# Enhancing Security in Connected Medical IoT Networks through Deep Learning-Based Anomaly Detection

Ismaila Sy, Birahime Diouf, Abdou Khadre Diop, Cyril Drocourt, David Durand

# Enhancing Security in Connected Medical IoT Networks through Deep Learning-Based Anomaly Detection

Ismaila SY[1] [0009-0007-7328-7849], Birahime DIOUF[1] [0000-0002-4384-6335],
Abdou Khadre DIOP[1] [0000-0002-1672-6047], Cyril DROCOURT[2] [0000-0003-1636-9462],
David DURAND[2] [0000-0001-8086-8886]

[1] Université Alioune Diop de Bambey, Sénégal
[2] Université de Picardie Jules Verne, France

ismaila.sy@uadb.edu.sn, cyril.drocourt@u-picardie.fr,
abdoukhadre.diop@uadb.edu.sn,
birahime.diouf@uadb.edu.sn, david.durand@u-picardie.fr

**Abstract.** In recent years, there has been an alarming increase in cyberattacks targeting connected medical devices. Distributed denial of service (DDoS) and botnet attacks are particularly common, and many vulnerabilities in IoT systems make these devices particularly vulnerable. Traditional intrusion detection techniques often fall short in addressing these threats. To overcome this challenge, we propose a deep learning-based intrusion detection system (IDS) for connected medical devices that utilizes four different architectures: multilayer perceptron (MLP), long short-term memory (LSTM), convolutional neural network (CNN), and hybrid CNN-LSTM. We evaluated our system on the UNSW-NB15 and Edge-IIoTset datasets, and achieved a classification accuracy of 99.8% for binary classification and 96% for multiclass classification, with a false alarm rate of less than 2%. Our results show that deep learning can be an effective tool for detecting fraud attacks in connected medical devices. This research aims to enhance the security posture of medical IoT systems and mitigate potential risks.

**Keywords:** Cybersecurity, Deep learning, IDS, IoT, Medical Data.

## 1 Introduction

Every second, 127 new devices connect to the Internet for the first time (McKinsey Digital). The number of connected devices is following an exponential curve, rising from 15 billion in 2015 to 30 billion in 2020 and 75 billion in 2025 (Statista). This curve is likely to increase even faster with the arrival of 5G wireless technology, developed in part for the IOT world and enabling deployment in private networks.
The business sectors concerned by IoT are wide-ranging: in 2018, they were mainly geared towards smart cities (23%), followed by connected industry (17%), with

healthcare accounting for just 6% (iot-analytics.com), but growing fast. In 2019, 86% of companies in the healthcare sector were using connected objects (Comparitech, i-SCOOP). By 2020, according to Forbes, 646 million IoT devices will be in use in hospitals, clinics and doctors' surgeries.
In the medical IoT domain, connected networks enable real-time patient monitoring, seamless data collection, and enhanced healthcare delivery. However, this integration also poses inherent security risks that pose significant threats to patient confidentiality, data integrity, and overall network security. Implementing IoT security measures and finding suitable storage solutions will be the top priorities in the near future. To mitigate these risks, robust security measures are imperative [1].
Traditional intrusion detection methods, such as rule-based IDSs and signature-based IDSs, have shown their limitations in effectively detecting and adapting to new threats emerging in dynamic IoT environments. This inherent limitation prompts the exploration of more sophisticated and adaptive solutions, among which deep learning stands out. Deep learning, renowned for its exceptional capabilities in pattern recognition and anomaly detection tasks, emerges as a promising avenue to address the evolving challenges posed by the intricacies of IoT security.

In this paper, we make a significant contribution by employing a diverse set of deep learning methods for enhancing security in connected medical IoT networks. Specifically, we utilize three powerful deep learning models: Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) to implement our anomaly detection approach. This multi-model strategy allows us to leverage the strengths of different architectures, ensuring a comprehensive coverage of potential threats.

Our primary research objective is twofold: first, to achieve a high level of accuracy in identifying security threats in medical IoT networks, and second, to minimize the false positive rate. Through extensive experiments using real-world data (Edge-IIoTset), we have demonstrated high performance. The results display precision rates of 99.8% in binary classification and 96% in multi-class classification. This underscores the efficacy of our deep learning-based approach in accurately identifying and classifying security threats in the complex and dynamic medical IoT environment.

Moreover, our work stands out in its success in substantially reducing false alarm rates. By leveraging advanced deep learning techniques, we have significantly enhanced the precision of our intrusion detection system, ensuring that security alerts are more reliable and actionable. This reduction in false positives is critical in preventing unnecessary disruptions and resource wastage, making our approach not only accurate but also highly practical for real-world deployment.

In summary, our research contributes to advancing the state-of-the-art in connected medical IoT network security by employing a multi-model deep learning approach that not only achieves exceptional accuracy but also significantly reduces false alarm rates.

This innovative methodology holds great promise for safeguarding patient data and improving the overall quality of healthcare delivery in the rapidly evolving digital landscape.
In the upcoming sections, we conduct a comprehensive review of the security issues within connected medical IoT networks and the current methods for identifying anomalies. Ultimately, we summarize the primary outcomes and suggest potential paths for future research to bolster security in linked medical IoT networks.

## 2 Literature Review

Numerous researchers and experts have recognized the gravity of the situation and are actively studying the security aspects of IoMT. Johnson [2] emphasized the need to address security concerns in the context of the Internet of Things in healthcare. Uslu [3] delved into the specific security and privacy implications of the Internet of Medical Things, underscoring the urgency of robust protection measures. Zeadally et al. [4] provided an extensive survey on IoT security, encompassing IoMT as a critical domain. Additionally, Kocabas et al. [5] conducted a comprehensive review of recent advancements and future directions in IoMT, with a particular focus on security implications. Ferrag et al. [6] have conducted a deep learning investigation for intrusion detection. They evaluates the models performances based on accuracy, false alarm rates, and detection rates. The CNNs showed more satisfactory performances than the FFN (Feedforward Neural Network) and RNN (Recurrent Neural Network). Odetola et al. [7] develop a multi-label classification method using a CNN on edge IoT devices. They also discuss recent research on IoT security, focusing on intrusion detection techniques based on neural network strategies. Tian et al. [9] proposed a distributed approach to identify cyber threats via URLs using deep learning algorithms. Their framework can be practically effective due to its automated collection functions, ease of upgradeability and reliability in defending against attacks on distributed deep models. In a big data situation, Hassan et al. [10] have concocted a way to determine break-ins that involve a combination of a Weight-Dropped Long Short-Term Memory (WDLSTM) model and a CNN model. Liu et al. [11] proposed a hybrid approach that combines data sampling, cost-sensitive learning, ensemble learning, and deep learning for intrusion detection in imbalanced network traffic. In [12], the authors propose an approach based on Deep Transfer Learning (DTL) for IoT attacks detection. They have performed three series of experiments on recent datasets and the experimental results show that the DTL model brings an improvement on the accuracy of detection compared to classical approaches. Kandhro et al. [13] presents a generative adversarial network for detecting cyber threats in IoT-driven IIC networks. Their approach is evaluated with the KDDCup99, NSL-KDD and UNSW-NB15 datasets. The results show an increase in performance between 95 % and 97 % in terms of accuracy, reliability and efficiency in detecting numerous attacks.
Wang et al. propose an anomaly detection model tailored for Industrial Control Systems (ICS), employing a deep residual Convolutional Neural Network (CNN). The model

strategically incorporates transfer learning to identify unknown attacks, thereby minimizing training time [14]. Nevertheless, it is important to note that the model relies on a dataset containing known attacks for effective operation.
In order to address the limitations of traditional machine learning techniques in detecting and classifying attacks in IoT networks, a novel anomaly-based intrusion detection model using deep learning, specifically convolutional neural networks (CNNs), is proposed by [15]. The proposed model is implemented in 1D, 2D, and 3D, and is evaluated using four different IoT intrusion detection datasets. Transfer learning is also used to implement binary and multiclass classification using a pre-trained CNN model. The proposed model achieves high accuracy, precision, recall, and F1 score compared to existing deep learning implementations.
To enhance the security of edge networks, L. Nie et al. [16] propose a deep learning-based intrusion detection algorithm based on the generative adversarial network (GAN). Their method includes three phases: feature selection, deep learning architecture design, and intrusion detection model combination. The proposed method achieves high accuracy in detecting multiple attacks, suggesting that GAN-based deep learning is a promising approach for intrusion detection in edge networks.

To identify IoT devices and/or IP addresses that are compromised by a Botnet attack, E. Gelenbe and M. Nakıp [17] propose a novel online Compromised Device Identification System (CDIS). CDIS uses an Auto-Associative Dense Random Neural Network (AADRNN) to train itself online during normal operation, using traffic metrics measured as traffic arrives. Experimental evaluation on publicly available Mirai Botnet attack data shows that CDIS achieves high performance with Balanced Accuracy of 97%, despite its low on-line training and execution time.
Y. K. Saheed et al. [18] propose a novel intrusion detection system (IDS) for the Internet of Medical Things (IoMT) using a deep recurrent neural network (DRNN) and supervised machine learning (SML) models. They first preprocess and normalize the network data, and then optimize the features using a bio-inspired particle swarm algorithm. Finally, they evaluate the proposed DRNN and SML models on a standard intrusion detection dataset. The results show that the proposed SML model outperforms existing approaches with an accuracy of 99.76%.

While experiments have undoubtedly made great strides in developing intrusion detection systems, the ongoing challenge lies in finding a delicate balance of accuracy and reducing false positives. Striking the optimal balance of accurately identifying real threats and minimizing false positives is an ongoing pursuit in cybersecurity. This challenge highlights the importance of optimizing intrusion detection methods to minimize the impact of false alarms on system performance and to ensure strong protection against cyber threats.

# 3 Methodological Approach: Deep Learning-Based Anomaly Detection for Strengthening Security in Connected Medical IoT Networks

In this section, we discuss the datasets and methods we use. We will evaluate the performance of the proposed approaches by considering evaluation metrics commonly used for deep learning algorithms, such as recall, accuracy, F1 score, detection rate, and false alarm rate.

## 3.1 Datasets selection

A good dataset is crucial for studying cyberattacks on IoT devices. By using diverse dataset, encompassing both hybrid traffic and specific IoT dataset, we can capture a wide range of attack vectors and scenarios, enhancing its robustness and generalizability. For our study, we utilized a hybrid dataset known as UNSW-NB15, which offers a comprehensive representation of various network traffic scenarios. This hybrid dataset incorporates both normal and attack data instances, making it a valuable resource for training and evaluating intrusion detection systems [19]. In addition to this, we employed the Edge-IIoTset dataset. This dataset focuses on IoT-specific network traffic, allowing us to investigate and enhance the security of connected IoT networks effectively.

## 3.2 Harnessing Deep Learning Algorithms to Safeguard Medical IoT Networks

In the exhilarating era of cyber infrastructure, where challenges in cybersecurity reach new heights, the exploration of vast data reservoirs in networks, operating systems, and information realms demands avant-garde solutions. Deep learning, a true catalyst of machine learning, emerges as the key for Intrusion Detection Systems (IDS), whether rooted in classical signatures or exploring anomalies. Plunging into the realms of classification and prediction, deep learning provides an immediate response by identifying unusual cybernetic patterns, anticipating not only ongoing attacks but also future threats, thereby redefining digital vigilance. With remarkable ingenuity, deep learning meets the escalating demands of Big Data, establishing a robust defense where high-performing IDS minimizes false alarms. In this captivating panorama, our approach highlights the use of deep learning in IDS, incorporating innovative approaches such as MLP, LSTM, CNN, and the hybrid CNN-LSTM, propelling proactive detection of malicious activities in an ever-evolving digital era. This wave of innovation holds crucial importance in the medical domain, accentuating the relevance of its applications and underscoring the critical necessity of resilient cybersecurity in this highly sensitive field.

### A. Multi-layer Perceptrons (MLPs)

Deep Neural Networks (DNNs) constitute a set of neurons organized into a sequence of multiple layers known as Multi-layer Perceptrons (MLPs). They distinguish themselves from traditional Artificial Neural Networks (ANNs) through their depth and the number of layers and nodes (neurons) comprising the network. When an ANN has two or more hidden layers, it is referred to as a deep neural network [20]. These networks aim to model data containing intricate architectures by combining various non-linear transformations (**Fig. 1**).
Rosenblatt[1] introduced the fundamental concept of the perceptron in 1958. The perceptron calculates a single output from multiple real-valued inputs (xi) by forming a linear combination based on its input weights (w) and then passing the output through a non-linear activation function. Mathematically, this can be expressed as follows:

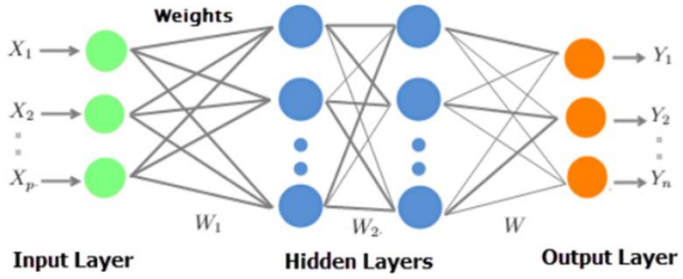
.

$$y = \delta\left(\sum_{n=1}^{n} W_i\ x_i + b\right) = \delta(W^T X + b) \qquad (1)$$

With:

- W: the weight vector.
- X: the input vector.
- b: represents the bias.
- δ: denotes the activation function

A multilayer perceptron network (MLP) consists of a set of source nodes forming an input layer, a hidden layer of one or more compute nodes, and an output layer of nodes. The input signal propagates through the network layer by layer. The signal flow in such a network with hidden layers is shown in Equation (1). Deep neural networks (DNN) are often used for supervised learning problems. During model training (learning), all weights and biases are set to optimal values.




[1] Frank Rosenblatt was an American psychologist who worked on artificial intelligence. As a prominent figure in the "neural network" movement, which aimed to construct artificial intelligence based on the design of the human neural network, he developed the perceptron in 1957 at Cornell University.

**Fig. 1.** The Layered Architecture of Deep Neural Networks (DNN)

### B. Convolutional Neural Networks (CNNs)

A Convolutional Neural Network (CNN) is an extension of traditional feed-forward neural networks (FFNs) inspired by biological factors. Initially designed for image processing, CNNs excel in tasks involving repetitive patterns, such as images with repeated edges and other motifs. CNNs outperform classical machine learning algorithms, achieving significant success in computer vision tasks. They find wide applications in image and video processing, natural language processing (NLP), recommendation systems, and more. Convolutional networks are particularly effective due to specialized layers, including convolutional layers, pooling layers, and fully connected layers (**Fig.2**).

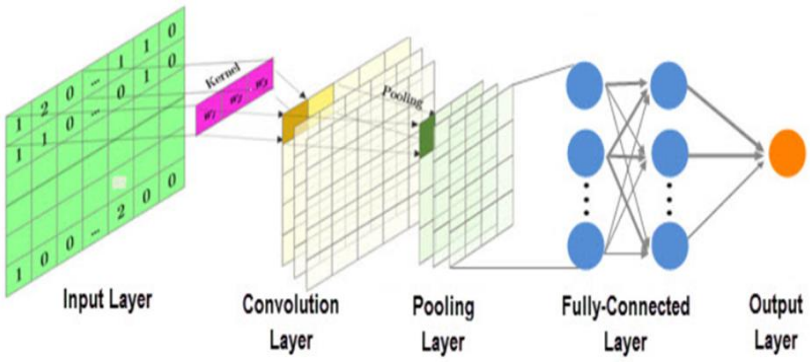



**Fig. 2.** Architectural of a Convolutional Neural Network Model

### C. Long Short-Term Memory units (LSTMs)

The RNN has a long time step as it considers the previously stored state when updating the weights. However, as training progresses, gradients become smaller, and after a few steps, errors may fail to propagate to the end of the network. This result in a negligible difference in the outcome, preventing weight updates. This issue with RNN is known as vanishing gradients. To overcome this problem, a Long Short-Term Memory (LSTM) architecture was proposed in the mid-1990s by German researchers Sepp Hochreiter and Juergen Schmidhuber for recurrent neural networks. Additionally, Gated Recurrent Units (GRU) were introduced to further address the vanishing gradients problem (**Fig.3**). Both LSTM and GRU architectures function similarly, but GRU uses fewer training parameters, requiring less memory and training faster than LSTMs. However, LSTMs tend to be more accurate on datasets with longer sequences [21].

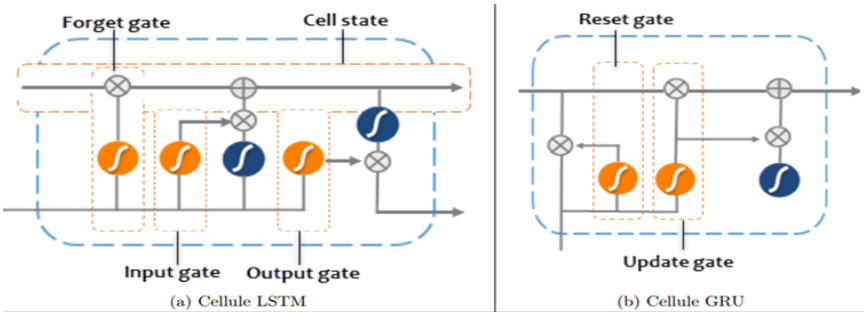



**Fig. 3.** Architectural Overview of LSTM and GRU Models

### D. Hybrid CNN-LSTM network

A hybrid CNN-LSTM network is a combined architecture that integrates Convolutional Neural Network (CNN) layers for feature extraction with Long Short-Term Memory (LSTM) layers for sequence modeling and prediction (**Fig.4**). This hybrid design is often employed in tasks such as visual time series prediction, where CNNs excel at capturing spatial features, and LSTMs handle temporal dependencies, offering a comprehensive approach to complex data patterns and activity recognition [22].

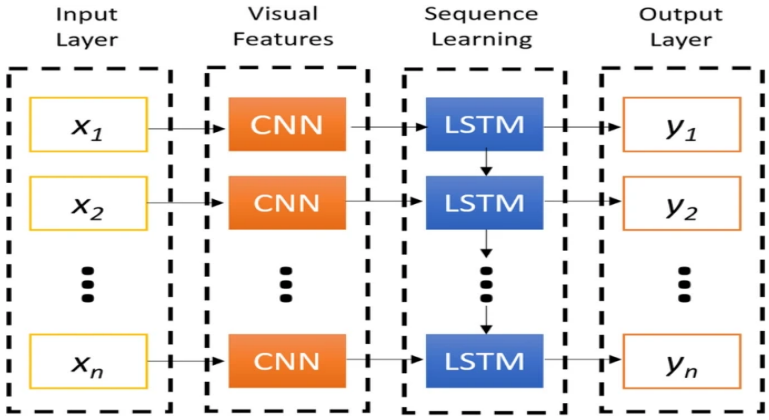



**Fig. 4.** Hybrid CNN-LSTM architecture

### 3.3 A Multi-Architecture Approach to Intrusion Detection in Connected Medical Devices

In this study, we introduce four distinct models: a MLP, CNN, LSTM and a hybrid CNN-LSTM model. Initially, we conduct binary classification, which involves identifying whether the network traffic is normal or malicious. Additionally, we delve into multi-class classification, where we classify the traffic type into either normal or various attack categories, such as DOS, DDOS, or MITM (Man-In-The Middle) attacks (**Fig.5**). This comprehensive approach allows us to accurately categorize and analyze the network traffic patterns for enhanced intrusion detection.
In summary, our methodology involved a dual-step classification process, first determining the normality of traffic versus maliciousness and then identifying the precise type of attack. Utilizing four models, including MLP, LSTM, CNN, and CNN-LSTM, we harnessed their strengths to discern between legitimate and malicious activities while achieving fine-grained attack categorization. This comprehensive approach not only enhances the detection accuracy but also equips cybersecurity practitioners with valuable insights for effective threat mitigation and network defense.

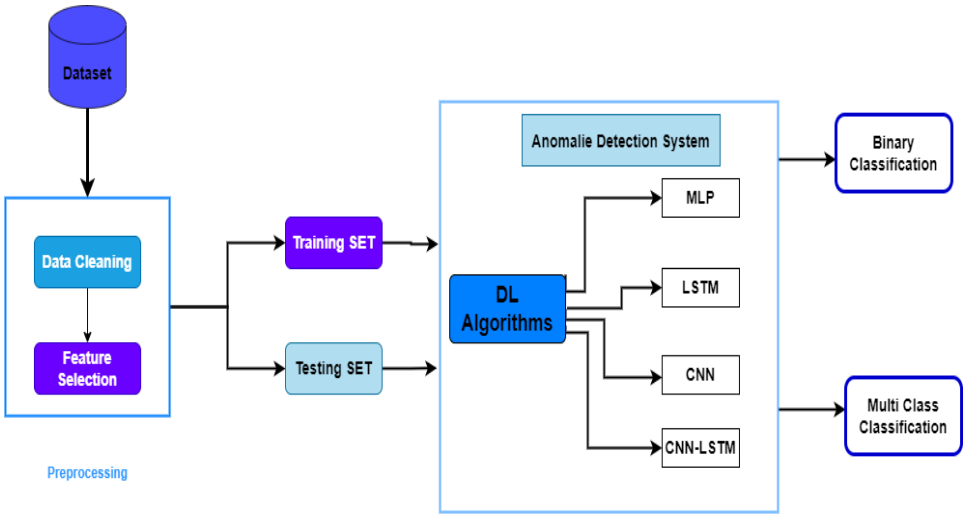



**Fig. 5.** Anomaly Detection Architecture

## 4 RESULTS AND DISCUTIONS

### 4.1 Binary Classification

This process involved training our selected classification models, namely the Multi-Layer Perceptron (MLP), Long Short-Term Memory (LSTM), Convolutional Neural Network (CNN), and a hybrid CNN-LSTM architecture.

**Table 1.** Binary Classification Models Performance

| Model | Accuracy | Validation accuracy | Loss |
|---|---|---|---|
| LSTM_UNSW-NB15 | 93,00 | 94,00 | 0.13 |
| MLP_Edge-IIoTset | 99,99 | 99,80 | 2.67e-04 |
| LSTM_Edge-IIoTset | 99,99 | 99,99 | 9.98e-05 |
| CNN_Edge-IIoTset | 99,99 | 99,87 | 0.16 |
| CNN-LSTM_Edge-IIoTset | 99,98 | 99,97 | 1.13e-04 |

### 4.2 Multi-Class Classification

In the Multi-Class Classification phase, we focused on the challenging task of classifying network traffic into multiple categories. By classifying the data into these six categories, we can gain a better understanding of the different types of attacks present in the dataset and develop more targeted and effective security measures to mitigate these threats. This reclassification provides a clearer and more concise representation of the diverse range of attacks encountered in real-world network traffic, enabling us to enhance the detection and prevention of cyber threats.

**Table 2.** Multi-Class Classification Performances

| | Accuracy | Recall | F1-score | Support |
|---|---|---|---|---|
| Normal | 1.00 | 1.00 | 1.00 | 409200 |
| DDoS | 0.91 | 0.99 | 0.95 | 86434 |
| Code Injection | 0.66 | 0.87 | 0.75 | 30810 |
| Malware | 0.94 | 0.49 | 0.65 | 25094 |
| Information Theft | 0.95 | 0.74 | 0.83 | 21257 |
| MITM | 1.00 | 1.00 | 1.00 | 107 |

In binary classification experiences (**Table 1**), we evaluated several classification models for binary network traffic analysis. The LSTM_UNSW-NB15 model demonstrated good performance with an accuracy of 93.98% on the test dataset, and an even higher accuracy of 94.99% during validation. The MLP_Edge-IIoTset model displayed remarkable accuracy, achieving a perfect 99.99% accuracy on the test dataset and maintaining a very high accuracy of 99.98% during validation. The model's exceptionally low loss value of 2.62e-04 indicates its successful ability to distinguish between normal and malicious network traffic. Additionally, we observed outstanding performance from the LSTM_Edge-IIoTset model, which achieved high accuracy of 99.99% both on the test dataset and during validation. For the CNN_Edge-IIoTset model, an accuracy of 99.98% on the test dataset and a validation accuracy of 99.97% were achieved, with a relatively small loss value of 0.1676, demonstrating robust performance in classifying normal and malicious traffic. Lastly, the CNN_LSTM_Edge-IIoTset model attained a perfect accuracy of 99.98% on both the test dataset and during validation. The model's low loss value of 1.1334e-04 further validates its effectiveness in accurately classifying network traffic.

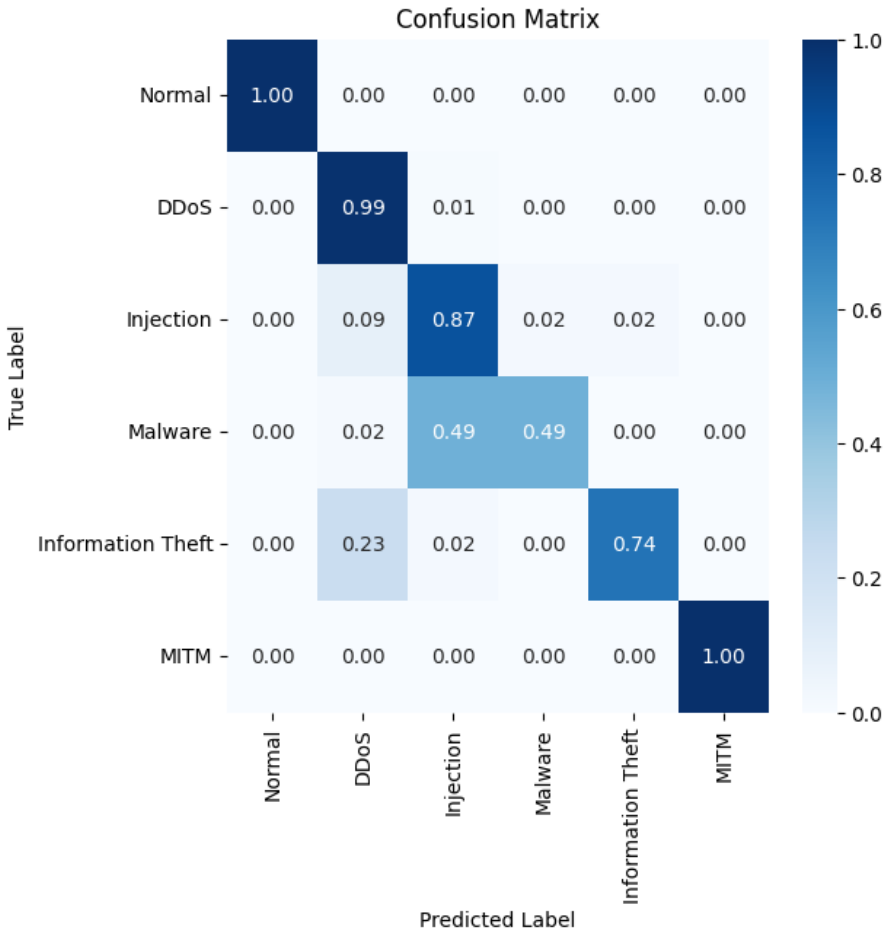



**Fig. 6.** Confusion Matrix for Multiclass Classification

The multiclass classification results (**Table 2)** underscore the model's commendable performance across various attack categories. Notably, the model achieves flawless identification of "Normal" traffic, demonstrating perfect accuracy, recall, and F1-score. The "DDoS" class also exhibits high accuracy and recall, indicative of the model's ability to effectively recognize instances, although the F1-score suggests some instances of misclassification. Challenges arise in the "Code Injection" class, where lower accuracy and F1-score suggest difficulty in precise identification, highlighting an area for potential improvement. In the "Malware" class, the model shows good accuracy but a lower recall, suggesting opportunities to enhance identification sensitivity. The "Information Theft" class demonstrates a balanced and robust performance across metrics. The "MITM" class achieves flawless classification. Importantly, the confusion matrix (**Fig.6**) reveals no instances of attacks misclassified as normal and vice versa, affirming the model's reliability in distinguishing between normal and malicious activities. While

the model performs admirably, targeted improvements in specific classes could further enhance its overall classification capabilities.

## 5 Conclusion

In this study, we present a deep learning based IoT traffic classification. We explore binary and multi-class classifications, differentiating normal and malicious network traffic, and identifying specific attack types within IoT networks. Experimental results validate the efficacy of real-world datasets like Edge-IIoTset for robust model training. However, challenges persist, including the intricacies of IoT ecosystems, model adaptability, and vulnerabilities to adversarial attacks.
Looking ahead, our research suggests integrating deep learning with steganography and Blockchain for more resilient intrusion detection. Incorporating edge computing and federated learning could enhance real-time data processing and privacy.
In conclusion, our deep learning approach strengthens IoT cybersecurity, bolstering intrusion detection and safeguarding patient data and healthcare systems. This study paves the way for future research to develop comprehensive solutions, addressing challenges and contributing to a safer IoT landscape.

### References

1. B. K. Tripathy and J. Anuradha, Eds., Internet of Things (IoT): Technologies, Applications, Challenges and Solutions, 1st ed. CRC Press, Boca Raton, FL, USA, 2017.
2. M. E. Johnson, "The Internet of Things in healthcare: Prospects for the future," Journal of Law and Medicine, vol. 23, no. 4, pp. 923-927, 2016.
3. B. Uslu, İ. Akkaya, and E. G. Sirer, "Security and privacy aspects of the Internet of Medical Things (IoMT)," Current Medical Research and Opinion, vol. 36, no. 5, pp. 805-808, 2020.
4. S. Zeadally, M. A. Tounsi, M. S. Obaidat, and M. E. Hassan, "Security of the Internet of Things: A review of the state of the art," ACM Computing Surveys (CSUR), vol. 47, no. 2, pp. 1-54, 2014.
5. O. E. Kocabas, M. Gumussoy, M. Cetinkaya, and S. Yildirim, "Internet of Medical Things (IoMT): A comprehensive survey on recent advancements and future directions," Journal of Medical Systems, vol. 42, no. 11, pp. 1-20, 2018.
6. M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cybersecurity in the internet of things: Concepts, applications, and experimental analysis," IEEE Access, vol. 9, pp. 138509-138542, 2021.
7. T. A. Odetola, O. Oderhohwo, and S. R. Hasan, "A scalable multi-label classification to deploy deep learning architectures for edge devices," arXiv preprint arXiv:1911.02098, 2019.
8. I. Idrissi, M. Azizi, and O. Moussaoui, "IoT security with deep learning-based intrusion detection systems: A systematic literature review," in 2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS), pp. 1-10, IEEE, 2020.

9. Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1963-1971, 2019.
10. M. M. Hassan, M. A. Hossain, M. S. Uddin, and M. R. Islam, "A hybrid deep learning model for efficient intrusion detection in big data environment," Computers & Security, vol. 87, 101681, 2019.
11. L. Liu, P. Wang, W. Wang, H. Li, and R. Wang, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," IEEE Access, vol. 9, pp. 7550-7563, 2021.
12. L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep transfer learning for IoT attack detection," IEEE Access, vol. 8, pp. 107335-107344, 2020.
13. I. A. Kandhro, S. M. Alanazi, F. Ali, A. Kehar, K. Fatima, M. Uddin, and S. Karuppayah, "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," IEEE Access, vol. 11, pp. 9136-9148, 2023.
14. W. Wang et al., "Anomaly detection of industrial control systems based on transfer learning," in Tsinghua Science and Technology, vol. 26, no. 6, pp. 821-832, Dec. 2021, doi: 10.26599/TST.2020.9010041.
15. I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
16. L. Nie et al., "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 134-145, Feb. 2022, doi: 10.1109/TCSS.2021.3063538.
17. E. Gelenbe and M. Nakıp, "Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices," in IEEE Access, vol. 10, pp. 126536-126549, 2022, doi: 10.1109/ACCESS.2022.3226700.
18. Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 161546-161554, 2021, doi: 10.1109/ACCESS.2021.3128837.
19. Canderra University, "The UNSW-NB15 dataset," Retrieved from https://research.unsw.edu.au/projects/unsw-nb15-dataset, Sydney, Australia, 2018.
20. Yin, Y., Jang-Jaccard, J., Xu, W., et al., "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," Journal of Big Data, vol. 10, no. 15, pp. 1-10, 2023, doi: 10.1186/s40537-023-00694-8.
21. Laghrissi, F., Douzi, S., Douzi, K., et al. "Intrusion detection systems using long short-term memory (LSTM)." Journal of Big Data 8, no. 65, 2021, https://doi.org/10.1186/s40537-021-00448-4.
22. A. Tasdelen and B. Sen, "A hybrid CNN-LSTM model for pre-miRNA classification," Sci. Rep., vol. 11, no. 1, p. 14125, Jul. 2021, doi: 10.1038/s41598-021-93656-0.