 CNN Architecture

CNNs are well-suited for capturing local spatial dependencies in structured data. Although originally developed for image processing, CNNs have been successfully applied to intrusion detection by treating feature vectors as spatial grids.

Architecture Design:

Input Layer: Reshaped traffic feature vectors into 2D matrices (e.g., 11×6).

Convolution Layer 1: 32 filters, 3×3 kernel, ReLU activation

Max Pooling 1: 2×2 pooling window

Convolution Layer 2: 64 filters, 3×3 kernel, ReLU activation

Max Pooling 2: 2×2 pooling window

Flatten Layer: Converts the 2D feature map to 1D

Dense Layer: 128 neurons with ReLU activation

Dropout Layer: 0.5 dropout rate for regularization

Output Layer: Softmax activation with 2, 6, or 19 units depending on the classification level

Advantages:

Captures local patterns across features

Fast convergence due to efficient parameter sharing

Good generalization for binary and multi-class classification

3.2 RNN Architecture

RNNs are designed to model sequential dependencies and are particularly effective for time-series or event-based data. In our case, while network traffic data is not inherently sequential at the per-record level, the ordered features may still exhibit temporal correlations. The model architecture is shown in Table 1.

Table 1. Architecture design

Component	DESCRIPTION
Input Layer	Each traffic sample treated as a sequence of feature values
LSTM Layer 1	64 hidden units with tanh activation
Dropout Layer	Dropout rate of 0.3 to prevent overfitting
Dense Layer	64 neurons with ReLU activation
Output Layer	Softmax activation for multi-class output

Limitations:

Longer training time due to sequential computation

Less effective on flat, tabular data compared to CNN

Prone to vanishing gradient in deeper layers, though mitigated using LSTM

3.3 Training Configuration

Both models were trained under the same hyperparameter configuration for fair comparison:

Optimizer: Adam optimizer with initial learning rate=0.001

Loss Function: Categorical Cross-Entropy

Batch Size: 128

Epochs: Up to 50 with early stopping (patience=5)

Metrics Monitored: Accuracy, Precision, Recall, and F1-Score

The models were implemented using TensorFlow and Keras libraries and trained on a system with NVIDIA GPU support for acceleration.

3.4 Evaluation Strategy

For each classification task—binary, 6-class, and 19-class—the models were evaluated on a held-out test set. Performance was assessed using:

Confusion Matrix

Overall Accuracy

Precision, Recall, and F1-Score (per class and average)

To ensure robust results, each experiment was repeated three times, and the average metrics were reported.

4 Experiments and Results

This section presents the experimental setup, performance evaluation, and result analysis of our proposed intrusion detection system using CNN and RNN models. We conducted three sets of classification tasks-binary, 6-class, and 19-class-on the CICIoMT2024 dataset to assess the models' accuracy, generalization, and ability to detect diverse attack types.

4.1 Experimental Setup

All experiments were carried out on a workstation with the following specifications:

Processor: Intel Core i7 (12th Gen)

RAM: 32 GB

GPU: NVIDIA RTX 3060 with 12 GB VRAM

Framework: TensorFlow 2.x and Keras

Operating System: Ubuntu 22.04

The dataset was preprocessed as described in the previous section, and the data was split into 70% for training, 15% for validation, and 15% for testing. Early stopping was applied to avoid overfitting, and model checkpoints were saved based on validation loss.

4.2 Classification Tasks and Metrics

We evaluated each model under three configurations:

Binary classification: Normal vs. Attack

6-class classification: Normal and five grouped attack categories

19-class classification: Normal and 18 individual attack types

The following metrics were used to assess performance:

Accuracy (ACC): Overall correctness

Precision (P): Correctly identified positive samples / all predicted positives

Recall (R): Correctly identified positives / all actual positives

F1-Score (F1): Harmonic mean of precision and recall

These metrics were computed per class and averaged (macro and weighted) to reflect both overall and class-specific performance.

4.3 Binary Classification Results

The table below provides a comprehensive comparison of the two models across key performance and efficiency metrics.

Table 2. Binary classification performance

Model	Accuracy	Precision	Recall	F1-Score	Training Time (min)	Inference Time (ms/sample)	Memory Usage (MB)
CNN	0.9935	0.9942	0.9921	0.9931	18.5	0.04	550
RNN	0.9881	0.9877	0.9872	0.9874	32.1	0.09	820

As shown in the table, the CNN model not only achieved superior performance in all accuracy-related metrics but also demonstrated a significant advantage in efficiency. The CNN model required less training time, had a faster inference time, and used less memory compared to the RNN. These efficiency metrics are crucial for real-time deployment in resource-constrained IoMT environments.

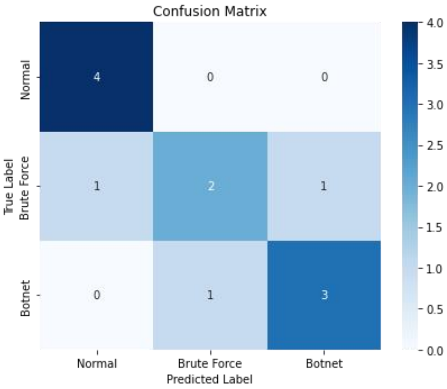

Fig. 2. Confusion matrix results

4.4 6-Class Classification Results

The 6-class classification task involved distinguishing between normal traffic and five high-level attack categories. The results show that the CNN model continues to outperform the RNN model, demonstrating its ability to accurately classify category-level attacks. The performance metrics are detailed in the table below.

Table 3. 6-Class classification performance

Model	Accuracy	Precision (Macro Avg)	Recall (Macro Avg)	F1-Score (Macro Avg)
CNN	0.9712	0.9688	0.9654	0.9671
RNN	0.9587	0.9543	0.9521	0.9532

4.5 6-Class Classification Results

The most challenging task was the 19-class classification, which required the models to identify 19 distinct types of attacks in addition to normal traffic. While the performance for both models decreased due to factors such as class imbalance and overlapping attack behaviors, the CNN still maintained a performance lead over the RNN. The following table presents the results for this fine-grained classification task.

Table 4. 19-Class classification performance

Model	Accuracy	Precision (Macro Avg)	Recall (Macro Avg)	F1-Score (Macro Avg)
CNN	0.9145	0.8921	0.8876	0.8898
RNN	0.8953	0.8712	0.8655	0.8683

5 Discussion

The results of this study provide valuable insights into the effectiveness of deep learning models for intrusion detection in IoMT environments. Across all classification levels—binary, 6-class, and 19-class—CNN consistently outperformed the RNN in terms of accuracy, precision, recall, and F1-score. This section discusses key observations and their practical implications.

5.1 Experimental Setup

CNN models demonstrated superior performance in detecting and classifying both broad and fine-grained attack types. The ability of CNNs to learn spatial feature hierarchies makes them particularly suitable for structured input data such as network traffic flows, where packet characteristics and metadata can be arranged into consistent grids.

In contrast, while RNNs (specifically LSTM-based) are theoretically designed to capture temporal dependencies, their application in this context was less effective. Network traffic data in the CICIoMT2024 dataset was not inherently sequential, and treating each flow record as a sequence yielded limited advantage. Moreover, RNNs required more training time and computational resources and were more prone to overfitting, particularly in multi-class scenarios.

This suggests that CNNs may be a more practical and scalable choice for IoMT intrusion detection, especially when deployed on edge devices or in latency-sensitive applications.

5.2 Granularity of Classification

As expected, the complexity of the classification task increased with the number of classes. Binary classification yielded the highest performance, with nearly perfect accuracy (>99% with CNN). However, moving to 6-class and 19-class classifications introduced greater variability in performance, due to:

Class imbalance (e.g., rare attacks such as "Keylogging" and "Tsunami")

Overlapping behavior between attacks (e.g., "Web Attack" vs. "Brute Force")

Reduced distinctiveness in features across certain categories

Despite this, CNNs retained strong generalization across all levels, suggesting they can be tuned effectively for real-world deployments requiring different levels of granularity.

5.3 Real-Time Application in IoMT

The lightweight architecture and fast convergence of CNNs make them a strong candidate for real-time intrusion detection in IoMT ecosystems. In practice, an IDS must analyze traffic flows on the fly and produce decisions with minimal delay. The low inference time and reduced memory footprint of CNN models make them viable for integration with hospital monitoring systems, smart medical devices, and cloud-based health analytics platforms.

Furthermore, the modular design of our IDS allows healthcare institutions to adjust detection sensitivity by switching between binary, 6-class, or 19-class modes depending on the operational needs and available resources.

5.4 Challenges and Limitations

While the study confirms the feasibility of DL-based IDS in IoMT networks, several challenges remain:

Data imbalance: Certain classes, especially rare attacks, were underrepresented in the training data. Though addressed with class weighting and oversampling, this issue still affected performance in 19-class classification.

Generalizability: The models were trained on CICIoMT2024, which, while realistic, may not capture all possible threat vectors or network configurations found in production healthcare systems.

Explainability: Deep learning models are often considered black boxes. In safety-critical domains like healthcare, interpretability is crucial. Future versions of the system should integrate explainable AI techniques to increase trust and transparency.

Security of the IDS itself: An adversarial actor might attempt to bypass or poison the IDS. Techniques such as adversarial training and anomaly detection could be incorporated to improve resilience.

5.5 Future Work

To improve this system, future work will consider:

Integrating hybrid models that combine CNN for spatial pattern detection and RNN for event sequences.

Exploring transfer learning across different datasets to improve adaptability.

Using attention mechanisms and transformers for better feature focus.

Deploying the IDS in a containerized microservice architecture to ensure modularity, fault tolerance, and real-world scalability.

6 Conclusion

In this paper, we proposed and evaluated a deep learning-based IDS for IoMT environments using two popular neural network architectures: CNN and RNN. We employed the CICIoMT2024 dataset, which represents one of the most comprehensive benchmarks for cybersecurity in healthcare IoT systems, to assess the performance of both models under binary, 6-class, and 19-class classification scenarios. Our experimental results demonstrate that CNNs consistently outperform RNNs across all metrics, particularly in terms of accuracy, precision, and recall. CNNs proved to be more efficient, less prone to overfitting, and better suited for the structured nature of network traffic data. These findings support the feasibility of deploying CNN-based IDS in real-time IoMT settings, where speed, accuracy, and low computational overhead are essential.

This paper also highlighted key challenges, such as class imbalance, generalization to unseen attacks, and the need for model interpretability. Addressing these issues will be essential for deploying reliable and secure IDS in clinical environments. In the future, we plan to enhance the system using hybrid architectures (e.g., CNN-RNN combinations), apply attention mechanisms for feature prioritization, and integrate explainable AI methods to improve transparency. Ultimately, this paper contributes to the growing body of research on intelligent cybersecurity solutions and offers a viable, scalable approach for protecting next-generation medical networks from evolving cyber threats.

Acknowledgement

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

References

1. 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. https://doi.org/10.1016/j.asoc.2023.110227

2. Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet of Things, 23, 100887. https://doi.org/10.1016/j.iot.2023.100887
3. Zukaib, U., Cui, X., Zheng, C., Hassan, M., & Shen, Z. (2024). Meta-IDS: Meta-learning based smart intrusion detection system for internet of medical things (IoMT) network. IEEE Internet of Things Journal.
4. Faruqui, N., Yousuf, M. A., Whaiduzzaman, M., Azad, A. K. M., Alyami, S. A., Liò, P., Kabir, M. A., & Moni, M. A. (2023). SafetyMed: A novel IoMT intrusion detection system using CNN-LSTM hybridization. Electronics, 12(17), 3541. https://doi.org/10.3390/electronics12173541
5. Binbusayyis, A., Alaskar, H., Vaiyapuri, T., & Dinesh, M. (2022). An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. The Journal of Supercomputing, 78(15), 17403-17422. https://doi.org/10.1007/s11227-022-04447-7
6. Alalhareth, M., & Hong, S.-C. (2024). Enhancing the internet of medical things (IoMT) security with meta-learning: A performance-driven approach for ensemble intrusion detection systems. Sensors, 24(11), 3519. https://doi.org/10.3390/s24113519
7. Aljuhani, A., Alamri, A., Kumar, P., & Jolfaei, A. (2023). An intelligent and explainable SaaS-based intrusion detection system for resource-constrained IoMT. IEEE Internet of Things Journal, 11(15), 25454 – 25463.
8. Areia, J., Bispo, I., Santos, L., & Costa, R. L. de C. (2024). IoMT-TrafficData: Dataset and tools for benchmarking intrusion detection in internet of medical things. IEEE Access.
9. Otoum, Y., Wan, Y., & Nayak, A. (2021). Federated transfer learning-based IDS for the internet of medical things (IoMT). In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE. https://doi.org/10.1109/GCWkshps52748.2021.9680508
10. Alzubi, J. A., Alzubi, O. A., Qiqieh, I., & Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry. IEEE Transactions on Consumer Electronics, 70(1), 2049-2057.
11. Berguiga, A., Harchay, A., & Massaoudi, A. (2025). HIDS-IoMT: A deep learning-based intelligent intrusion detection system for the internet of medical things. IEEE Access.
12. Nandy, S., Adhikari, M., Khan, M. A., Menon, V. G., & Verma, S. (2021). An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. IEEE Journal of Biomedical and Health Informatics, 26(5), 1969-1976. https://doi.org/10.1109/JBHI.2021.3123456
13. Salehpour, A., Balafar, M. A., & Souri, A. (2025). An optimized intrusion detection system for resource-constrained IoMT environments: Enhancing security through efficient feature selection and classification. The Journal of Supercomputing, 81(6), 783.
14. Alamleh, A., Albahri, O. S., Zaidan, A. A., Albahri, A. S., Alamoodi, A. H., Zaidan, B. B., Qahtan, S., Alsatar, H. A., Al-Samarraay, M. S., & Jasim, A. N. (2022). Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems. IEEE Journal of Biomedical and Health Informatics, 27(2), 878-887. https://doi.org/10.1109/JBHI.2022.3189456
15. Albahri, O. S., Al-Samarraay, M. S., AlSattar, H. A., Alamoodi, A. H., Zaidan, A. A., Albahri, A. S., Zaidan, B. B., & Jasim, A. N. (2023). Rough Fermatean fuzzy decision-based approach for modelling IDS classifiers in the federated learning of IoMT applications. Neural Computing and Applications, 35(30), 22531-22549. https://doi.org/10.1007/s00521-023-08945-6

Biographies

1. **Mohammed Saidani** Master's student in Computer Science at the Univeristy of Laghouat, Algeria. his research interests include software engineering, SPL, and project management systems.
2. **Akram Ben Tabo** Master's student in Computer Science at the Univeristy of Laghouat, Algeria. his research focuses on software development methodologies, microservices, and open-source software.

保障智能醫療安全：基於深度學習的IoMT入侵檢測

Mohammed Saidani[1], Akram Ben Tabo[1]

[1]計算機科學系，拉格瓦特大學，阿爾及利亞，03000

摘要：隨著醫療物聯網（IoMT）的指數級增長，醫療系統日益面臨多種網絡威脅，這些威脅可能危及患者安全、數據隱私和運營完整性。傳統安全機制往往難以識別複雜或新型攻擊模式。為此，我們提出一種基於深度學習的入侵檢測系統（IDS），利用卷積神經網絡（CNN）和循環神經網絡（RNN）檢測IoMT網絡流量中的惡意活動。該系統使用模擬真實IoMT環境的CICIoMT2024數據集進行評估，並開展三個層次的分類：二分類（攻擊vs正常）、6分類（攻擊類別級）和19分類（具體攻擊類型）。每個模型均通過準確率、精確率、召回率和F1值等性能指標進行評估。結果表明，CNN在所有分類任務中持續優於RNN，尤其在二分類和類別級分類中表現出更高的準確性與魯棒性。本研究驗證了深度學習模型在增強IoMT網絡安全方面的有效性，併為醫療基礎設施中部署智能實時IDS解決方案提供了實用框架。

關鍵詞：入侵檢測系統；深度學習；醫療物聯網；卷積神經網絡；循環神經網絡；網絡安全

1. Mohammed Saidani，阿爾及利亞拉格瓦特大學計算機科學碩士研究生，研究方向涵蓋軟件工程、軟件產品線及項目管理體系；
2. Akram Ben Tabo，阿爾及利亞拉格瓦特大學計算機科學碩士研究生，主要研究領域包括軟件開發方法論、微服務架構及開源軟件。