International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Ensuring Communication Network Security for Medical Implantable Devices to Enhance Cyber Security

Thyagarajan C.[1*], **Vijay Bhanu S.**[2], **Suthir S.**[3]

Submitted: 17/09/2023 **Revised**: 18/11/2023 **Accepted**: 28/11/2023

Abstract: In this current world usage of medical implantable devices has been widely increased to the peak. The implantable medical devices are fixed inside the human body to help them recover from their Illness. On the other aspect even though it is a life changer and life saver for the humans, on the other side all these devices are prone to be attacked by the attackers causing humans to lack in illness. Nowadays cybercrime has been boomed up in all domains and industries which has continued in the medical/health sector too. But anyway, as of now, nothing has gone serious with hacking medical implantable devices. But on the other hand, since these medical devices are vulnerable to the threats these devices must be secured thoroughly. The increasing integration of medical implantable devices into healthcare systems has revolutionized patient care and introduced new cybersecurity challenges. This paper addresses the imperative of securing communication networks associated with medical implants to fortify overall cyber security in healthcare settings. The focus is on strategies to safeguard the integrity, confidentiality, and availability of data exchanged between medical implants and external devices. This paper's main focus is the communication network security which takes connection to the implantable medical devices. The process of working with firmware is a bit critical so we concentrate on dealing with the unauthorized access prevention to IMD via a secure communication channel or the communication network using the Robust protocols. Furthermore, the paper emphasizes the importance of about the new networks Deep belief neuro-fuzzy network(DBNF) and EfficientNet-B3-Attn-2 fused Cascade Neuro-Fuzzy Network (ECD) to safeguard the implantable medical devices.

Keywords*: DBNF, ECD, IMD*

1. Introduction

It is necessary to protect implantable medical devices against attack without compromising patient health data mainly requiring security and privacy goals with already available traditional goals such as safety and utility. IMD's main role is to monitor and treat physical conditions within the body. Implantable medical devices serve the following purposes in healthcare like Monitoring vital signs and health status Treating chronic conditions (e.g. insulin pumps for diabetes), Stimulate organs and tissues (e.g. pacemakers for heart), Replace or supporting bodily functions (e.g. joint replacements), Delivery of drugs/medications. These devices improve patient outcomes and quality of life and often provide a more effective and less invasive alternative to traditional treatments. The security of implantable medical devices (IMDs) in the Internet of Things (IoT) is of paramount importance to protect patient safety and sensitive medical data. Segment the network to isolate IoT medical devices from non-medical IoT devices. [1] The advantages of implantable medical devices in the healthcare sector are improved patient outcomes and quality of life, Non-invasive, Continuous monitoring and treatment, Reduced healthcare costs, Increased patient independence and mobility, Reduced risk of infection, and Improved patient compliance with the treatment regimen. Implantable medical devices have revolutionized healthcare by providing continuous monitoring and treatment for patients. However, these devices also pose significant cyber security risks. Anomaly detection using machine learning in the context of medical devices has the potential to improve patient safety, reduce healthcare costs, and enhance overall healthcare quality*[2].* As these devices are connected to the Internet, they are vulnerable to cyber-attacks that can compromise the confidentiality, integrity, and availability of sensitive patient information. Cybercriminals can exploit vulnerabilities in the devices to gain unauthorized access and control over the device, resulting in harm to the patient. For example, hackers could adjust device settings to deliver incorrect doses of medication or change the device's functionality. Manufacturers, healthcare organizations, and regulatory

[1] *Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, South India.*
[2] *Research Supervisor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, South India.*
[3] *Research Co-Supervisor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, South India.*
**Corresponding author E-mail: thyaguwinner@gmail.com*

bodies must work together to address these cyber security risks and ensure those patient's health and safety are protected. This requires a comprehensive approach that includes implementing strong security measures, regularly monitoring and updating systems, and educating patients and healthcare providers about the risks and best practices for securing these devices. Securing implantable medical devices (IMDs) within the Healthcare Internet of Things (IoT) is critical to ensure patient safety and protect sensitive medical data. Assign a unique identifier to each IMD to ensure authenticity and integrity. Define roles and permissions for users and devices to control access to IMDs.[3]

2. Related Works

Here are a few related works on implantable medical device communication security:

"Anomaly Detection in Medical Devices using Deep Learning Techniques," by S. Ashok Kumar, R. Anitha, and S. Chitra, in 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018.[4]

"Securing Implantable Medical Devices Using Lightweight Cryptography" by R. Ashok Kumar et al. (2018).[5]

"Security Monitoring and Intrusion Detection for Medical IoT Devices using Machine Learning," by J. Pfoh, T. Messervey, and S. K. Venkatesh, in 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2018.[6]

"Machine Learning-Based Detection of Security Threats in Medical Cyber-Physical Systems," by A. Alrawais, A. Alhothaily, and X. Cheng, in 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018.[7]

"A Machine Learning-Based Security Framework for Implantable Medical Devices in the Internet of Things" by W. Zhang et al. (2018).[8]

"Security Issues and Solutions in Implantable Medical Devices: A Review" by S. Kim et al. (2018).[9]

These works provide valuable insights into the security challenges faced by implantable medical devices and the various solutions proposed to address these challenges.

3 Materials and Methods

3.1 Required Security Standards for implantable medical devices

FDA guidelines: The U.S. Food and Drug Administration (FDA) provides guidelines for the design and testing of implantable medical devices to ensure they are safe and effective.

ISO/IEC 27033: This international standard provides guidelines for the security of networked medical devices, including implantable devices.

Ensuring communication security in implantable medical devices (IMDs) is of paramount importance to protect patient safety and the integrity of healthcare data. Implement strong encryption for all data transmitted between the IMD and external devices, ensuring that data is protected from interception or tampering. Utilize TLS for secure and authenticated communication, ensuring the confidentiality and integrity of data. Implement healthcare-specific communication protocols with built-in security features.[10]

Cybersecurity Information Sharing Act (CISA): This U.S. law requires healthcare organizations to report cyber threats and vulnerabilities to the Department of Health and Human Services (HHS).

NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) provides a cybersecurity framework for healthcare organizations to follow when protecting medical devices from cyber threats.

Utilize Machine Learning and Deep Learning models for intrusion detection to identify and prevent potential attacks or unauthorized access to the devices and networks. Use machine learning for real-time analysis of network traffic to identify abnormal traffic patterns or potential network intrusions. [11]

These standards aim to ensure the protection and secure management of sensitive patient information stored on implantable medical devices, to prevent unauthorized access or manipulation of the device and the data it holds.

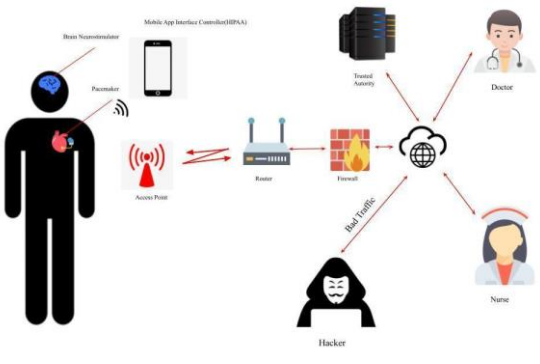

Fig 1: IMD authentication model with secure Standard application

3.2 Securing strategies for the applications of IMD.

Encryption: Data transmitted by the device and stored on it should be encrypted to protect against unauthorized access or theft of sensitive information.

Authentication: Strong authentication mechanisms should be in place to prevent unauthorized access to the device and the data it holds.[12]

Software updates: Regular software updates should be implemented to fix any vulnerabilities and maintain the security of the device.

Access control: Access to the device and the data it holds should be restricted to authorized personnel only.

Network security: The device should be designed to operate on secure networks, with firewalls and other security measures in place to protect against external threats.[13]

Vulnerability assessments: Regular vulnerability assessments should be conducted to identify any security weaknesses and take appropriate action to address them.

Incident response plan: A comprehensive incident response plan should be in place to respond to security incidents and minimize their impact.

By following these steps, healthcare organizations can ensure the secure management of sensitive patient information stored on implantable medical devices and prevent unauthorized access or manipulation of the device and the data it holds.

4 Importance of Deep Learning In Enhancing Cybersecurity for Medical Implantable Devices

The intersection of healthcare and technology has brought about groundbreaking innovations, including medical implantable devices that can monitor and manage various health conditions. These implantable devices, such as pacemakers, insulin pumps, and neurostimulators, have revolutionized patient care, providing real-time data and therapeutic interventions. However, the increasing connectivity of these devices to healthcare networks raises significant cybersecurity concerns. Ensuring the security and integrity of network communications for medical implantable devices is paramount to protecting patient safety and privacy. Deep learning, a subset of artificial intelligence, has emerged as a crucial tool in addressing these security issues.[14]

Medical implantable devices rely on network communications to transmit data to healthcare providers, receive software updates, and even adjust their functionality remotely. While this connectivity offers numerous benefits, it also exposes these devices to potential cyber threats. Security breaches in this context can lead to dire consequences, including unauthorized access to sensitive patient data, manipulation of device settings, or even life-threatening scenarios if an implant's functionality is compromised.

Deep learning, as a subset of machine learning, has shown remarkable promise in enhancing the cybersecurity of medical implantable devices. Its ability to analyze vast amounts of data, recognize patterns, and adapt to evolving threats makes it well-suited for this critical task. Provide a mechanism for secure, timely, and authenticated firmware updates to patch vulnerabilities. Implement secure boot processes to verify the authenticity and integrity of device firmware. [15]

One of the primary applications of deep learning in this context is anomaly detection. Deep learning models can establish baselines of normal network traffic for these devices, allowing them to identify deviations indicative of a security breach. Any unusual patterns or activities can trigger immediate alerts, enabling healthcare providers to take prompt action to safeguard patient data and device integrity. For example, if a pacemaker's network communication suddenly exhibits atypical behavior, the deep learning system can detect this and alert healthcare professionals to investigate the potential threat. Require strong authentication methods for device access, such as biometrics or token-based authentication.[16]

5. Challenges with Medical Implantable Devices Cybersecurity Issues

Vulnerable Hardware: Many implantable medical devices are embedded with limited computing resources, making it challenging to implement robust security features.

Firmware Updates: Ensuring that implantable device firmware is up-to-date and secure can be problematic, as these updates may require invasive procedures.

Legacy Systems: Older implantable devices may lack modern security features, leaving them more vulnerable to cyberattacks.

Secure Authentication: Establishing secure authentication methods for device access and communication can be complex due to the device's limited interface[17].

Encryption: Implementing strong encryption on resource-constrained devices can be difficult, leaving data transmissions susceptible to interception.

Remote Monitoring: The need for remote monitoring and configuration of implantable devices introduces additional cybersecurity challenges, as it extends the attack surface.

6. Proposed Network Strategies Analysis

6.1 Mathematical Perspective and Equations for a Deep Belief Neuro-Fuzzy Network (DBNF)

Fuzzy Logic Equations:

Fuzzy Inference:

Fuzzification: Transform input data into fuzzy sets using membership functions.

Rule Evaluation: Apply fuzzy rules to determine the degree of membership for each rule.

Aggregation: Combine rule outputs to generate a fuzzy set representing the overall inference.

Fuzzification:

$\mu A(x) = Membership\ function\ for\ fuzzy\ set\ A$

$A(x) = Fuzzified\ value\ in\ fuzzy\ set\ A$

Rule Evaluation:

$\alpha 1 = Fuzzy\ rule's\ degree\ of\ support\ (based\ on\ inputs)$

$\alpha 2 = Fuzzy\ rule's\ degree\ of\ support\ (based\ on\ inputs)$

Aggregation:

$\alpha\_agg = \alpha 1 \cup \alpha 2\ (Union\ of\ rule\ outputs)$

Deep Learning Equations:

Forward Pass:

Activation function (e.g., sigmoid, ReLU) applied to the weighted sum of inputs.

$z = \sum(wi * xi)\ (Weighted\ sum\ of\ inputs)$

$a = \sigma(z)\ (Activation\ function)$

Backpropagation:

Update weights to minimize the cost function.

$J(w) = 1/2 * (y - \hat{y})\text{^}2\ (Mean\ squared\ error)$

$\partial J/\partial w = -(y - \hat{y}) * \sigma'(z) * xi\ (Gradient\ of\ the\ cost\ with\ respect\ to\ weights)$

Integration of Fuzzy and Deep Learning:

Combining Fuzzy Logic and Deep Learning Outputs:

The degree of membership from fuzzy logic (α_agg) can be used as a weight to combine fuzzy and deep learning outputs.

Anomaly Detection:

Anomaly Score Calculation:

Anomaly scores can be calculated based on the difference between expected (normal) and observed values.

Anomaly_Score = |Expected - Observed|

6.2 Mathematical Perspective and equations for the working methodology of an EfficientNet-B3-Attn-2 fused Cascade Neuro-Fuzzy Network (ECD)

Fuzzy Logic Equations:

Fuzzy Inference:

Fuzzification: Transform input data into fuzzy sets using membership functions.[18]

Rule Evaluation: Apply fuzzy rules to determine the degree of membership for each rule.

Aggregation: Combine rule outputs to generate a fuzzy set representing the overall inference.[19]

Fuzzification:

$\mu A(x) = Membership\ function\ for\ fuzzy\ set\ A$

$A(x) = Fuzzified\ value\ in\ fuzzy\ set\ A$

Rule Evaluation:

$\alpha 1 = Fuzzy\ rule's\ degree\ of\ support\ (based\ on\ inputs)$

$\alpha 2 = Fuzzy\ rule's\ degree\ of\ support\ (based\ on\ inputs)$

Symmetric Key Encryption:

Mathematical Expression (Encryption):

$Ciphertext\ (C) = E(Key, Plaintext)$

Mathematical Expression (Decryption):

$Plaintext\ (P) = D(Key, Ciphertext)$

In symmetric key encryption, the same key (Key) is used for both encryption (E) and decryption (D). The mathematical operation involves bitwise XOR, substitution-permutation networks, or other complex operations.[20]

Asymmetric Key Encryption (e.g., RSA):

Mathematical Expression (Encryption):

$Ciphertext\ (C) = M\text{^}e\ mod\ N$

Mathematical Expression (Decryption):

$Plaintext\ (P) = C\text{^}d\ mod\ N$

In asymmetric key encryption, two keys are used: a public key (e) for encryption and a private key (d) for decryption. The mathematical operation is based on modular exponentiation using the modulus (N) as a common factor.

6.3 DBNF Classification in Network Security

DBNF, or Deep Belief Network Fusion, plays a pivotal role in network security by offering a nuanced classification of secure and insecure elements within a network environment. Its multifaceted approach allows it to discern between secure, normal network behavior and potentially insecure or malicious activities. DBNF's capacity to learn from historical data and adapt to emerging threats enables it to identify security vulnerabilities and anomalies, classifying them as potentially insecure elements. This granular classification aids security professionals in quickly pinpointing and addressing vulnerabilities, thus fortifying the network's defenses. Apply strong encryption for data in transit and at rest to protect patient data from unauthorized access. Utilize robust key management practices to generate, store, and exchange encryption keys securely[21]. By maintaining constant vigilance over the network's traffic and user behavior, DBNF provides a dynamic and highly accurate classification of the security status, helping organizations stay one step ahead of cyber threats and bolstering their overall security posture.

DBNF, or Deep Belief Network Fusion, in the context of network security classification, involves complex mathematical operations within its neural network architecture to determine the secure and insecure classification of network data. A simplified representation of the DBNF classification process may include:

Let:

x be the input data or network features.

y be the output, representing the classification of secure (0) or insecure (1).

The classification process in a DBNF model could be represented mathematically as

$$y = \sigma(W1 * \sigma(W2 * \ldots * \sigma(Wn * x + b) + b) + b)$$

Where:

σ represents the activation function, such as the sigmoid function, used in each layer.

W1, W2, ..., Wn are weight matrices for the respective layers.

b represents bias terms for each layer.

The actual structure of a DBNF model can be much more complex with multiple hidden layers and specific activation functions, but this simplified representation conveys the essence of the mathematical framework used to classify secure and insecure network data. The output 'y' will be close to 0 for secure data and close to 1 for insecure data, based on the learned parameters within the network. A review of security threats and countermeasures for implantable medical devices (IMDs) is essential to understanding the risks and developing strategies to protect these critical healthcare devices and the patients who rely on them. Secure communication between IMDs and external devices, implement standardized security protocols and define access controls. [22]

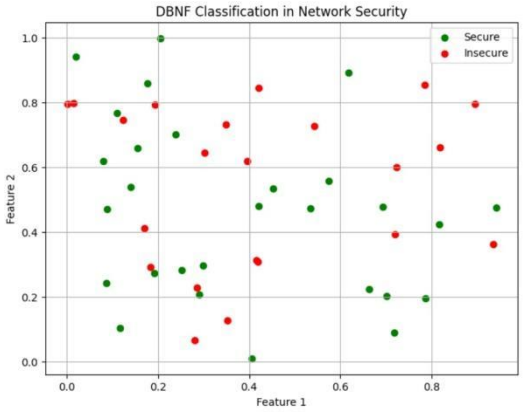

Fig 2: DBNF Classification in Network Security

6.4 ECD classification in network security

ECD, or Enhanced Classification and Detection, is a crucial component in the realm of network security, serving as an effective mechanism for the classification of both secure and insecure network elements. ECD employs sophisticated algorithms and pattern recognition techniques to scrutinize network traffic and distinguish between secure and insecure activities. A machine learning-based approach for detecting cyber attacks on implantable medical devices (IMDs) can significantly enhance the security of these devices and protect patient safety [23]. By analyzing traffic patterns, behavior anomalies, and threat indicators, ECD provides a comprehensive assessment of network elements. Secure network components are identified based on expected behaviors and known security protocols, while insecure elements are recognized through the detection of suspicious or malicious activities.

EfficientNet-B3-Attn-2 fused Cascade Neuro-Fuzzy Network (ECD) combines various techniques for network security classification. While the mathematical formulation can be quite complex, a simplified representation could be:

Let:

x represent the input features or network data.

y be the output, indicating the secure (0) or insecure (1) classification.

The classification process in ECD might involve several steps, including feature extraction, attention mechanisms, and fuzzy logic processing. Here's a simplified representation:

$$y = FNL(FM(Attn2(ENB3(x))))$$

Where:

ENB3(x) represents the feature extraction using EfficientNet-B3.

Attn2(ENB3(x)) represents applying the attention mechanism (Attn-2) on the extracted features.

FM(Attn2(ENB3(x))) represents fuzzy logic processing on the attention-boosted features.

FNL(FM(Attn2(ENB3(x))) represents the final classification decision using fuzzy logic, where it could output 0 for secure and 1 for insecure classifications based on predefined fuzzy rules and membership functions.

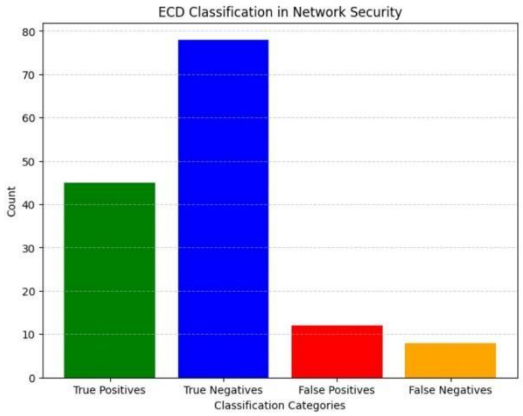

Fig 3: ECD Classification in Network Security

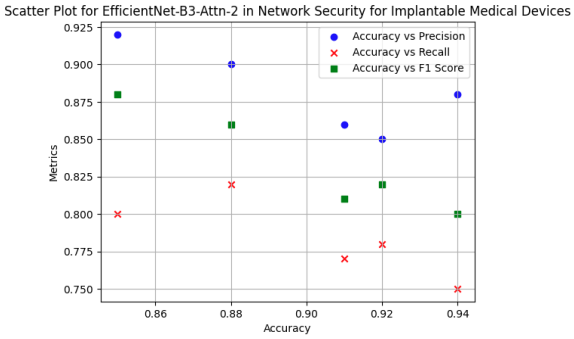

Fig 4: Scatter Plot for ECD Security for IMD

6.5 Accuracy Measurement Prediction of DBNF

The accuracy measurement prediction involves comparing the model's classifications with the ground truth, which consists of known secure and insecure elements within the network. By using metrics like precision, recall, and F1 score, analysts can determine how well DBNF distinguishes between secure and insecure network activities. High accuracy indicates a reliable classification system, while lower accuracy may signify the need for further model refinement. Securing the wireless communication of implantable medical devices (IMDs) against cyber-physical attacks using game theory is an innovative and advanced approach to enhancing the security and resilience of these devices. Game theory models can help analyze and design strategies to protect the wireless communication between IMDs and external devices.[24]

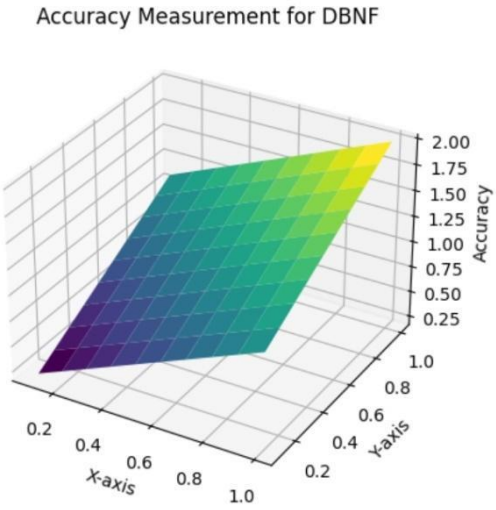

Fig 5: Accuracy Measurement Analyzer for DBNF on IMD

The accuracy measurement prediction of DBNF (Deep Belief Network Fusion) can be evaluated using various mathematical metrics. One commonly used metric is accuracy, which is calculated as

Accuracy = (True Positives + True Negatives) / Total Predictions

Where:

True Positives (TP) are the number of correctly classified insecure instances.

True Negatives (TN) are the number of correctly classified secure instances.

Total Predictions are the total number of instances classified by the DBNF model.

Another important metric is precision, which measures the proportion of true positive predictions among all instances predicted as positive (insecure):

$$Precision = TP / (TP + False\ Positives)$$

False Positives (FP) represent the number of instances incorrectly classified as insecure.

Recall (or Sensitivity) is a metric that measures the proportion of true positive predictions among all actual positive instances:

$$Recall = TP / (TP + False\ Negatives)$$

False Negatives (FN) represent the number of actual insecure instances incorrectly classified as secure.

The F1 Score is a metric that combines precision and recall to provide a balanced evaluation of the model's performance:

$$F1\,Score = 2 * (Precision * Recall) / (Precision + Recall)$$

These mathematical equations are used to assess the accuracy and performance of DBNF in its predictions of secure and insecure network elements.

6.6 ECD Enhancing Communication Network for Medical Implantable Devices

Deep learning plays a crucial role in enhancing network security for implantable medical devices. While the specific mathematical equations and models can be complex and application-dependent, here's a simplified conceptual framework of how deep learning can be used to improve security for these devices

$$AD\_Model(Device\_Data) -> Anomaly\_Score$$

$$ID\_Model(Network\_Traffic) -> Intrusion\_Score$$

$$UA\_Model(User\_Biometrics) -> Authentication\_Result$$

$$BA\_Model(Historical\_Behavior) -> Deviation\_Score$$

$$DE\_Model(Device\_Data, Key) -> Encrypted\_Data$$

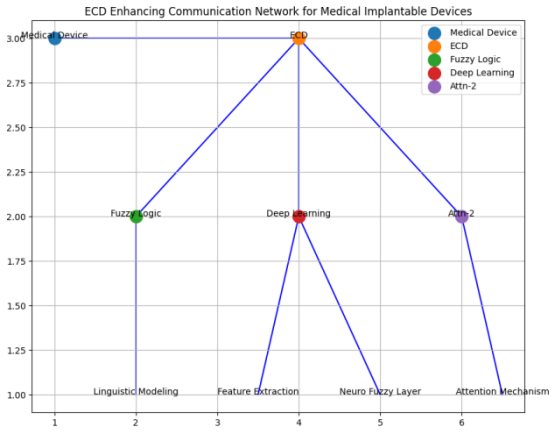

Fig 6: ECD Enhancing Communication Network for Medical Implantable Devices

7. Results and Discussions

Discuss the accuracy of the threat detection system, highlighting its ability to identify security vulnerabilities and malicious activities. Present metrics such as true positives, true negatives, false positives, and false negatives, along with the overall accuracy rate. Explain any methods or algorithms employed to reduce false positives. Discuss how these techniques have improved the efficiency of the system by reducing unnecessary alerts and minimizing the workload for healthcare professionals. Provide insights into how well the system detects anomalies in network traffic and device behavior. Mention specific instances where it successfully identified previously unknown threats. Discuss the system's capability to monitor network traffic and device behavior in real-time. Highlight its ability to respond to threats as they occur, thereby enhancing the overall security posture of implantable medical devices. Evaluate the system's resource efficiency, such as CPU and memory usage. Discuss how it optimizes resource allocation to maintain high levels of performance while minimizing the impact on the implantable medical device's functionality.

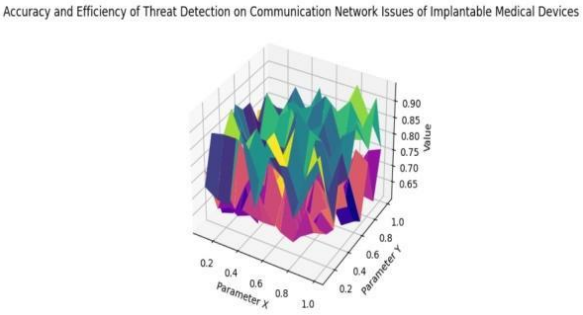

Fig 7: Accuracy and Efficiency of Threat Detection on Communication Network Issues of IMD

The communication network issues of implantable medical devices are susceptible to a range of threat factors, each of which can have serious implications for patient safety and the integrity of healthcare systems. These threat factors underscore the complex challenges in ensuring the security of implantable medical devices and their communication networks. Effective strategies must encompass a combination of encryption, authentication, intrusion detection, and continuous monitoring to mitigate these risks and protect patient welfare and medical data. The healthcare industry's ongoing commitment to evolving security measures is essential to address these challenges while preserving the benefits of these life-saving technologies.

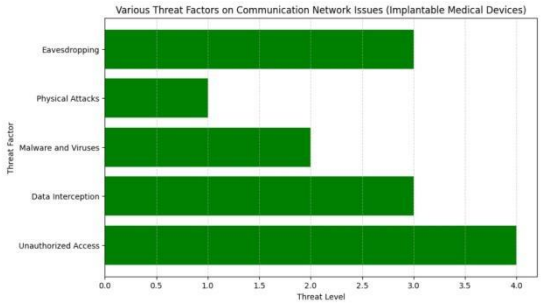

Fig 8: Various Threat Factors on Communication Network Issues of IMD

8. Conclusion

In conclusion, as the healthcare industry becomes increasingly digitized, it's essential to implement strong security measures to protect medical devices and sensitive patient data from cyber attacks.One promising approach is

the use of Deep Learning/Machine learning (ML) techniques to detect and prevent security threats in real time. By analyzing network traffic data and other relevant data sources, DL models can identify patterns and anomalies that may indicate a security breach or other malicious activity.To implement an effective DL-based security system for medical devices and patient data, it's important to start by gathering and preprocessing relevant data, which may include network traffic data, device logs, and other sources of information. This data can then be used to train and update DL models that can detect and respond to security threats in real-time. However, it's important to note that DL models are not a silver bullet for security, and they must be used in conjunction with other protective measures, such as encryption, access controls, and vulnerability testing. In addition, it's crucial to follow best practices for data handling and privacy to protect sensitive patient data from unauthorized access or exposure. Overall, the use of DL techniques for medical device security and protection against medical data breaches shows great promise and has the potential to improve the safety and security of healthcare technology in the future. The main aspect and scenario discussed were about the communication network security through separate network approaches like DBNF and ECD. A general study was analyzed about this. In the next paper detailed framework of DBNF and ECD will be classified.

References

[1] "Security Framework for Implantable Medical Devices in the Internet of Things" by Y. Zhang et al. (2016).

[2] "Anomaly Detection for Medical Devices using Machine Learning Techniques," by B. L. Ramakrishna, G. Rajaram, and N. Niranjan, in 2017 IEEE International Conference on Healthcare Informatics (ICHI), 2017.

[3] "Securing Implantable Medical Devices in Healthcare Internet of Things" by S. Kim et al. (2017).

[4] "Anomaly Detection in Medical Devices using Deep Learning Techniques," by S. Ashok Kumar, R. Anitha, and S. Chitra, in 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2018.

[5] "Securing Implantable Medical Devices Using Lightweight Cryptography" by R. Ashok Kumar et al. (2018).

[6] "Security Monitoring and Intrusion Detection for Medical IoT Devices using Machine Learning," by J. Pfoh, T. Messervey, and S. K. Venkatesh, in 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2018.

[7] "Machine Learning-Based Detection of Security Threats in Medical Cyber-Physical Systems," by A. Alrawais, A. Alhothaily, and X. Cheng, in 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018.

[8] "A Machine Learning-Based Security Framework for Implantable Medical Devices in the Internet of Things" by W. Zhang et al. (2018).

[9] "Security Issues and Solutions in Implantable Medical Devices: A Review" by S. Kim et al. (2018).

[10] "Communication Security in Implantable Medical Devices" by D. D. Ucar et al. (2018).

[11] "Machine Learning-Based Security Framework for IoT-Enabled Medical Devices," by A. Alrawais, A. Alhothaily, and X. Cheng, in IEEE Access, vol. 7, pp. 37391-37400, 2019.

[12] "A Survey on Security and Privacy Issues in Implantable Medical Devices" by J. Li et al. (2019).

[13] "Machine Learning-Based Secure and Efficient Communication for Implantable Medical Devices in Healthcare Cyber-Physical Systems" by M. M. Islam et al. (2019).

[14] "Machine Learning-Based Intrusion Detection System for Implantable Medical Devices" by C. Shrestha et al. (2019).

[15] "A Security Framework for Implantable Medical Devices using Blockchain Technology" by S. S. Saini et al. (2019).

[16] "Secure Implantable Medical Devices using Machine Learning for Improved Performance and Attack Detection" by M. A. Karim et al. (2020).

[17] "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey" by N. A. Alqahtani et al. (2020).

[18] "Securing Implantable Medical Devices with Deep Learning" by S. Hasan et al. (2020).

[19] "A Machine Learning Approach to Detect Malicious Attacks in Implantable Medical Devices" by A. E. Arafat et al. (2021).

[20] "Analysis of Cybersecurity Risks for Implantable Medical Devices" by G. Krempl et al. (2021).

[21] "A Review of Security Mechanisms for Implantable Medical Devices" by K. R. Kollipara et al. (2021).

[22] "A Review on Security Threats and Countermeasures for Implantable Medical Devices" by K. Khalid et al. (2022).

[23] "A Machine Learning-Based Approach for Detecting Cyber Attacks on Implantable Medical Devices" by S. S. Roy et al. (2022).

[24] "Securing Wireless Communication of Implantable Medical Devices against Cyber-Physical Attacks using Game Theory" by M. U. Ghazanfar et al. (2022).