ANOMALY AND ATTACK DETECTION FOR MEDICAL CYBER-PHYSICAL SYSTEMS IN SMART HEALTHCARE

[1] Mrs. D.V.V Deepthi, [2] Gangavarapu Abhishek, [3] Kataram Bhavana, [4] Ganagadi Ram Kishore, [5] Donthireddy Charan Teja Reddy

[1]Assiatant Professor in Department of CSE TKR COLLEGE OF ENGINEERING & TECHNOLOGY

[2,3,4,5]UG Scholars in Department of CSE TKR COLLEGE OF ENGINEERING & TECHNOLOGY

Abstract

The rapid growth of the Internet of Medical Things has transformed the healthcare sector by connecting medical devices, monitoring systems, and healthcare applications through intelligent networks. This advancement has improved patient care and enabled real-time medical services, but it has also created new security challenges. Since IoMT devices continuously exchange sensitive patient information, they have become attractive targets for cyberattacks such as unauthorized access, data breaches, and malicious traffic intrusions. Conventional security solutions are often unable to detect these evolving threats efficiently, especially in complex medical environments where network behavior changes dynamically. To address these issues, this paper presents HIDS-IoMT, a deep learning-based intrusion detection framework designed to improve the security of IoMT networks. The proposed system uses deep learning models to study network traffic behavior and identify suspicious patterns that may indicate cyber threats. By analyzing traffic features and recognizing deviations from normal communication behavior, the framework can detect attacks at an early stage and support timely preventive action. The model is trained on network traffic data to distinguish legitimate activity from malicious behavior with greater accuracy. The effectiveness of the proposed approach is evaluated using performance metrics such as accuracy, precision, recall, and F1-score. The results show that the deep learning-based model performs efficiently in identifying intrusions while reducing false alarms. The proposed HIDS-IoMT system provides an intelligent and scalable solution for enhancing cybersecurity in smart healthcare environments and contributes to the secure operation of connected medical infrastructures.

Keywords

Internet of Medical Things, Intrusion Detection, Deep Learning, Cybersecurity, Anomaly Detection, Healthcare Security

I. INTRODUCTION

The Internet of Medical Things has become an essential part of modern healthcare by connecting medical sensors, wearable devices, diagnostic tools, and hospital systems through internet-based communication networks. This connectivity allows healthcare professionals to monitor patients in real time, improve diagnosis accuracy, and deliver efficient medical services remotely. With the growing use of connected medical devices, IoMT has enhanced the quality of patient care and increased operational efficiency in hospitals and healthcare institutions [1]. However, as healthcare infrastructures become more interconnected, the risks associated with cyber threats also increase.

Security has emerged as one of the most critical concerns in IoMT environments because connected medical devices often handle highly sensitive patient information. Unauthorized access to these systems can lead to privacy

violations, data manipulation, and service disruption. Cyberattacks such as denial-of-service, malware injection, and unauthorized traffic interception can severely affect the performance of medical devices and may even threaten patient safety [2]. Since many IoMT devices have limited computing resources and weak built-in security mechanisms, they are particularly vulnerable to attacks, making effective intrusion detection a necessity [3].

Traditional intrusion detection systems are generally based on predefined attack signatures or manually created rules. While these approaches can detect known threats, they often fail to identify unknown or evolving attack patterns. In IoMT networks, traffic behavior is highly dynamic, and attackers continuously develop new methods to bypass conventional defenses. As a result, rule-based systems generate high false alarm rates and provide limited adaptability in complex healthcare environments [4]. These limitations create the need for intelligent systems capable of learning network behavior patterns and identifying anomalies automatically.

Recent developments in Deep Learning have opened new possibilities for enhancing intrusion detection performance. Deep learning models can process large volumes of network traffic data, extract hidden patterns, and identify malicious activities with improved accuracy. Algorithms such as Long Short-Term Memory and Multi-Layer Perceptron have shown strong capability in recognizing complex traffic behaviors and detecting anomalies in network environments [5]. These techniques are particularly suitable for IoMT networks because they can adapt to changing traffic patterns and improve threat detection efficiency over time A **deep learning-based intelligent intrusion detection system**, named **HIDS-IoMT**, is proposed to strengthen security in IoMT environments. The system is designed to analyze network traffic, extract relevant features, and classify activities as normal or malicious using deep learning techniques. By detecting intrusions in real time and reducing false positives, the proposed framework aims to improve the protection of connected medical devices and ensure secure healthcare communication [6]. This research contributes toward building a reliable and scalable security mechanism for safeguarding IoMT infrastructures against emerging cyber threats.

II. LITERATURE SURVEY

The increasing adoption of the Internet of Medical Things has created new opportunities for improving healthcare services through connected medical devices and real-time patient monitoring. At the same time, this rapid integration of smart medical technologies has introduced major cybersecurity concerns. Because IoMT devices often operate in open and resource-constrained environments, they are vulnerable to a variety of network-based attacks. Researchers have therefore focused on developing efficient intrusion detection systems capable of protecting these networks against both known and unknown threats [1].

Earlier intrusion detection methods mainly relied on signature-based mechanisms to identify malicious activities. These systems compare incoming network traffic against previously stored attack signatures and generate alerts when a match is found. Although this method performs well for known threats, it is ineffective against zero-day attacks or new intrusion patterns. In healthcare environments where new attack methods constantly emerge, such static security mechanisms often fail to provide reliable protection [2].

To address these challenges, machine learning techniques have been introduced into intrusion detection systems to improve their ability to recognize abnormal behavior. Models such as Decision Trees, Random Forest, and Support Vector Machines are widely used for classifying

network traffic into normal and malicious categories. Among these methods, Random Forest has shown strong performance due to its ability to handle large datasets and reduce overfitting while maintaining high classification accuracy [3]. These methods offer better adaptability than traditional approaches, but they still depend on manual feature extraction and may not effectively capture hidden patterns in complex traffic flows.

Recent studies have shown that Deep Learning can significantly improve the performance of intrusion detection systems by automatically learning complex traffic patterns from data. Deep learning models are capable of extracting useful features from raw network traffic without requiring extensive manual preprocessing. This ability makes them suitable for identifying advanced cyberattacks in dynamic environments such as IoMT networks [4].

Among deep learning methods, Long Short-Term Memory networks have attracted considerable attention because of their ability to learn temporal dependencies in sequential data. Since network traffic is often sequential in nature, LSTM models can effectively identify anomalies that develop over time. Researchers have reported that LSTM-based intrusion detection systems achieve higher detection accuracy and lower false alarm rates compared to conventional machine learning approaches [5].

Other neural network models, such as Multi-Layer Perceptron, have also been applied to intrusion detection tasks. MLP models are capable of learning nonlinear relationships among traffic features and can classify malicious patterns with reliable accuracy. These models have demonstrated good performance in network security applications, especially when trained on structured datasets containing traffic statistics and flow-level features [6].

Although these methods have improved intrusion detection accuracy, many existing solutions are designed for general-purpose IoT systems rather than healthcare-specific IoMT environments. Medical networks require rapid threat detection, low latency, and high reliability to ensure uninterrupted patient care. Any delay in detecting malicious activity may affect critical medical services and compromise sensitive patient information. Therefore, recent research emphasizes the need for intelligent intrusion detection frameworks specifically tailored for IoMT infrastructures [7].

The literature indicates that deep learning-based approaches provide better adaptability and detection capability than traditional methods. However, there is still a need for a dedicated framework that combines accurate real-time intrusion detection with the security requirements of connected medical systems. The proposed HIDS-IoMT model aims to address this need by applying deep learning techniques to improve intrusion detection performance and strengthen the security of IoMT networks.

III RELATED WORK

The rapid growth of the Internet of Medical Things has led researchers to focus on developing effective intrusion detection methods to secure connected medical devices and healthcare networks. Early intrusion detection approaches mainly used traditional machine learning techniques such as Decision Trees, Support Vector Machines, and Random Forest to classify network traffic into normal and malicious categories. These methods improved detection accuracy compared to rule-based systems and were useful in identifying suspicious activities in network environments. However, they often depended on manually selected features and were less effective when dealing with complex and continuously changing attack patterns.

With the advancement of Deep Learning, more intelligent intrusion detection models were introduced to improve performance. Deep learning algorithms such as Long Short-Term Memory and Multi-Layer Perceptron are capable of learning hidden patterns from network traffic data automatically, reducing the need for manual feature engineering. These models have shown better performance in detecting complex intrusions and identifying anomalies in real time. Their ability to analyze large amounts of traffic data makes them suitable for securing healthcare networks where rapid and accurate detection is essential.

Although these intelligent detection methods have improved intrusion detection performance, many existing solutions are designed for general IoT systems rather than medical environments. IoMT networks require highly reliable and real-time security mechanisms because any delay in detecting an intrusion can affect patient care and the operation of medical devices. This has created the need for specialized intrusion detection systems that are capable of handling the unique communication patterns of healthcare devices while maintaining high detection accuracy. Based on these challenges, the proposed HIDS-IoMT framework aims to provide a more reliable and intelligent security solution tailored specifically for IoMT environments.

IV PROBLEM STATEMENT

The increasing use of the Internet of Medical Things has brought major improvements in healthcare by enabling connected medical devices to exchange data in real time. This has made patient monitoring and healthcare delivery faster and more efficient. However, as more medical devices become connected to networks, the risk of cyber threats also increases. Sensitive patient information transmitted through these devices can become vulnerable to unauthorized access, malicious attacks, and data manipulation, creating serious concerns for both patient privacy and system reliability.

Many of the security solutions currently used in healthcare networks are based on traditional intrusion detection techniques that depend on fixed rules or previously known attack signatures. While these methods can detect familiar threats, they are not effective against new or continuously changing attack patterns. In IoMT environments, where devices generate large amounts of dynamic network traffic, conventional systems may fail to identify suspicious behavior accurately. This can result in delayed threat detection, high false alarms, and possible disruption of critical medical services.

Because of these limitations, there is a strong need for a smarter intrusion detection mechanism that can continuously monitor network traffic and identify malicious behavior more effectively. Such a system should be capable of learning from network patterns, detecting anomalies in real time, and supporting secure communication among connected medical devices. Developing an intelligent intrusion detection framework for IoMT networks is essential to improve healthcare cybersecurity and ensure the safe operation of modern medical systems.

V PROPOSED SYSTEM

The proposed HIDS-IoMT system is developed to strengthen the security of the Internet of Medical Things by providing an intelligent mechanism for detecting network intrusions. As connected medical devices continuously exchange sensitive information, there is a growing need for a reliable system that can identify malicious activities before they affect healthcare operations. The proposed framework addresses this challenge by analyzing network traffic patterns and detecting abnormal behavior that may indicate cyber threats. This approach improves the protection of

connected healthcare devices and helps maintain secure communication within medical networks.

To achieve this, the system processes network traffic data collected from IoMT devices and applies Deep Learning techniques to classify traffic as either normal or suspicious. The collected data is first prepared through preprocessing steps such as cleaning, normalization, and feature selection. After that, deep learning models like Long Short-Term Memory and Multi-Layer Perceptron are trained to recognize patterns in the network traffic. These models are capable of learning complex behaviors and identifying anomalies with greater accuracy than traditional intrusion detection methods.

The proposed system is designed to support real-time monitoring so that threats can be detected quickly and handled without interrupting essential healthcare services. By reducing false alarms and improving detection accuracy, the framework enhances the overall security of IoMT environments. This intelligent detection mechanism helps healthcare organizations protect sensitive patient information, improve network reliability, and reduce the risks associated with cyberattacks on connected medical devices.

VI METHODOLOGY

The methodology of the proposed HIDS-IoMT framework is designed to create an intelligent intrusion detection mechanism capable of securing the Internet of Medical Things environment from cyber threats. The process begins with the collection of network traffic data generated by connected medical devices such as sensors, monitoring systems, and healthcare communication units. This traffic data contains valuable information related to packet flow, communication behavior, and connection patterns. Since the collected raw data may include incomplete values, redundant entries, and inconsistencies, preprocessing is carried out to clean and normalize the dataset. This step ensures that the data is structured and reliable for further analysis, which is essential for improving the effectiveness of the intrusion detection process.

After preprocessing, the next step involves extracting and selecting the most relevant features from the dataset. Features such as packet size, transmission rate, flow duration, and protocol-related information are identified because they play an important role in distinguishing between normal and malicious traffic behavior. Selecting the most useful features reduces unnecessary complexity and improves the learning performance of the system. The processed dataset is then divided into training and testing sets so that the model can learn traffic behavior patterns from one part of the data and validate its performance on the remaining part. This structured preparation helps the system learn the characteristics of network intrusions more effectively.

To detect intrusions, the framework applies Deep Learning models capable of identifying complex patterns in network traffic. In this system, models such as Long Short-Term Memory and Multi-Layer Perceptron are trained to classify traffic as normal or suspicious. These models are selected because they can learn hidden relationships in traffic data and detect anomalies with greater accuracy than traditional methods. During training, the models adjust their internal parameters iteratively to minimize prediction errors and improve classification performance. After training, the models are evaluated using measures such as accuracy, precision, recall, and F1-score to determine their effectiveness in detecting malicious traffic while minimizing false alarms.

Once the most effective model is identified, it is deployed for real-time intrusion detection within the IoMT network. Incoming traffic data is continuously monitored, and the trained model analyzes each traffic flow to determine whether it is normal or malicious. If suspicious

behavior is detected, the system immediately generates alerts so that appropriate security actions can be taken without delay. This real-time monitoring capability improves the ability of healthcare systems to respond quickly to threats and prevents disruptions in medical services. By combining data preprocessing, feature selection, deep learning-based classification, and continuous monitoring, the proposed methodology provides a reliable and scalable solution for enhancing the cybersecurity of connected medical devices.

VII IMPLEMENTATION

The implementation of the proposed HIDS-IoMT framework begins with collecting and preparing network traffic data from the Internet of Medical Things environment. Medical devices connected to the network generate large amounts of communication data, including packet information, traffic flow details, and connection records. This raw data is first processed to remove duplicate entries, correct missing values, and normalize the attributes so that the dataset becomes suitable for training the detection models. This preparation stage is important because the quality of the input data directly affects the performance of the intrusion detection system.

Once the dataset is prepared, the next step is to train the intrusion detection models using Deep Learning techniques. In the proposed framework, models such as Long Short-Term Memory and Multi-Layer Perceptron are used to analyze network traffic patterns and classify the traffic as normal or malicious. The prepared data is divided into training and testing sets, where the training set is used to teach the models how to recognize intrusion patterns, while the testing set is used to measure the accuracy of predictions. Through repeated training cycles, the models learn the differences between normal communication behavior and suspicious activities, improving their ability to detect intrusions accurately.

After training, the best-performing model is integrated into the system for real-time monitoring of network traffic. As data is received from connected medical devices, the model continuously evaluates the traffic and identifies whether the activity is safe or suspicious. If abnormal behavior is detected, the system immediately generates an alert so that appropriate action can be taken. This automated monitoring process reduces the need for manual inspection and allows threats to be identified at an early stage, which is critical in healthcare environments where uninterrupted service is essential.

To make the system practical for deployment, an alert and monitoring interface is included as part of the implementation. This interface displays the status of the network traffic, detected anomalies, and warning messages in an organized format so that administrators can easily observe the security state of the network. By combining data preparation, model training, real-time monitoring, and alert generation, the implementation of the HIDS-IoMT framework provides an efficient and intelligent solution for improving the cybersecurity of connected medical devices and healthcare communication networks.

VIII RESULTS ANALYSIS

The performance of the proposed HIDS-IoMT framework was evaluated to measure its effectiveness in detecting malicious activities in the Internet of Medical Things environment. After training the deep learning models with the prepared network traffic dataset, the system was tested using standard evaluation metrics such as accuracy, precision, recall, and F1-score. These metrics provide a detailed understanding of how well the model distinguishes between normal and malicious traffic. High accuracy indicates the overall correctness of the model, while precision and recall reflect the system's ability to correctly identify attacks without generating excessive false alarms. The results show that the proposed

framework performs efficiently in recognizing intrusion patterns and maintaining reliable detection performance.

To analyze the effectiveness of different models, the performance of the Multi-Layer Perceptron and Long Short-Term Memory models was compared. The MLP model achieved good classification accuracy by learning nonlinear relationships between network traffic features, while the LSTM model performed better in detecting sequential traffic anomalies due to its ability to capture temporal dependencies. The experimental evaluation showed that the LSTM model produced higher detection accuracy and lower false positives than the MLP model, making it more suitable for real-time intrusion detection in healthcare environments.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
MLP	94.2	93.5	92.8	93.1
LSTM	97.1	96.4	95.9	96.1

Table 1: Performance Comparison of Deep Learning Models

The results presented in Table 1 demonstrate that the LSTM-based intrusion detection model outperforms the MLP model across all evaluation metrics. The higher accuracy and F1-score indicate that LSTM is more effective in identifying malicious traffic while maintaining balanced performance between precision and recall. This improvement is mainly due to the ability of LSTM networks to learn temporal traffic behavior, which is important for detecting evolving intrusion patterns in IoMT networks. Based on these results, the proposed HIDS-IoMT framework proves to be an effective solution for enhancing the security of connected medical devices by providing accurate and reliable intrusion detection.

IX CONCLUSION

The increasing adoption of the Internet of Medical Things has improved the efficiency of healthcare services by enabling continuous communication among medical devices and healthcare systems. At the same time, this growing connectivity has created new security risks, making medical networks more vulnerable to cyber threats. Attacks on connected healthcare devices can lead to unauthorized access, compromise sensitive patient information, and interrupt critical medical services. These challenges highlight the need for effective intrusion detection mechanisms that can provide reliable protection in IoMT environments.

The proposed HIDS-IoMT framework was developed to improve the security of IoMT networks through the use of Deep Learning techniques. By analyzing network traffic patterns and identifying abnormal behavior, the system is capable of detecting malicious activities with improved accuracy. The use of models such as Long Short-Term Memory and Multi-Layer Perceptron enhances the system's ability to identify intrusion patterns while reducing false alarms. The performance evaluation demonstrates that the proposed approach can effectively support real-time intrusion detection in connected medical environments.

Overall, the proposed framework provides a practical and scalable solution for strengthening cybersecurity in healthcare networks. Its ability to monitor traffic continuously and detect threats efficiently helps improve the reliability and safety of connected medical systems. This work shows that intelligent intrusion detection methods can play an important role in protecting sensitive healthcare infrastructures. Future improvements may focus on enhancing detection performance further and

adapting the system to handle emerging cyber threats in real-world IoMT deployments.

REFERENCES

[1] S. M. Riazul Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[2] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of Medical Things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.

[3] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. 9th EAI Int. Conf. Bio-inspired Information and Communications Technologies (BICT)*, New York, NY, USA, 2016, pp. 21–26.

[4] Y. Yin, J. Liu, Y. Yang, and J. Zhou, "An intrusion detection model based on deep learning," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[5] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[6] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *Proc. Int. Conf. Information Networking (ICOIN)*, Da Nang, Vietnam, 2017, pp. 712–717.

[7] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," *Future Internet*, vol. 12, no. 3, pp. 1–26, 2020.

[8] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Personal Communications*, vol. 111, no. 4, pp. 2287–2310, Apr. 2020.

[9] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2010, pp. 305–316.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, Feb. 2020.