# On the Performance of Cyber-Biomedical Features for Intrusion Detection in Healthcare 5.0

**Pedro H. Lui[1], Lucas P. Siqueira[1], Juliano F. Kazienko[1], Vagner E. Quincozes[2], Silvio E. Quincozes[3], and Daniel Welfer[1]**

[1]Universidade Federal de Santa Maria (UFSM), Santa Maria – RS, Brasil

[2]Universidade Federal Fluminense (UFF), Niterói – RJ, Brasil

[3]Universidade Federal do Pampa (UNIPAMPA), Alegrete – RS, Brasil

{pedro.lui, kazienko}@redes.ufsm.br, lucas.pittella@acad.ufsm.br

vequincozes@id.uff.br, silvioquincozes@unipampa.edu.br

daniel.welfer@ufsm.br

***Abstract.*** *Healthcare 5.0 integrates Artificial Intelligence (AI), the Internet of Things (IoT), real-time monitoring, and human-centered design toward personalized medicine and predictive diagnostics. However, the increasing reliance on interconnected medical technologies exposes them to cyber threats. Meanwhile, current AI-driven cybersecurity models often neglect biomedical data, limiting their effectiveness and interpretability. This study addresses this gap by applying eXplainable AI (XAI) to a Healthcare 5.0 dataset that integrates network traffic and biomedical sensor data. Classification outputs indicate that XGBoost achieved 99% F1-score for benign and data alteration, and 81% for spoofing. Explainability findings reveal that network data play a dominant role in intrusion detection whereas biomedical features contributed to spoofing detection, with temperature reaching a Shapley values magnitude of 0.37.*

## 1. Introduction

The advent of Healthcare 5.0 marks a transformation in medical innovation. Building on Healthcare 4.0's technological integration, it shifts the focus to patient-centered treatment and care, integrating Artificial Intelligence (AI), the Internet of Things (IoT), and human-centered design to enhance personalized medicine, predictive diagnostics, and real-time monitoring. These technologies are also reshaping cybersecurity in healthcare, offering new information (features) and generating opportunities to enhance data-driven security mechanisms [Gadekallu et al. 2024].

The exponential growth of the Digital Health market, projected to reach $258.25 billion by 2029 [Statista 2025], underscores the critical need to prioritize cybersecurity in the Internet of Medical Things (IoMT). As connected biosensors, telemedicine platforms, and digital treatment tools become integral to healthcare delivery, their reliance on sensitive patient data and connectivity exposes vulnerabilities to cyberattacks. A single breach could compromise patient safety, disrupt critical care, and erode trust in rapidly expanding markets. As healthcare becomes increasing reliant on digital solutions, accelerated by post-pandemic adoption, proactive research into IoMT cybersecurity is essential to safeguard data integrity, ensure regulatory compliance, and sustain the sector's growth. Addressing these risks now will protect both technological innovation and human lives.

In cybersecurity, AI is instrumental in detecting threats through network traffic analysis, with Intrusion Detection Systems (IDS) based on Machine Learning (ML) algorithms to identify malicious patterns and strengthen network defenses. However, a significant limitation arises in the era of Healthcare 5.0: many AI-driven cybersecurity solutions are tailored for non-healthcare domains [Hady et al. 2020], and rely on datasets lacking critical biomedical data from wearable devices and medical sensors. This absence restricts their usefulness in healthcare, diminishes transparency, and complicates incident response efforts. To overcome this limitation, recent initiatives have focused on creating integrated datasets that combine network traffic with biomedical sensor data (*i.e., Cyber-Biomedical features*), alongside the development of Explainable AI (XAI) frameworks to improve interpretability and decision-making [Ali et al. 2023][Alani et al. 2023b][Aljuhani et al. 2024][Sohail et al. 2024]. However, such initiatives emphasize network traffic features while overlooking the role of XAI in assessing biomedical data contributions to intrusion detection. This gap limits IDS effectiveness in detecting adversarial manipulations of biometric signals—such as falsified heart rate or oxygen levels—potentially compromising patient safety.

In this work, we evaluate the predictive contributions of biomedical and network features in IDSs for IoT-driven Healthcare 5.0 environments. For analysis, SHAP (SHapley Additive exPlanations)[1] was used as a XAI tool to analyze feature prediction relevance from the WUSTL-EHMS-2020 dataset [Hady et al. 2020], which joins network and biomedical features. Our results indicate that network data plays a primary role in intrusion detection, while biomedical data are highly relevant for the detection of cyber-physical attacks that manipulate biometric signals. These findings expose a major shortcoming in current medical cybersecurity research: the failure to integrate biomedical data into IDS models, despite the growing interconnectivity of Cyber-Physical Systems (CPS) in the healthcare domain. By providing a transparent assessment of feature importance, this study reinforces the need to merge real-time network analytics with biomedical insights, strengthening Healthcare 5.0 cybersecurity to patient safety and data integrity.

The paper is structured as follows: Section 2 introduces key concepts, while Section 3 reviews related work in Healthcare 5.0 and identifies research gaps. Section 4 details the methodology, covering experimental setups, AI models, and evaluation metrics. Section 5 presents the results, including SHAP-based feature analysis and interpretations. Finally, Section 6 concludes the study and discusses future research directions.

## 2. Background

This section introduces key concepts and technologies, including Healthcare 5.0, the role of machine learning and XAI in decision-making and transparency, and the importance of IDS for healthcare cybersecurity.

### 2.1. Healthcare 5.0

Healthcare 5.0 represents the next stage in healthcare evolution, characterized by personalized, proactive, and patient-centered treatment enabled by advanced technologies such as smart wearables, ML, and the IoMT. Devices like biosensors and fitness trackers enhance clinical decision-making and patient self-management by enabling real-time data analysis, remote care, and continuous health monitoring. By integrating

[1]SHAP Tool. Available at: `https://shap.readthedocs.io/en/latest/`

ML and IoMT, Healthcare 5.0 advances predictive analytics, early disease detection, and tailored treatments, significantly improving healthcare efficiency and patient outcomes [Tandel et al. 2024].

However, as connected medical devices become increasingly prevalent, cybersecurity emerges as a critical concern. The interconnectivity of smart healthcare systems exposes patient data and medical infrastructure to cyber threats, necessitating robust security mechanisms. AI-driven cybersecurity solutions play a pivotal role in mitigating these risks by detecting anomalies, identifying potential intrusions, and ensuring the reliability of connected healthcare devices [Khan et al. 2024]. Ensuring the security and integrity of medical data is essential for realizing the full potential of Healthcare 5.0, reinforcing the need for solutions that balance innovation with privacy and system resilience.

### 2.2. Machine Learning and Explainable AI

ML plays a fundamental role in AI, enabling automation across a wide range of tasks. However, most ML models operate as black boxes, making their decision-making processes opaque and difficult to interpret [Ali et al. 2023]. This lack of transparency has led to the rise of XAI, which seeks to enhance model interpretability while maintaining high accuracy. In healthcare, where decision-making must be transparent and justifiable [Dave et al. 2020], this challenge is particularly critical. The inability to explain AI-driven predictions reduces clinical trust, as the risks associated with unverified or uninterpretable AI recommendations may outweigh benefits in accuracy, speed, and efficiency. Thus, XAI plays a crucial role in increasing trust, improving accountability, and ensuring the safe integration of AI in medical applications.

### 2.3. Intrusion Detection Systems

IDSs play a crucial role in cybersecurity by continuously monitoring network activity and identifying anomalous behavior [Javeed et al. 2024]. AI-driven IDSs have gained prominence due to their ability to rapidly analyze vast amounts of data, uncovering complex attack patterns that traditional security methods might miss. These systems are particularly valuable in high-stakes environments such as the IoMT and critical infrastructure, where security breaches can have severe operational and safety implications. In healthcare, IDSs are essential for detecting cyber threats targeting connected medical devices, hospital networks, and remote monitoring platforms, where a single vulnerability could jeopardize patient safety and data integrity [Alani et al. 2023a]. These IDSs are typically trained on datasets composed of features and samples, which must be representative to ensure accurate detection of both normal and malicious network behavior. As IoMT adoption continues to expand, ensuring the robustness of IDS solutions becomes increasingly urgent to protect interconnected healthcare systems from evolving cyber threats.

## 3. Literature Review

In recent years, an expanding body of research has investigated the integration of Healthcare 5.0 principles with cybersecurity frameworks. This section reviews studies in this domain. Additionally, a comparative analysis is presented in Table 1, which evaluates the approaches and limitations of these works in relation to the current study.

**Table 1. Comparison to the Related Works.**

| Reference | Biomedical Feature Impact Analysis on IDS | Biomedical Feature Merged with IDS | EHMS Dataset | XAI |
|---|---|---|---|---|
| [Alani et al. 2023b] | No | Yes | Yes | Yes |
| [Alani et al. 2023a] | No | Yes | Yes | Yes |
| [Aljuhani et al. 2024] | No | Yes | Yes | Yes |
| [Tauqeer et al. 2022] | No | Yes | Yes | No |
| [Ghubaish et al. 2024] | No | Yes | Yes | No |
| [Dave et al. 2020] | - | - | No | Yes |
| [Sohail et al. 2024] | No | No | Yes | Yes |
| [Ashraf et al. 2024] | - | - | No | Yes |
| Our work | Yes | Yes | Yes | Yes |

The work [Hady et al. 2020] introduces the WUSTL-EHMS-2020 dataset, demonstrating that combining network flow metrics and biomedical data improves intrusion detection in healthcare. The authors developed an Enhanced Healthcare Monitoring System (EHMS) testbed, which leverages machine learning capabilities to address security challenges using a range of healthcare sensors. The system comprises a gateway for data collection, an IDS computer to monitor network traffic and identify anomalous activities, an attacker module to simulate real-world attack scenarios, and a server. The system enables the evaluation of how integrating network and biometric data enhances the detection of intrusions in healthcare environments.

The studies [Alani et al. 2023b] and [Alani et al. 2023a] proposed systems to protect IoMT devices using robust classifier algorithms, leveraging the WUSTL-EHMS-2020 dataset and analyzing results with the SHAP framework. Both works provided only summary plots ranking features and focused on the impact of network features, identifying the most influential ones while noting features with minimal or no contribution to the classifier outputs. However, the studies did not explore biomedical features or emphasize the multiclass nature of the classification, leaving a significant gap in the analysis of biomedical aspects and limiting the comprehensiveness of their evaluation.

The research [Aljuhani et al. 2024] explores the balance between practicality and security in healthcare environments that utilize IoMT on a daily basis. It proposes a system that employs ensemble machine learning and deep neural networks to classify attacks and normal traffic using the WUSTL-EHMS-2020 dataset. The results are analyzed using SHAP tools, which rank the features that most significantly impact the algorithm's output. Among these, blood pressure and peripheral oxygen saturation emerge as highly influential features. Nevertheless, the study limits its analysis to feature ranking without delving deeper into the underlying reasons or implications of these findings.

The analysis by [Tauqeer et al. 2022] highlights the significance of IoMT and its associated security challenges, employing multiple machine learning algorithms to classify cyberattacks and normal connections using the WUSTL-EHMS-2020 dataset, achieving strong accuracy. Similarly, [Ghubaish et al. 2024] addresses the complexities of IoMT environments and introduces a feature engineering approach for ML, evaluated on three datasets, including WUSTL-EHMS-2020. While both studies deploy algorithms for cyberattack detection, neither incorporates explainability into their methodologies.

The authors of [Sohail et al. 2024] explored the use of IDS in the IoMT domain, focusing on multiclass classification of cyberattacks using three boosting algorithms. They employed the CICIoMT-2024 dataset, which contains only IoMT traffic data without biomedical data. To improve model interpretability, they integrated SHAP, offering transparency into the IDS framework's decision-making process.

Furthermore, [Dave et al. 2020] emphasizes AI explainability for IoMT systems, demonstrating SHAP and LIME on heart disease datasets to interpret black-box models. [Ashraf et al. 2024] similarly applies these techniques to disease prediction data based on symptoms, increasing transparency in AI decision-making.

## 4. Material & Methods

This section describes the methodology used to analyze explainability in the WUSTL-EHMS-2020 dataset. The study applies SHAP analysis to assess the impact of network and biomedical features on intrusion detection models.

### 4.1. Dataset

The WUSTL-EHMS-2020 dataset [Hady et al. 2020] was collected in a controlled testbed environment, where IoMT sensors attached to a patient's body transmitted physiological signals to a gateway device. These signals were relayed through a network switch and router to a server for real-time monitoring. Although, the transmission path was vulnerable to interception by malicious users seeking to compromise sensitive medical data.

The dataset provides both binary and multiclass labeling. In this study, we adopt the latter, which includes three classes: benign, spoofing, and data alteration. Spoofing attacks intercept and manipulate network packets, compromising data confidentiality, while data alteration attacks modify packet contents to undermine integrity. To address these threats, an IDS was deployed in the testbed to capture both network and biomedical data, analyzing them for anomalies. The dataset consists of 16,318 samples, with 14,272 (87.5%) labeled as benign and 2,046 (12.5%) as attacks. It includes 45 features, comprising:

- **35 network flow metrics**, such as packet transmission rates and protocol-specific metadata.
- **8 biometric measurements**, including heart rate and oxygen saturation.
- **2 classification labels**, representing the binary attack indicator (Normal or Attack) and the multiclass attack category (Normal, Spoofing, or Data Alteration).

Integrating network and biomedical features enables context-aware anomaly detection, bridging cybersecurity with human-device interactions in Healthcare 5.0. Multiclass labeling enhances classification granularity and supports SHAP-based interpretability, improving insights into intrusion detection models in healthcare environments.

### 4.2. Methodology

The methodology adopted to analyze the WUSTL-EHMS-2020 dataset followed a structured pipeline (Figure 1), consisting of data preprocessing, model training, evaluation, and explainability.

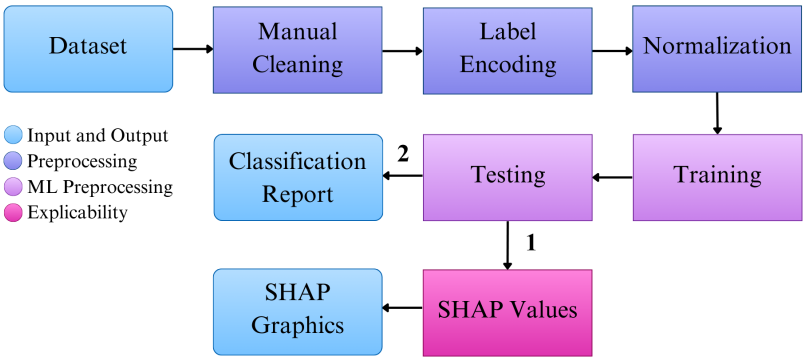



**Figure 1. Methodology Flow Chart.**

As shown in Figure 1, preprocessing was performed in multiple steps to prepare the dataset for machine learning models. Manual cleaning involved removing non-contributory features: the `Source MAC Address` and `Label` columns were discarded to prevent model overfitting, as attacks originated from a single device. The `Attack Category` was retained as the target variable, while `Dir` and `Flgs` features were dropped due to missing records. Additionally, three anomalous samples with invalid `Source Port` entries were excluded, resulting in a dataset with 16,315 samples.

Next, categorical features were encoded using scikit-learn's LabelEncoder, ensuring compatibility with ML models. Without this transformation, features such as `Source Port` would contain NaN values, which lack SHAP interpretability. To ensure numerical stability, all features were normalized using StandardScaler. The dataset was split into 80% training and 20% testing subsets, as shown in Figure 1 (Training and Testing steps).

After preprocessing, the dataset was used to train and evaluate four classifiers: XGBoost (XGB), Random Forest (RF), Decision Tree (DT), and Support Vector Classifier (SVC). These models were selected for their ability to handle imbalanced datasets and structured tabular data. XGB was chosen for its gradient-boosting approach, which improves learning efficiency while incorporating regularization techniques to mitigate overfitting [Chen and Guestrin 2016]. RF, an ensemble of decision trees, was employed for its bagging strategy and feature randomness, enhancing generalization while maintaining feature importance interpretability. SVC was used for its ability to model nonlinear decision boundaries in high-dimensional spaces, making it effective in detecting subtle attack patterns. Finally, DT [Pedregosa et al. 2011] was included as a simpler, rule-based classifier, offering an interpretable reference point for comparison.

To assess classification performance, precision, recall, and F1-score were computed. Precision quantifies the proportion of correctly predicted attacks among all attack predictions, whereas recall evaluates the model's ability to identify actual attacks. Since IDSs must balance false positives and false negatives, F1-Score was selected as the harmonic mean of precision and recall, ensuring a reliable metric for assessing effectiveness.

To ensure model interpretability, SHAP was applied to assess feature importance. As indicated in Figure 1, SHAP Graphics were generated to analyze how each feature influenced classification decisions. By leveraging Shapley values from game theory,

SHAP provides a transparent and interpretable framework for understanding the decision-making process of intrusion detection models [Lundberg and Lee 2017]. In order to assure the results reproducibility, the materials used are publicly available[2].

## 5. Results and Discussion

This section shows a model performance evaluation. Also, it is presented and discussed the feature impact in model prediction from the XAI perspective.

### 5.1. Classification Results

Using the Classification Report function from the Scikit-learn[3], we computed the precision, recall, and F1-score for each label, with results presented in Table 2. According to these results, all models achieved high F1-scores for Benign and Data Alteration labels. However, detecting spoofing attacks posed significant challenges, with performance varying widely across classifiers. This issue is likely influenced by the class imbalance in the dataset, where malicious samples account for only 12.5% of the data.

**Table 2. Testing Results With Four Classifiers**

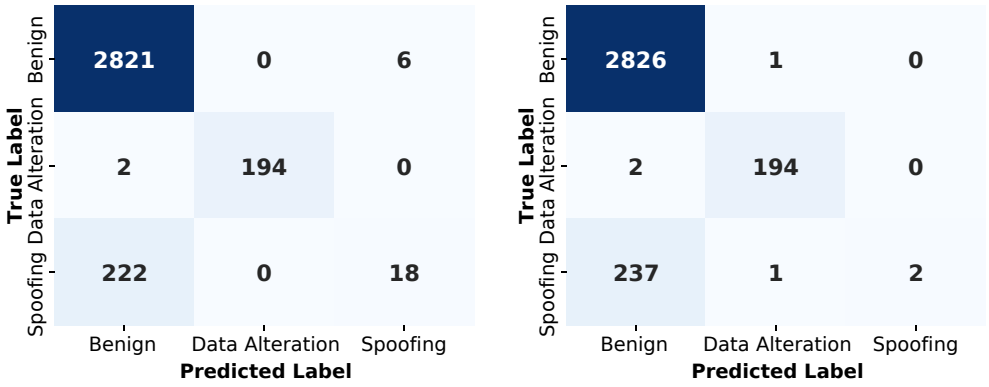
| Model | Label | Precision | Recall | F1-Score |
|---|---|---|---|---|
| XGB | Benign | 0.98 | 0.99 | 0.99 |
| | Data Alteration | 0.99 | 0.99 | 0.99 |
| | Spoofing | 0.92 | 0.72 | 0.81 |
| RF | Benign | 0.93 | 1.00 | 0.96 |
| | Data Alteration | 1.00 | 0.99 | 0.99 |
| | Spoofing | 0.75 | 0.07 | 0.14 |
| DT | Benign | 0.97 | 0.98 | 0.97 |
| | Data Alteration | 1.00 | 1.00 | 1.00 |
| | Spoofing | 0.71 | 0.67 | 0.69 |
| SVC | Benign | 0.92 | 1.00 | 0.96 |
| | Data Alteration | 0.99 | 0.99 | 0.99 |
| | Spoofing | 1.00 | 0.01 | 0.02 |

Notably, Random Forest and Support Vector Machines performed poorly in identifying spoofing attacks, as evident in their confusion matrices (Figure 2). Both models exhibit a high misclassification rate, with RF misclassifying 222 spoofing samples as benign and SVC misclassifying 237 spoofing samples as benign, leading to very low recall scores (Table 2). This suggests that these models struggle to distinguish spoofing from benign traffic, potentially due to overlapping feature distributions. Deeper analysis suggests the RF's tendency to favor the class with more number of samples—imbalance datasets results in weak learning of the spoofing class, whereas SVC's margin-maximization criterion and choice of kernel may fail to capture the nuanced patterns of spoofed samples, compounding their misclassification rates.

In contrast, XGBoost demonstrated more consistent performance across all labels, particularly in spoofing detection, achieving a recall score of 0.72, significantly outperforming RF (0.07) and SVC (0.01). XGB's superior performance can be attributed to its

[2]Available at: `https://github.com/lps5e/IA2S/`

[3]Scikit-learn library. Available at: `https://scikit-learn.org/`




(a) Confusion Matrix - RF.

(b) Confusion Matrix - SVC.

**Figure 2. Confusion matrices for RF and SVC classifiers, highlighting misclassification issues in spoofing detection.**

gradient-boosting framework, which effectively handles imbalanced datasets and reduces overfitting. Consequently, XGB was selected for SHAP-based explainability analysis, as it provides the most reliable attack classification while maintaining model interpretability.

### 5.2. Explaining Feature Contributions using SHAP Analysis

This section presents SHAP explainability plots to identify the most relevant features in predicting each attack category. Two plot types were generated: (i) the summary bar plot, which ranks features by their average SHAP values, and (ii) the summary plot, which provides a detailed view of feature contributions across samples.

Figure 3 illustrates the SHAP summary bar plot, ranking the ten most influential features by their mean SHAP values. As expected, Source Load (`SrcLoad`) appears as the most impactful feature in Data Alteration detection, reinforcing the idea that attackers often manipulate traffic rates to evade anomaly detection. Attackers may introduce artificial delays, reduce transmission rates, or flood the network with modified packets, making `SrcLoad` variations a strong indicator of malicious activity. Similarly, Destination Interpacket Arrival Time (`DIntPkt`) emerges as another critical feature across all classifications. Higher interpacket arrival times can suggest stealthy attack techniques, where adversaries intentionally slow down data transmission to avoid triggering rate-based IDS mechanisms. The Source Port (`Sport`) also plays a major role, particularly in Benign and Spoofing classifications, aligning with well-documented spoofing strategies where attackers modify source port numbers to masquerade as legitimate traffic [Sasi et al. 2024]. The presence of `DstJitter` and `SrcJitter` in the top-ranked features further supports the hypothesis that attackers tend to introduce irregular packet timing, a common evasion technique to avoid signature-based IDS detection.

Interestingly, several biomedical features also appear among the most relevant indicators of intrusions, particularly in spoofing detection. Features such as Temperature (`Temp`), Pulse Rate, Peripheral Oxygen Saturation (`SpO2`), Respiratory Rate (`Resp Rate`), and ECG ST Segment (`ST`) demonstrate significant contributions to classification, reinforcing the argument that physiological signals should not be overlooked in cybersecurity applications. One possible explanation is that spoofing attacks may introduce

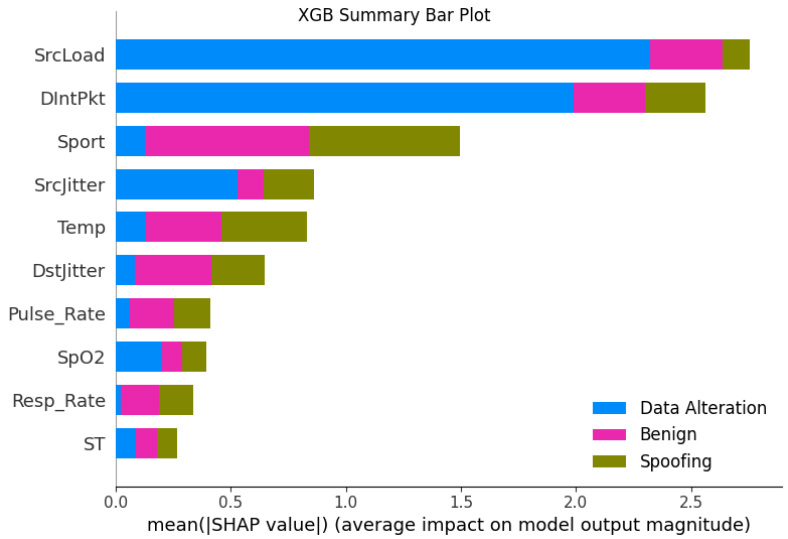


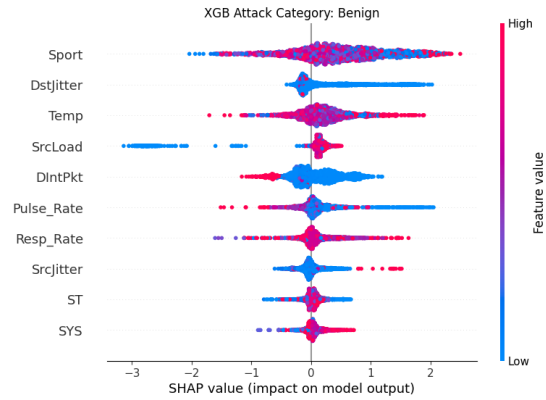

**Figure 3. SHAP Summary Bar Plot.**

anomalies in biomedical data streams, either through sensor interference, adversarial data injections, or inconsistencies in physiological responses during an attack event. For instance, anomalous fluctuations in temperature or heart rate could indicate tampering with wearable or implantable medical devices, as seen in previous research on biomedical sensor vulnerabilities [Khan et al. 2020]. These findings emphasize the potential for hybrid IDS models, where integrating both network and biomedical features can enhance the detection of cyber-physical attacks in Healthcare 5.0 environments.

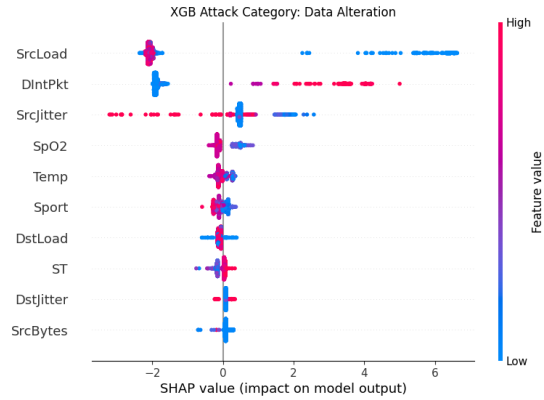
Sequentially, using SHAP summary plots, each classification label will be thoroughly examined for a more detailed approach. Figure 4(a) presents the SHAP summary plot for the Benign label, highlighting the ten most relevant features. Positive SHAP values indicate a higher likelihood of benign classification, while negative values push the prediction toward a non-benign label. The color scale represents the magnitude of each feature value, from low (blue) to high (red).

The most relevant feature is `Sport`. Lower port numbers (blue, left-skewed dots) correlate with non-benign traffic, whereas higher and medium port numbers are linked to benign traffic. This divergence likely stems from differences in port allocation mechanisms, as benign traffic typically adheres to standard automated port assignment protocols, whereas malicious traffic frequently employs manually specified ports. Other network-related features are also present, `DstJitter` and `DIntPkt` indicate that lower variation in time between packets and lower interpacket arrival time in destination contribute to identifying a sample as Benign. However, the opposite occurs for `SrcJitter` and `SrcLoad`, where lower variation and lower load at the source push the classification as a non-benign classification. Additionally, biomedical features such as `Temp`, `Pulse_Rate`, `Resp_Rate`, `ST`, and `SYS` also contribute to the classifier's decision-making. Their presence among the most relevant features suggests that physiological data might hold useful information for distinguishing benign traffic.

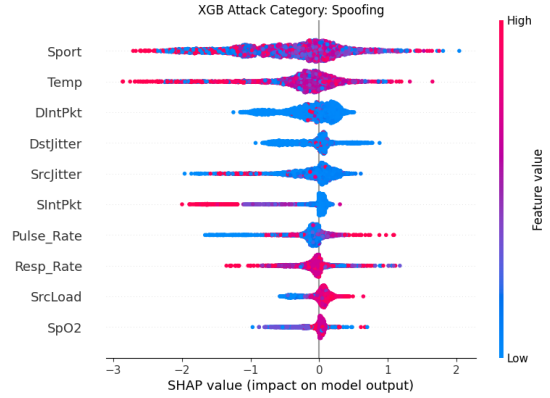
Figure 4(b) represents the SHAP Plot for the Data Alteration label, which refers to instances of packet modification that violate data integrity. `SrcLoad` is the attribute with the strongest predictive influence. According to the analysis, smaller `SrcLoad`




(a) SHAP Summary Plot Benign.




(b) SHAP Summary Plot Data Alteration.




(c) SHAP Summary Spoofing.

**Figure 4. SHAP plots showing feature importance for (a) benign, (b) data alteration and (c) spoofing attacks.**

values are highly correlated with classifications that lean toward malicious, while higher values cause predictions to lean toward normal traffic. On the other hand, `DIntPkt` shows that high interpacket arrival times are relevant for detecting Data Alteration attacks. This pattern is consistent with well-known evasion strategies used in cyberattacks, where malicious actors frequently reduce data transfer speeds to evade detection systems, resulting in low bit rates and high arrival times. Additionally, `SrcJitter` with high values contributes to reducing SHAP values, indicating a lower occurrence of Data Alteration attacks when those values are high. Furthermore, we observe that biomedical features (`SpO2`, `Temp`, `ST`) appear in the plot with SHAP values fluctuating within a limited range, suggesting that while they have some level of variability, their impact on the model's decision-making process is less pronounced compared to network-related attributes. This indicates that, for Data Alteration attacks, the model relies primarily on network-based features, though the potential role of biomedical data in other attack scenarios should not be disregarded.

Lastly, Figure 4(c) highlights the most influential features for detecting spoofing attacks. The network feature `Sport` and the biomedical feature `Temp` exhibit the strongest impact on model predictions. Lower `Sport` values (blue) tend to reduce the likelihood of a spoofing attack, whereas higher values (red) push the model toward predicting spoofing. Similarly, `Temp` exhibits a wide range of SHAP values, indicating that

variations in body temperature are considered by the model when predicting spoofing attempts, though the exact nature of this relationship requires further analysis.

Network-related attributes such as `DIntPkt`, `DstJitter`, and `SrcJitter` suggest that lower values increase the likelihood of an attack, reinforcing the idea that spoofing attacks often involve altered timing characteristics. Additionally, `SrcLoad` suggests that increased source load may be indicative of spoofing activity, possibly due to altered traffic patterns in such attacks.

Overall, spoofing detection appears weaker compared to other attack categories, as previously discussed in Section 5.1 and summarized in Table 2. This limitation may stem from the nature of spoofing attacks.

## 6. Conclusion and Future Works

Existing datasets and experimental frameworks in IDS predominantly focus on network traffic data, with empirical analyses largely confined to network-layer attacks. In IoT-health ecosystems, adversarial manipulations of biomedical sensor data remain critically understudied due to this methodological gap. By incorporating cutting-edge technologies, the Healthcare 5.0 idea seeks to address this problem. Through SHAP value analysis, our investigation reveals that network traffic features dominate categorization outcomes in all scenarios. In contrast, biomedical sensor inputs—such as heart rate, blood pressure, and glucose monitoring data—demonstrate relevance in most cases. However, their low attribution scores in data alteration attack detection indicate negligible influence on model decisions. For future work, we intend to (i) investigate the inclusion of more intricate datasets, particularly those incorporating clinically significant biomedical attack vectors, addressing the need for evaluation in diverse clinical contexts, and (ii) perform XAI analysis across biomedical, network, and combined data, exploring three different groups.

## Acknowledgments

This research effort is sponsored in part by resources from “Edital PRPGP/UFSM N.50/2024 - Programa de Fortalecimento e Redução de Assimetrias da Pós-Graduação da UFSM”. Also, this work is partially supported by CIARS RITEs/FAPERGS project.

## References

Alani, M. M., Mashatan, A., and Miri, A. (2023a). Explainable ensemble-based detection of cyber attacks on internet of medical things. In *Int Conf on Dependable, Autonomic and Secure Computing, Int Conf on Pervasive Intelligence and Computing, Int Conf on Cloud and Big Data Computing, Int Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 0609–0614. IEEE.

Alani, M. M., Mashatan, A., and Miri, A. (2023b). XMeDNN: An Explainable Deep Neural Network System for Intrusion Detection in Internet of Medical Things. In *International Conf. on Information Systems Security and Privacy*, pages 144–151.

Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., and Herrera, F. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. *Information Fusion*, 99:101805.

Aljuhani, A., Alamri, A., Kumar, P., and Jolfaei, A. (2024). An Intelligent and Explainable SaaS-Based Intrusion Detection System for Resource-Constrained IoMT. *IEEE Internet of Things Journal*, 11(15):25454–25463.

Ashraf, K., Nawar, S., Hosen, M. H., Islam, M. T., and Uddin, M. N. (2024). Beyond the Black Box: Employing LIME and SHAP for Transparent Health Predictions with Machine Learning Models. In *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, pages 1–6. IEEE.

Chen, T. and Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '16, pages 785–794, New York, NY, USA. ACM.

Dave, D., Naik, H., Singhal, S., and Patel, P. (2020). Explainable AI meets Healthcare: A Study on Heart Disease Dataset. *arXiv preprint arXiv:2011.03195*.

Gadekallu, T. R., Maddikunta, P. K. R., Boopathy, P., Deepa, N., Chengoden, R., Victor, N., Wang, W., Wang, W., Zhu, Y., and Dev, K. (2024). XAI for Industry 5.0 - Concepts, Opportunities, Challenges and Future Directions. *IEEE Open Journal of the Communications Society*, pages 1–1.

Ghubaish, A., Yang, Z., Erbad, A., and Jain, R. (2024). LEMDA: A Novel Feature Engineering Method for Intrusion Detection in IoT Systems. *IEEE Internet of Things Journal*, 11(8):13247–13256.

Hady, A. A., Ghubaish, A., Salman, T., Unal, D., and Jain, R. (2020). Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access*, 8:106576–106584.

Javeed, D., Gao, T., Kumar, P., and Jolfaei, A. (2024). An Explainable and Resilient Intrusion Detection System for Industry 5.0. *IEEE Transactions on Consumer Electronics*, 70(1):1342–1350.

Khan, N., Ahmad, K., Tamimi, A. A., Alani, M. M., Bermak, A., and Khalil, I. (2024). Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview of the Literature, associated Challenges, the existing Solutions, and Potential Research Directions. *arXiv preprint arXiv:2408.03335*.

Khan, S., Parkinson, S., Grant, L., Liu, N., and Mcguire, S. (2020). Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. *ACM Computing Surveys*, 53(4):1–29.

Lundberg, S. M. and Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R., editors, *Advances in Neural Information Processing Systems 30*, pages 4765–4774. Curran Associates, Inc.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., and Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830.

Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., and Iqbal, S. (2024). A comprehensive survey on iot attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, 2(6):455–513.

Sohail, F., Bhatti, M. A. M., Awais, M., and Iqtidar, A. (2024). Explainable Boosting Ensemble Methods for Intrusion Detection in Internet of Medical Things (IoMT) Applications. In *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, pages 1–8. IEEE.

Statista (2025). Digital Health - Worldwide. Available in: `https://www.statista.com/outlook/hmo/digital-health/worldwide`. Accessed on February 20, 2025.

Tandel, V., Kumari, A., Tanwar, S., Singh, A., Sharma, R., and Yamsani, N. (2024). Intelligent wearable-assisted digital healthcare industry 5.0. *Artificial Intelligence in Medicine*, 157:103000.

Tauqeer, H., Iqbal, M. M., Ali, A., Zaman, S., and Chaudhry, M. U. (2022). Cyberattacks detection in iomt using machine learning techniques. *Journal of Computing & Biomedical Informatics*, 4(01):13–20.