LSTM-Driven Multi-Class Intrusion Detection in IoMT Networks with Chi-Square Feature Selection

Kadir Ileri
Electrical and Electronics Engineering
Bandirma Onyedi Eylul University
Balikesir, Türkiye
kileri@bandirma.edu.tr

Abstract— **The Internet of Medical Things (IoMT) has become a vital component of modern healthcare, allowing continuous monitoring, remote diagnosis, and personalized treatment. However, the sensitivity of medical data and the critical nature of healthcare systems make IoMT networks prime targets for cyberattacks. To overcome these challenges, this study introduces an Intrusion Detection System (IDS) based on Long Short-Term Memory (LSTM), specifically designed for IoMT environments. The MedSec-25: IoMT Cybersecurity Dataset is utilized, covering both benign traffic and multiple attack categories, including Exfiltration, Initial Access, Lateral Movement, and Reconnaissance. To improve computational efficiency, Chi-Square filter-based feature selection is employed to reduce the feature set from 83 to 20 features. For validation, Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) models are also implemented for comparison. Among the evaluated models, the proposed Chi-Square + LSTM approach achieved the best results, reaching an accuracy of 0.992751, precision of 0.992724, recall of 0.992751, and an F1-score of 0.992735, thereby demonstrating superior detection accuracy and efficiency.**

Keywords— Chi-Square, Cybersecurity, Feature Selection, Internet of Medical Things (IoMT), Intrusion Detection System (IDS), Long Short Term Memory (LSTM)

I. INTRODUCTION

The swift advancement of the Internet of Things (IoT) has brought significant transformations across various domains, such as smart homes, industrial systems, and healthcare [1]. Among these, the Internet of Medical Things (IoMT) has gained notable momentum, largely driven by the COVID-19 pandemic, which spurred the rapid integration of remote healthcare solutions [2]. IoMT networks enable continuous monitoring, remote diagnosis, and timely medical interventions. As a result, IoMT has become a fundamental component of modern healthcare systems.

IoMT networks typically consist of interconnected sensors, biosensors, and wearable devices that monitor vital signs, medical conditions, and treatment progress of patients [3]. These devices transmit sensitive health data to medical professionals through wireless communication channels, supporting real-time decision-making and personalized healthcare services. The reliability and accuracy of such systems depend heavily on the confidentiality, availability, and integrity of the transmitted data [4].

However, the increasing reliance on IoMT networks introduces serious cybersecurity challenges [5]. Healthcare data, which is highly sensitive and confidential, has become a prime target for cybercriminals. Unauthorized access or manipulation of IoMT data poses serious security risks, as it can compromise patient privacy and hinder critical hospital operations, potentially resulting in life-threatening consequences. Therefore, developing robust Intrusion Detection Systems (IDS) tailored for IoMT environments is crucial to safeguard patient information, ensure secure data transmission, and maintain the resilience of healthcare infrastructure.

A variety of IDSs have been proposed to secure IoMT networks. In one of these studies, [6] introduced a swarm-neural network-based IDS to address security and privacy concerns in patient data transmission. The model was assessed on the NF-ToN-IoT dataset, incorporating telemetry, operating system, and network data, and achieved 89% accuracy, outperforming standard intrusion detection models on the same dataset. A recent work studied in [7] proposed an IDS using a stacking ensemble of deep learning and machine learning models within a Kappa Architecture framework to support real-time data processing. The system effectively detects and classifies various cyberattacks, achieving 0.991 accuracy in binary detection and 0.993 accuracy in multi-class detection, demonstrating the capability of using ensemble learning. Similarly, [8] proposed an IDS using tree-based machine learning classifiers incorporated with filter-based feature selection approaches. The approach applied XGBoost and Mutual Information for feature selection, followed by a set intersection method to extract common features, thereby improving accuracy and reducing computational cost. Evaluated on the CICIDS2017 dataset, the model scored 98.79% accuracy, demonstrating its effectiveness for binary intrusion detection. Furthermore, [9] developed an IDS by integrating Recursive Feature Elimination (RFE) with deep learning and machine learning models, evaluated on the WUSTL-EHMS real-time dataset. The proposed RFE-based Decision Tree achieved accuracy of 97.85%, demonstrating effective anomaly detection in IoMT systems against cyberattacks. In another study, [10] proposed a machine learning-based IDS that employed classifiers such as Decision

Trees, Logistic Regression, Naive Bayes, Random Forest, Adaptive Boosting, Gradient Boosting, and XGBoost. Among these, Adaptive Boosting achieved the best performance on the ToN-IoT dataset across multiple metrics, including accuracy, precision, recall, F1-score, false detection rate, and false positive rate.

[11] proposed a blockchain-driven federated learning-based IDS, addressing privacy and security challenges inherent in centralized ML approaches. The system combines blockchain for secure transaction records, federated learning for local model training, and adaptive Convolutional Neural Network (CNN) model for classification and evaluated on the Edge-IIoTSet and TON-IoT datasets, achieved accuracies 97.43%, and 98.21%, respectively. Similarly, [12] proposed a machine learning-based IDS to mitigate DDoS attacks in blockchain-enabled IoMT networks using the CICIoMT2024 dataset. The study evaluated XGBoost, Decision Tree, and Random Forest models, with the Decision Tree achieving the most efficient prediction time while maintaining high performance across standard classification metrics. Another study [13] explored the use of ensemble learning with meta-learning for IDS. The proposed weighted meta-learning approach adaptively allocates voting weights to classifiers based on confidence, loss, and accuracy, improving detection performance. Experiments demonstrated superior results compared to existing models, highlighting the potential of meta-learning to enhance IDS robustness in IoMT networks.

However, most of these IDSs do not specifically target medical-domain datasets and instead rely on general IoT datasets, which do not accurately represent the unique characteristics of medical network environments. In this research, an LSTM-based IDS is proposed to detect cyberattacks in IoMT networks, specifically targeting a medical-domain dataset. To enhance efficiency, Chi-Square filter-based feature selection is applied to reduce the feature set, thereby lowering computational overhead. For comparative analysis, Recurrent Neural Network (RNN)-based and CNN-based models are also employed, and the results show that the proposed LSTM-driven IDS outperforms these approaches. The main contributions of this study are summarized as follows:

- An LSTM-based IDS is developed for IoMT networks, achieving superior performance compared to other methods reported in the literature on the same dataset.
- The feature set is reduced from 83 to 20 using Chi-Square filter-based feature selection, improving computational efficiency.
- RNN and CNN models are also implemented for comparison to verify the effectiveness of the proposed LSTM-based approach.

The remainder of this paper is organized as follows: Section 2 describes the methods used in this study, Section 3 provides details of the IoMT dataset, Section 4 explains the proposed methodology and preprocessing steps, Section 5 presents and discusses the results, and Section 6 concludes the paper.

II. Methods

This section outlines the methodologies employed in this study. An LSTM-based IDS is proposed for detecting cyberattacks in an IoMT network. The model is designed to perform multi-class classification, enabling it to distinguish between different types of attacks as well as non-attack traffic. To reduce the computational cost of the IDS, Chi-Square feature selection is applied to reduce the number of input features. The principles of Chi-Square feature selection method and the LSTM deep learning approach are described in detail below.

A. Chi-Square

Chi-Square is a statistical method used to evaluate the dependency between the target variable and each feature [14]. In the context of classification, it evaluates the extent to which the actual distribution of feature values differs from the distribution expected under the assumption of independence from the class labels. Features with higher Chi-Square scores are regarded more relevant, as they exhibit a stronger association with the target class. The Chi-Square test statistic is calculated as follows:

$$X^2 = \sum((O_i - E_i)^2/E_i) \tag{1}$$

where:

- E_i is the expected frequency of feature value i,
- O_i is the actual frequency of feature value i,
- X^2 is the Chi-Square score.

B. Long Short-Term Memory (LSTM)

Long Short-Term Memory (LSTM) method is an advanced variant of RNNs modeled to effectively process sequential data, making it highly appropriate for time-series analysis tasks such as network traffic data [15].

Unlike traditional RNNs, which often suffer from the vanishing gradient problem that restricts their capability to preserve information across long sequences, LSTMs overcome this limitation through a unique memory cell architecture. This design enables LSTMs to capture both long-term and short-term temporal dependencies, thereby enhancing their capability to model complex sequential patterns in data [16].

A typical LSTM unit consists of several key components:

- **Cell State**: Operates as the memory of the network, maintaining and transferring important information across time steps. It enables the selective preservation or removal of information through gating mechanisms, thereby facilitating long-term dependency learning.
- **Input Gate:** Regulates the incorporation of new information into the cell state by determining which parts of the previous hidden state and the current input should be stored.

- **Forget Gate**: Controls the disposal of irrelevant or outdated information from the cell state, guaranteeing that only useful knowledge is preserved for future predictions.
- **Output Gate:** Identifies how much of the information from the cell state is exposed to the next hidden state, thereby influencing the output at each time step.

In the context of cyberattack classification, LSTMs can process sequences of network traffic features to learn temporal dependencies that distinguish normal activity from malicious behavior. Attack patterns often evolve over time, with subtle variations in packet sequences or payload structures. LSTMs capture these sequential patterns by mapping the input time-series data into a latent representation and propagating contextual information across multiple time steps. The final hidden state of the LSTM is then passed to dense layers for classification, where softmax or sigmoid activation functions are used depending on whether the task comprises multi-class or binary attack detection.

III. IoMT Intrusion Detection Dataset

The dataset used in this study is the MedSec-25: IoMT Cybersecurity Dataset [17], which is publicly available at https://www.kaggle.com/datasets/abdullah001234/medsec-25-iomt-cybersecurity-dataset (accessed on 17 September 2025). Unlike most existing datasets that rely on generic intrusion detection collections unrelated to IoMT communications, this dataset captures realistic traffic from a custom-built healthcare IoT lab that mimics hospital operations. The lab setup incorporated diverse IoMT devices and protocols (e.g., MQTT, SSH, Telnet, FTP, HTTP, DNS) to reflect real-world communication patterns. The dataset was collected from a range of medical sensors and environmental sensors connected through Raspberry Pi nodes to an IoT server, with network traffic recorded over 7.5 hours. In total, the dataset comprises 554,534 flows, consisting of 83 input features and a single target column.

Data collection was conducted under normal conditions (Benign) and four types of cyberattacks: Reconnaissance, Initial Access, Lateral Movement, and Exfiltration. Comprehensive details of the dataset, including the data collection process, experimental setup, equipment specifications, feature descriptions, and device configurations, are provided in [17]. The dataset was created by collecting network traffic data in a controlled laboratory environment at Rochester Institute of Technology, Dubai, and has been fully anonymized in compliance with privacy regulations such as HIPAA. No personally identifiable information or sensitive patient data were included.

IV. Architecture of Proposed Intrusion Detection System (IDS)

This section presents the architecture of the proposed IDS model employed in this study. The proposed IDS is based on a LSTM network, designed to detect cyberattacks in a IoMT environment. It is capable of performing multi-class classification.

The workflow of the proposed IDS is illustrated in Fig. 1 and consists of two main steps: data preprocessing, and classification. Each of these steps is described in detail below.

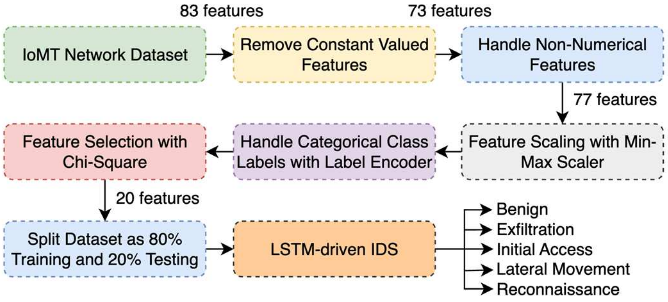
83 features
73 features
IoMT Network Dataset
Remove Constant Valued Features
Handle Non-Numerical Features
77 features
Feature Scaling with Min-Max Scaler
Handle Categorical Class Labels with Label Encoder
Feature Selection with Chi-Square
20 features
Split Dataset as 80% Training and 20% Testing
LSTM-driven IDS
Benign
Exfiltration
Initial Access
Lateral Movement
Reconnaissance

Fig. 1. Workflow Diagram of the Proposed IDS.

A. Data Preprocessing

In the data preprocessing step, features with constant values were first eliminated, as they do not contribute to the learning process. The eliminated features include: Bwd Blk Rate Avg, Fwd Byts/b Avg, Init Fwd Win Byts, Fwd Seg Size Min, Fwd URG Flags, Bwd Pkts/b Avg, Fwd PSH Flags, Fwd Blk Rate Avg, Bwd Byts/b Avg, and Fwd Pkts/b Avg, reducing the number of features to 73.

The dataset contained non-numerical columns such as Timestamp, Src IP, and Dst IP, which needed to be converted into numerical values to enable numerical processing by the machine learning model. The Timestamp attribute was decomposed into new columns representing second, minute, hour, year, month, and day. Both Src IP and Dst IP were transformed into their corresponding integer representations. Additionally, the Flow ID feature was dropped since its information is already captured by other features such as Dst Port, Dst IP, Src IP, and Protocol. After these transformations, the dataset contained 77 features.

The features were standardized using the Min-Max Scaler to normalize the input space. The scaling formula is defined as follows:

$$x' = (x - x^{min})/(x^{max} - x^{min}) \tag{2}$$

where x is the original feature value, x^{max} is the maximum value of the feature, and x^{min} is the minimum value of the feature. Following this, class labels were then encoded into numerical values using a Label Encoder (with mappings as Benign: 0, Exfiltration: 1, Initial Access: 2, Lateral Movement: 3, and Reconnaissance: 4).

Since 77 features is computationally expensive for IDSs, which require fast attack detection, Chi-Square feature selection was applied to reduce the number of features to 20. The selected features include Dst Port, Flow Duration, Flow IAT Std, Flow IAT Max, Fwd IAT Tot, Bwd IAT Tot, Bwd IAT Std, Bwd IAT Max, Bwd PSH Flags, RST Flag Cnt, PSH Flag Cnt, ACK Flag Cnt, Down/Up Ratio, Idle Mean, Init Bwd Win Byts, Idle Min, Idle Max, Month, Day, and Minute. This reduction enhances the computational efficiency of the machine learning model while retaining discriminative power.

Finally, the preprocessed dataset was split into two parts: 80% was used for training the model, while the remaining 20% was set aside for testing its performance.

B. Architecture of the LSTM-driven IDS Model

The proposed model is designed using a sequential architecture comprising one Input layer, one LSTM layer, one Dense layer, two Batch Normalization layers, and two Dropout layers. It initiates with an input layer that receives the preprocessed feature set. A single LSTM layer follows it with 16 hidden units, which captures temporal dependencies within the IoMT communication data. To improve training stability and accelerate convergence, a Batch Normalization layer is employed immediately after the LSTM output. This is followed by a Dropout layer with a rate of 0.3 to mitigate overfitting.

The extracted temporal features are further refined through one fully connected (Dense) layer with 8 neurons, employing the activation function as ReLU. This Dense layer is interleaved with Batch Normalization and Dropout layers to enhance generalization. The architecture concludes with an output Dense layer, utilizing softmax activation function for multi-class classification process.

For training the model, the Adam optimizer was used with a learning rate of 0.0001, which helped the model learn steadily without making sudden jumps in the parameter updates. The loss function was set as categorical cross-entropy, since the task involved multi-class classification and this function is well-suited for handling errors across multiple classes. Training was run for 50 epochs with a batch size of 32, a setup that provided a good balance between training speed and the model's ability to generalize.

V. Results and Discussion

A. Evaluation Metrics

The performance of the proposed LSTM-based IDS was assessed using widely adopted classification metrics, including F1-score, precision, recall, and accuracy. These evaluation metrics are derived from the fundamental evaluation parameters, including False Positives (FP), True Positives (TP), False Negatives (FN), and True Negatives (TN), where TP denotes correctly classified attack instances, TN represents correctly recognized normal traffic, FP corresponds to normal traffic misclassified as attacks, and FN denotes attack instances that were incorrectly classified as normal. Based on these values, the performance metrics are defined as follows:

$$F1 - Score = \frac{2 \times (Recall \times Precision)}{Recall + Presicion} \tag{3}$$

$$Precision\ = TP/(FP + TP) \tag{4}$$

$$Recall\ = TP/(FN + TP) \tag{5}$$

$$Accuracy = (TP + TN)/(FP + TP + FN + TN) \tag{6}$$

B. Discussion of Experimental Results

The performance of the proposed Chi-Square + LSTM model was compared with Chi-Square + RNN, and Chi-Square + CNN models using standard classification metrics: F1-score, precision, recall, and accuracy. The results are summarized in Table 1.

Among the models, the Chi-Square + LSTM approach achieved the highest performance, with an F1-score of 0.992735, precision of 0.992724, recall of 0.992751, and accuracy of 0.992751. The Chi-Square + RNN model also demonstrated strong performance, achieving an F1-score of 0.990654, precision of 0.990630, recall of 0.990740, and accuracy of 0.990740, indicating that incorporating temporal dependencies improves classification results compared to CNN-based models. The Chi-Square + CNN model, while performing well, yielded lower metrics with an F1-score of 0.942138, precision of 0.953244, recall of 0.937641, and accuracy of 0.937641.

The results indicate that combining Chi-Square feature selection with recurrent architectures, particularly LSTM, significantly enhances classification performance. This improvement can be attributed to ability of LSTM to capture long-term dependencies in the feature space, which is especially beneficial for datasets with complex temporal or sequential patterns. The consistent improvement across all evaluation metrics demonstrates the robustness and reliability of the proposed Chi-Square + LSTM model compared to other architectures.

TABLE I. Performance Results of the Classification Models with Feature Selection Process

Model	F1-Score	Precision	Recall	Accuracy
Chi-Square + CNN	0.942138	0.953244	0.937641	0.937641
Chi-Square + RNN	0.990654	0.990630	0.990740	0.990740
Chi-Square + LSTM	**0.992735**	**0.992724**	**0.992751**	**0.992751**

*Best results are in bold.

The class-level performance of the proposed LSTM-based IDS with Chi-Square feature selection method was evaluated to assess its ability to accurately detect each type of attack. In addition proposed IDS, the class-level performances of CNN-based IDS and RNN-based IDS were also assessed. The obtained class-based results of Chi-Square + CNN, Chi-Square + RNN, and Chi-Square + LSTM approaches are given in Table 2, Table 3, and Table 4, respectively.

As shown in Table 2, the Chi-Square + CNN-based IDS achieved perfect detection performance for the Benign class only. The Reconnaissance, Lateral Movement, and Initial Access classes yielded promising results with accuracies of 0.951990, 0.949600, and 0.942502, respectively. The lowest performance was observed in the Exfiltration class with an F1-score of 0.753853, precision of 0.877724, recall of 0.660621, and accuracy of 0.660621.

TABLE II. CLASS-BASED DETECTION PERFORMANCE OF PROPOSED CHI-SQUARE + CNN APPROACH

Class	F1-Score	Precision	Recall	Accuracy
Benign	1.0	1.0	1.0	1.0
Exfiltration	0.753853	0.877724	0.660621	0.660621

Initial Access	0.926016	0.910097	0.942502	0.942502
Lateral Movement	0.579378	0.416857	0.949600	0.949600
Reconnaissance	0.967893	0.984337	0.951990	0.951990

As shown in Table 3, the Chi-Square + RNN-based IDS performed perfect detection for the Benign and Reconnaissance classes, with all metrics equal to 1.0, indicating that these classes are easily recognizable by the approach. The Initial Access class also demonstrated strong performance with an F1-score of 0.999976, precision of 0.999951, recall of 1.0, and accuracy of 1.0. The lowest performance was observed in the Lateral Movement class with an F1-score of 0.787753, precision of 0.815767, recall of 0.761600, and accuracy of 0.761600. The Exfiltration class followed as the second weakest performing one.

TABLE III. CLASS-BASED DETECTION PERFORMANCE OF PROPOSED CHI-SQUARE + RNN APPROACH

Class	F1-Score	Precision	Recall	Accuracy
Benign	1.0	1.0	1.0	1.0
Exfiltration	0.902478	0.888556	0.916844	0.916844
Initial Access	0.999976	0.999951	1.0	1.0
Lateral Movement	0.787753	0.815767	0.761600	0.761600
Reconnaissance	1.0	1.0	1.0	1.0

As given in Table 4, the proposed Chi-Square + LSTM-based IDS achieved perfect detection for the Benign, Initial Access, and Reconnaissance classes, with all metrics equal to 1.0, indicating that these classes are easily distinguishable by the proposed approach. For the Exfiltration class, the model achieved an F1-score of 0.922737, precision of 0.919204, recall of 0.926298, and accuracy of 0.926298, demonstrating strong performance, though slightly lower than the benign classes. The Lateral Movement class posed the greatest challenge, with an F1-score of 0.837903, precision of 0.844715, recall of 0.8312, and accuracy of 0.8312, suggesting some overlap or similarity with other classes.

TABLE IV. CLASS-BASED DETECTION PERFORMANCE OF PROPOSED CHI-SQUARE + LSTM APPROACH

Class	F1-Score	Precision	Recall	Accuracy
Benign	1.0	1.0	1.0	1.0
Exfiltration	0.922737	0.919204	0.926298	0.926298
Initial Access	1.0	1.0	1.0	1.0
Lateral Movement	0.837903	0.844715	0.831200	0.831200
Reconnaissance	1.0	1.0	1.0	1.0

The results state that the Chi-Square + LSTM model is highly effective for multi-class detection, achieving near-perfect performance for most classes while maintaining robust detection for more challenging attack types. This highlights the capability of the proposed IDS to handle imbalanced and complex datasets with diverse attack categories. Furthermore, by lessening the number of features, the IDS enhances computational efficiency, enabling timely and reliable identification of cybersecurity threats within IoMT networks.

C. Comparison of Results with State-of-the-Art Models

The proposed Chi-Square + LSTM approach is evaluated against other models reported in the literature using the same dataset. Decision Tree and K-Nearest Neighbors (KNN) models, as employed in [17], serve as benchmarks. The testing results indicate that the proposed Chi-Square + LSTM model achieves an F1-score of 0.9927 and accuracy of 0.9928, outperforming the Decision Tree model, which achieves an F1-score of 0.9778 and accuracy of 0.9835, as well as the KNN model, which achieves an F1-score of 0.9745 and accuracy of 0.9809. This demonstrates that the Chi-Square + LSTM approach provides a notable improvement in predictive performance across traditional machine learning models. Fig. 2 presents a visual comparison of the accuracies, clearly highlighting the superior performance of the proposed Chi-Square + LSTM approach.

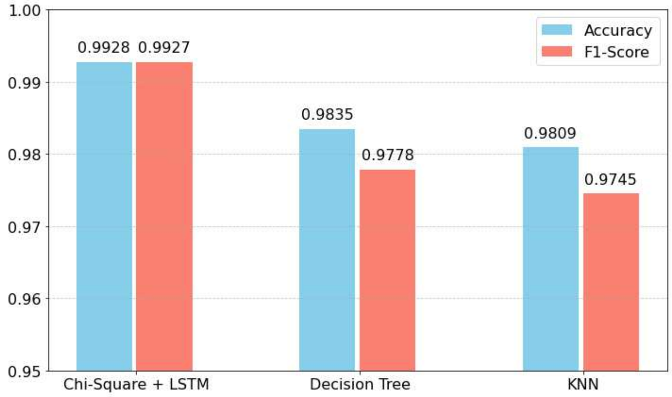

Fig. 2. Performance Comparison of the Proposed Chi-Square + LSTM Approach with the Other Models from the Literature.

VI. CONCLUSION

In this study, an LSTM-based IDS was proposed to enhance the security of IoMT networks using the MedSec-25: IoMT Cybersecurity Dataset. The system was designed to detect both benign and malicious activities, including Exfiltration, Initial Access, Lateral Movement, and Reconnaissance attacks. To improve computational efficiency, Chi-Square feature selection method was applied to reduce the number of features, enabling faster processing. For comparison, RNN-based and CNN-based IDS models were also implemented, and the experimental results demonstrated that the Chi-Square + LSTM technique achieved superior performance across evaluation metrics, outperforming the alternative models.

Despite these promising results, the proposed IDS has certain limitations. Its performance was validated only on a single IoMT dataset, which may restrict its generalizability across different real-world scenarios and diverse IoMT environments. To address this, future research should assess the robustness of the IDS on multiple IoMT datasets to ensure broader applicability. Moreover, the LSTM model can be further enhanced by integrating more advanced deep learning architectures, such as hybrid or attention-based models, to improve detection accuracy and adaptability against evolving cyber threats.

Acknowledgment

This work was financially supported by the Scientific and Technological Research Council of Türkiye (TUBITAK) under the 2224-A - Grant Program for Participation in Scientific Meetings Abroad Programme, grant number 1919B022508945.

References

[1] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," Sensors, vol. 23, no. 16, p. 7194, Aug. 2023, doi: 10.3390/s23167194.

[2] A. A. El-Saleh, A. M. Sheikh, M. A. M. Albreem, and M. S. Honnurvali, "The Internet of Medical Things (IoMT): opportunities and challenges," Wireless Networks, vol. 31, no. 1, pp. 327–344, Jan. 2025, doi: 10.1007/s11276-024-03764-8.

[3] I. Ud Din, A. Almogren, M. Guizani, and M. Zuair, "A Decade of Internet of Things: Analysis in the Light of Healthcare Applications," IEEE Access, vol. 7, pp. 89967–89979, 2019, doi: 10.1109/ACCESS.2019.2927082.

[4] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of Security and Privacy for the Internet of Medical Things (IoMT)," in 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE, May 2019, pp. 457–464. doi: 10.1109/DCOSS.2019.00091.

[5] M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, Jun. 2022, doi: 10.1002/ett.4049.

[6] J. B. Awotunde, K. M. Abiodun, E. A. Adeniyi, S. O. Folorunso, and R. G. Jimoh, "A Deep Learning-Based Intrusion Detection Technique for a Secured IoMT System," 2022, pp. 50–62. doi: 10.1007/978-3-030-95630-1_4.

[7] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, and M. Ilyas, "Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Environments," Sensors, vol. 25, no. 3, p. 624, Jan. 2025, doi: 10.3390/s25030624.

[8] G. Balhareth and M. Ilyas, "Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection," Sensors, vol. 24, no. 17, p. 5712, Sep. 2024, doi: 10.3390/s24175712.

[9] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, and M. El bekkali, "An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system," Results in Engineering, vol. 23, p. 102659, Sep. 2024, doi: 10.1016/j.rineng.2024.102659.

[10] P. Kulshrestha and T. V. Vijay Kumar, "Machine learning based intrusion detection system for IoMT," International Journal of System Assurance Engineering and Management, vol. 15, no. 5, pp. 1802–1814, May 2024, doi: 10.1007/s13198-023-02119-4.

[11] K. Begum, M. A. I. Mozumder, M.-I. Joo, and H.-C. Kim, "BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks," Sensors, vol. 24, no. 14, p. 4591, Jul. 2024, doi: 10.3390/s24144591.

[12] M. Akkal, S. Cherbal, K. Kharoubi, B. Annane, A. Gawanmeh, and H. Lakhlef, "An Intrusion Detection System For Detecting DDoS Attacks In Blockchain-Enabled IoMT Networks," in 2024 7th International Conference on Signal Processing and Information Security (ICSPIS), IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/ICSPIS63676.2024.10812635.

[13] M. Alalhareth and S.-C. Hong, "Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems," Sensors, vol. 24, no. 11, p. 3519, May 2024, doi: 10.3390/s24113519.

[14] L. Ali, A. Rahman, A. Khan, M. Zhou, A. Javeed, and J. A. Khan, "An Automated Diagnostic System for Heart Disease Prediction Based on ${\chi^{2}}$ Statistical Model and Optimally Configured Deep Neural Network," IEEE Access, vol. 7, pp. 34938–34945, 2019, doi: 10.1109/ACCESS.2019.2904800.

[15] I. Malashin, V. Tynchenko, A. Gantimurov, V. Nelyub, and A. Borodulin, "Applications of Long Short-Term Memory (LSTM) Networks in Polymeric Sciences: A Review," Polymers (Basel), vol. 16, no. 18, p. 2607, Sep. 2024, doi: 10.3390/polym16182607.

[16] V. Hnamte and J. Hussain, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," Telematics and Informatics Reports, vol. 10, p. 100053, Jun. 2023, doi: 10.1016/j.teler.2023.100053.

[17] W. Almobaideen, M. Abdullah, U. Alam, S. B. Hussain, and A. Bouharrat, "MedSec-25: Creating an IoMT Dataset for a Healthcare IoT Environment," in 7th International Conference on Blockchain Computing and Applications (BCCA), IEEE, Oct. 2025.