IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
University of Kut Journal
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
Special Issue for the Researches of the 6th Int. Sci. Conf. for Creativity for 16 -17 April 2025

Intelligent Cyber Attacks Detection Approaches in Internet of Medical Things Environment: Current Challenges and Future Solutions

Manar Laith [1] , Hiba Zuhair [2]

Abstract

The Internet of Medical Things (IoMT) offers significant benefits for healthcare but faces growing cybersecurity challenges. This paper provides a holistic panorama of cyber-attacks detection systems developed recently for IoMT environment. By exploring the evolution and impact of cyber-attack versions, including Denial of Service (DoS), malware, Man-in-the-Middle (MitM), and data injection attacks; the detection approaches are categorized and examined including signature-based, anomaly-based, and hybrid-based approaches those leverage machine learning and deep learning algorithms. Then, the key distinction of detection approaches that assisted by ensemble machine learning, is highlighted to demonstrate their superior performance outcomes for securing IoMT environment through characterizing the challenges acquired to optimize in the nearest future research direction. As such, challenges of defeating the sophisticated cyber-attacks and the need to improve the existing detection approaches would provide valuable insights to researchers aiming at finding optimized cyber-defense to save operation of IoMT systems.

Keywords: Cyber-attacks, Anomaly Detection, Ensemble Machine Learning, Intrusion Detection Systems (IDS), Internet of Medical Things (IoMT)

Affiliation of Authors

[1, 2] Department of Automation and Artificial Intelligence Engineering, College of Information Engineering, Al-Nahrain University, Iraq, Baghdad, 1000

[1]manar.msei23@ced.nahrainuniv.edu.iq
[2]hiba.zuhair.pcs2013@nahrainuniv.edu.iq

[1] **Corresponding Author**

Paper Info.
Published: Oct. 2025

مناهج الكشف الذكي عن الهجمات السيبرانية في بيئة إنترنت الأشياء الطبية: التحديات الحالية والحلول المستقبلية

منار ليث [1] ، هبة زهير [2]

المستخلص

يقدم إنترنت الأشياء الطبية (IoMT) فوائد كبيرة لقطاع الرعاية الصحية، لكنه يواجه تحديات متزايدة في مجال الأمن السيبراني. تستعرض هذه الورقة بشكل شامل أنظمة كشف الهجمات السيبرانية التي تم تطويرها مؤخرًا في بيئة IoMT. من خلال تحليل تطور وتأثير أنواع الهجمات السيبرانية، مثل هجمات حجب الخدمة (DoS)، والبرمجيات الخبيثة، وهجمات الرجل في الوسط (MitM)، وهجمات حقن البيانات، يتم تصنيف ودراسة طرق الكشف، والتي تشمل الأساليب القائمة على التوقيع، والأساليب القائمة على الشذوذ، والأساليب الهجينة التي تستفيد من خوارزميات التعلم الآلي والتعلم العميق. بعد ذلك، يتم تسليط الضوء على الميزة الأساسية لأساليب الكشف المدعومة بتعلم الآلة التجميعي، لإثبات تفوق أدائها في تأمين بيئة IoMT، مع التركيز على التحديات التي يجب معالجتها في أبحاث المستقبل القريب. ومن هذا المنطلق، فإن التحديات المتعلقة بمواجهة الهجمات السيبرانية المتطورة والحاجة إلى تحسين أساليب الكشف الحالية، توفر رؤى قيمة للباحثين الذين يسعون إلى تطوير حلول دفاعية سيبرانية محسنة لضمان استمرارية عمل أنظمة IoMT.

الكلمات المفتاحية: الهجمات السيبرانية، كشف الشذوذ، تعلم الآلة التجميعي، أنظمة كشف التسلل (IDS)، إنترنت الأشياء الطبية (IoMT)

انتساب الباحثين

[1، 2] قسم هندسة الاتمتة والذكاء الاصطناعي، كلية هندسة المعلومات، جامعة النهرين، العراق، بغداد، 10001

[1]manar.msei23@ced.nahrainuniv.edu.iq
[2]hiba.zuhair.pcs2013@nahrainuniv.edu.iq

[1] **المؤلف المراسل**

معلومات البحث
تأريخ النشر: تشرين الاول 2025

I. INTRODUCTION

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling real-time

patient monitoring, predictive analytics, and personalized treatment plans. However, the rapid proliferation of IoMT devices has introduced significant cybersecurity challenges. These devices often lack robust security features, making them vulnerable to cyberattacks such as data breaches, ransomware, and man-in-the-middle (MitM) attacks. For instance, attacks on insulin pumps and pacemakers have demonstrated the life-threatening consequences of compromised IoMT systems [1] [2].

The need for hybrid detection mechanisms arises from the limitations of traditional security approaches, which struggle to address the dynamic and heterogeneous nature of IoMT environments. Hybrid methods, combining machine learning (ML) and deep learning (DL) techniques, have shown promise in improving detection accuracy and reducing false positives. For example, ensemble learning models like Random Forest and XGBoost have achieved over 98% accuracy in detecting intrusions in IoMT networks [3].

The current security landscape is marked by an increasing reliance on Intrusion Detection Systems (IDS) tailored for IoMT. These systems must balance high detection rates with low computational overhead to operate effectively in resource-constrained environments. Recent advancements, such as the integration of federated learning and edge computing, have further enhanced the scalability and efficiency of IDS in healthcare settings [2] [4].

The importance of securing IoMT cannot be overstated, as cyberattacks on medical devices can compromise patient safety, disrupt healthcare services, and lead to significant financial losses. For example, ransomware attacks on hospitals have resulted in operational shutdowns and delayed patient care, underscoring the critical need for robust IDS solutions.

This review focuses on detection techniques that leverage hybrid AI models, including ensemble learning, deep learning, and feature engineering methods. These techniques are evaluated for their ability to detect a wide range of attacks, such as Distributed Denial of Service (DDoS), malware infections, and zero-day exploits, which are prevalent in IoMT environments [3].

The implementation environments covered include cloud-based systems, edge computing frameworks, and decentralized architectures like federated learning. These environments are critical for ensuring real-time threat detection while addressing the resource constraints of IoMT devices [2] [4].

The primary goal of this review is to evaluate the effectiveness of ensemble machine learning algorithms in IDS models for detecting cyberattacks in IoMT environments. Specific objectives include assessing the performance of ensemble techniques using metrics such as accuracy, recall, F1-score, and false positive rates. The review also addresses challenges such as high computational overhead, scalability issues, and the detection of zero-day attacks in IoMT systems. Expected outcomes involve identifying the most effective ensemble models and providing practical recommendations for their implementation in real-world IoMT environments. The contribution to the field includes offering a comprehensive roadmap for future research, including the integration of lightweight ensemble models, federated learning for privacy preservation, and adaptive mechanisms for evolving threats.

II. CYBER-ATTACKS IN IOMT ENVIRONMENT

a. Denial of Services (DoS/DDoS):

Medical devices that are found in the healthcare sector are in high dependency on the Internet of Medical Things (IoMT). However, this growing reliance is leading to major security challenges, especially with DoS/DDoS attacks which are becoming an unignorable issue. The DoS/DDoS are now coming in different and more sophisticated forms, Volumetric Attacks that consume bandwidth resources, Protocol Attacks that exhaust server's resources, and Application Layer Attacks that are able to take down the healthcare application themselves. In detailed study performed by Hernandez-Jaimes, et al [5], it has been reported that DDoS attacks in IoMT environments are on the rise and nearly one third of all security incidents. As a result of those incidents, Modern Intrusion Detections Systems (IDS) have adapted to recognizing the DDoS attacks by analyzing the Abnormal Traffic Signature, Protocol Activity and Resource Consumption Pattern Detection. Based on this evolution, Khraisat et al. [6] showed a very promising steps towards achieving good detection capabilities with a nearly perfect accuracy and low false alarm rate by using a Hybrid IDS that can overcome the disadvantages of Signature-Based IDS (SIDS) and Anomaly-Based IDS (IDS) by using Naïve Bayes and decision tree based that was able to achieve detection rate of 99.63%.

Despite the significant progress that has been made in detection capability, the use of such systems within healthcare environment would require innovative solutions that are tailored with thoughtful considerations. Adaptive Federated Learning Approach to DDoS (FLAD), as it is introduced by Doriguzzi-Corin et al. [7], is an adaptive approach of Federated Learning (FL) implement a mechanism to monitor the classification accuracy of the global model on the client's validations sets without requiring any exchange of data and thanks to this mechanism it can estimate the performance of the aggregated model and dynamically tune the FL process by assigning more computation to those clients whose attack profiles are harder to learn. FLAD has been proven to significantly reduce convergence time while also enhancing classification accuracy when compared to current state-of-the-art FL Solutions.

b. Man-in-the-Middle (MITM) Attacks

The Transition of the healthcare Environments from a manual environment to an Automated one has brough in unavoidable security loopholes where Man-in-The-Middle (MITM) attacks distinguishes themselves among the significant emerging threats that disrupt clinical communications. Over the years, these attacks have improved such as those that intercept and manipulate sensitive data within the healthcare IT Systems.

According to Ahmed et al. [8], a detailed study shows that in the healthcare sector MITM attacks may succeed via one of three advanced delivery mechanisms: Manipulation of medical device protocols, Hijack of essential patient data sessions, or Interception of private and confidential medical traffic. Messinis et al. [9]even go as far as to emphasize the severity of this type of attacks in relation to the IoMT Networks and its potential serious repercussions, highlighting that MITM attacks can inflict irreparable damage to medical data integrity and patient confidentiality due to its sophisticated protocol exploitation techniques.

To counter these nested threats, the cybersecurity community has been producing effective detection

methods for some time and recent development in artificial intelligence, such as the model proposed by Iddrisu et al. [10], a Convolutional Neural Network (CNN) based system that proved its practicality by achieving an impressive 98.6% accuracy score. CCN Algorithm can potentially enhance the detection of MITM attacks by effectively analyzing network traffic data and identifying subtle attack patterns that traditional methods may overlook since it is influenced by the architecture and functioning of the visual cortex of the brain which is also known for its ability to detect and identify visual patterns. [9]

c. Data Injection Attacks

In addition to the previously discussed attacks, IoMT networks are also highly susceptible to Data Injection Attacks which poses an alarming threat to medical systems. Such advance attacks can take the form of SQL Injection, Command Injection and False Data Insertion, all of which are serious threats that can resonate through the healthcare operations. [5], Stated that the healthcare sector present with particular vulnerabilities toward these types of attacks because of its capability of altering patient information, device settings and treatment protocols. Their work has highlighted the manner in which these cyber-attacks can exploit weak points in the healthcare IT systems — database interfaces and data-in-transit — and how that, in turn, places patients at significant risk.

This has led to tremendous advances in combating these threats using new and innovative detection techniques. modern intrusion detection systems, through their extensive recording methods are able to prove effective in detecting injection-based attacks as indicated in systematic review by Alqhtani et al. [11], Their findings show that using queries based on suspicious input patterns, observing structural variations in query plans and tracking data integrity variations with the help of these features allows detection systems to have high accuracy in identifying instances where attacks are being conducted.

d. Authentication Attack

With Authentication attacks are a critical threat to the Internet of Medical Things (IoMT), as they exploit weak or compromised authentication mechanisms to gain unauthorized access to medical devices and sensitive patient data. These attacks often target vulnerabilities in password-based systems, biometric authentication, or cryptographic protocols, leading to data breaches, device manipulation, and even life-threatening consequences. For example, attackers can exploit weak passwords or stolen credentials to impersonate legitimate users, gaining access to insulin pumps, pacemakers, or other critical medical devices [1] [12].

Intrusion Detection Systems (IDS) play a vital role in mitigating authentication attacks by monitoring network traffic and identifying suspicious activities. Machine learning-based IDS models, such as Random Forest and XGBoost, have demonstrated high accuracy (up to 99.5%) in detecting unauthorized access attempts and anomalous behavior in IoMT networks [3] [4]. These models leverage feature selection techniques, such as Mutual Information (MI) and Principal Component Analysis (PCA), to reduce computational complexity and improve detection performance [3] [4]. Additionally, federated learning-based IDS frameworks have emerged as a promising solution, enabling distributed detection while preserving data privacy. These frameworks achieve detection accuracy rates of 95–99% and are particularly effective against zero-day

authentication attacks [13] [14]. Despite these advancements, challenges remain in implementing IDS for authentication attacks in IoMT. Resource constraints of medical devices, such as limited computational power and memory, necessitate the development of lightweight detection algorithms. Furthermore, the heterogeneity of IoMT devices and communication protocols complicates the deployment of standardized security solutions [13] [14].

e. Protocol-Specific Attacks

As it has been stated before, the emerging of IoMT has sparked a great deal of examination of the vulnerabilities associated with network protocols which in turn is driving many IDS systems to play a critical role for protecting healthcare communications amongst other mission-assisted services. Dupont [15] performed a groundbreaking laboratory study that unmasked various techniques through which attackers can undermine healthcare protocols through specific techniques such as spoofing, which allows them to impersonate legitimate devices and gain unauthorized access to sensitive data.

Based on such insights, Mejía-Granda et al. [16]have showed how these vulnerabilities exist in actual medical devices and have argued for detection methods that are sophisticated enough to detect protocol anomalies prior to affecting patient care delivery. Muñoz and Valiente [17] also present a state-of-the-art work on graph-based protocol analysis that attains 98.16% classification accuracy on malicious network behavior with low interference level as false alarms that can hinder critical medical services. Almeghlef [18] has further supplemented this protocol security progress by addressing CoAP protocols challenges to conduct in secure healthcare environments. Their decision to approach IDS differently pays off, and they have a high detection rate of application layer protocol attacks through analysis of protocol behaviors in real-time. These are major advancements in the protections surrounding various communications between one medical device and another, which correspondingly may be increasingly sensitive to even small protocol violations due to their lifesaving implications.

The evolution of cyber-attacks in IoMT environments from 2015 to 2025 demonstrates a significant escalation in their impact and sophistication. Figure 1 illustrates the progression of four major attack types: DDoS, Malware Infections, Man-in-the-Middle (MitM), and Data Injection attacks. The analysis reveals a concerning trend where attacks that were once considered moderate or low impact have evolved to become severe threats. Notably, both DDoS and Malware attacks have progressed from moderate impact in 2015 to extreme impact levels predicted for 2024-2025, while MitM attacks have evolved from low to very high impact. This escalation underscores the critical need for robust detection mechanisms in IoMT environments. The impact of the main cyber-attacks in IoMT detected by Intrusion Detection Systems (IDS) over the past decade is measured based on the frequency of attacks, detection accuracy, and potential consequences on healthcare systems. as shown in Figure (1)

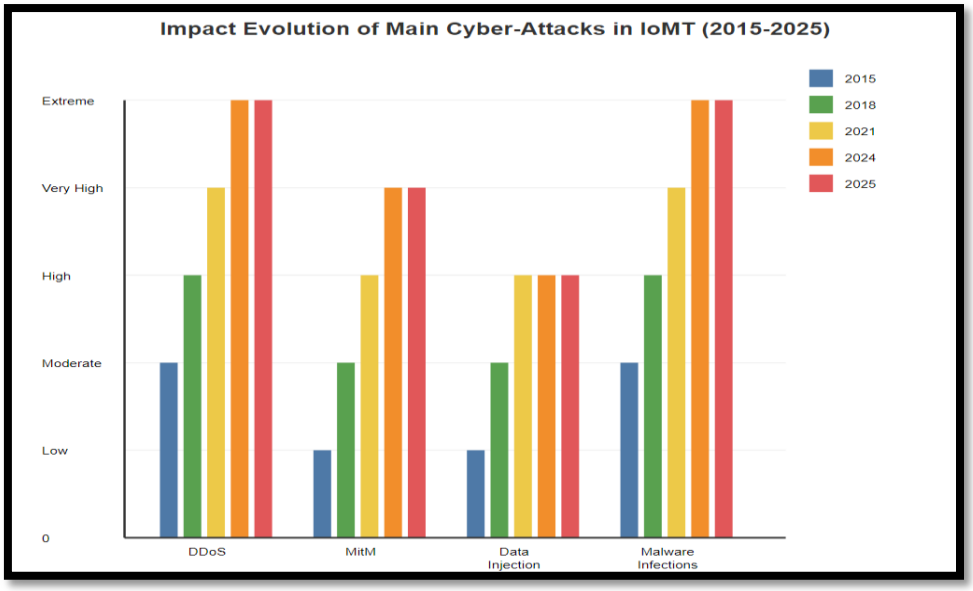

Figure 1 Impact Evolution of Main Cyber-Attacks in IoMT (2015-2025)

III. Analysis of Cyber-Attacks Detection Approaches in IoMT

The rapid adoption of Internet of Medical Things (IoMT) devices has created new challenges in protecting sensitive healthcare data and critical medical operations from cyber threats. This section analyzes the detection techniques employed in Intrusion Detection Systems (IDS) to safeguard IoMT networks. The analysis explores three fundamental approaches: signature-based detection, anomaly-based detection, and hybrid approaches, examining how each technique contributes to identifying and preventing cyber-attacks while ensuring the continuous and secure operation of medical devices and healthcare networks.

a. Signature-based IDS Detection

The evolution of healthcare cybersecurity has placed signature-based Intrusion Detection Systems (IDS) at the forefront of protecting sensitive medical networks. Through their comprehensive analysis, Asad et al. [19] demonstrate how these systems excel at identifying known attack patterns, highlighting how diverse signature databases work together to create a robust defense shield for healthcare networks. This becomes particularly crucial as medical facilities increasingly rely on interconnected devices for patient care.

Building on this foundation, Negi and Kumar (2024) [20] showcase recent advancements in signature-based detection specifically tailored for healthcare environments. Their research reveals how modern signature-based systems effectively balance security requirements with the practical limitations of medical devices, ensuring that life-critical healthcare operations remain both secure and efficient

b. Pattern Matching

The increasing complexity of cyber threats in healthcare environments has highlighted the vital importance of pattern matching techniques within signature-based Intrusion Detection Systems (IDS) for IoMT security. Mejía-Granda et al. [16] demonstrate how pattern matching mechanisms serve as the first line of defense in protecting medical device communications, successfully

identifying unauthorized access attempts and protocol violations with a remarkable accuracy rate for known attack patterns. This high level of accuracy becomes particularly significant when considering the findings of Bhushan et al. [20], who reveal how carefully designed pattern matching algorithms can effectively safeguard medical device traffic by meticulously comparing network packets against an established database of known attack signatures.

While pattern matching shows promising results in protecting healthcare data integrity, its implementation presents both opportunities and challenges. Nemec Zlatolas et al. [21] highlight the technique's ability to identify suspicious patterns in real-time while maintaining minimal false positives, a crucial factor in ensuring uninterrupted healthcare operations. However, as Alghamdi and Bellaiche [22] thoughtfully point out, the effectiveness of pattern matching heavily depends on regular signature updates to combat evolving cyber threats in IoMT environments. Their research emphasizes the importance of integrating pattern matching with complementary detection techniques to create a more comprehensive defense system, particularly as healthcare networks face increasingly sophisticated cyber challenges

c. Rule-based Detection

The landscape of healthcare security has witnessed significant evolution in rule-based detection systems, particularly in their approach to protecting IoMT environments. Mustafa et al. [23] reveals the remarkable potential of combining case-based reasoning with rule-based systems, achieving an impressive accuracy rate in medical diagnostics. This breakthrough in healthcare security is further enhanced by innovative neural network-based rule models that bring much-needed clarity to healthcare decision-making, especially when security teams need to understand and justify detection alerts [24]. These advancements demonstrate how carefully crafted rules, informed by medical expertise, can create a robust security framework without compromising healthcare operations.

The ongoing challenge of protecting diverse medical devices has spurred creative solutions in rule optimization and maintenance. A groundbreaking study by Pritika et al. [25] introduces a hybrid fuzzy logic approach that achieves an exceptional detection accuracy across various IoMT devices while maintaining the flexibility needed in dynamic healthcare environments. This achievement resonates with findings from a comprehensive hybrid framework study [26],which shows how combining optimized rule-based systems with deep learning can dramatically improve threat detection while minimizing disruptive false alarms. These developments highlight the healthcare sector's success in adapting security measures to meet its unique challenges while maintaining robust protection against evolving cyber threats.

d. Anomaly-based IDS Detection

Anomaly-based Intrusion Detection Systems (IDS) play a crucial role in securing the Internet of Medical Things (IoMT) by identifying unusual patterns and deviations from normal behavior. Tabassum et al. [27], explore the use of machine learning techniques, such as Support Vector Machines (SVM) and Random Forests (RF), for anomaly detection in IoMT. These models are trained on historical data to learn the normal behavior of the system and detect any deviations from it. Deep learning approaches, particularly

autoencoders and Long Short-Term Memory (LSTM) networks, have also shown promising results in improving detection accuracy and reducing false positive rates [28]. Balhareth and Ilyas [3] propose an optimized intrusion detection system for IoMT networks using tree-based machine learning algorithms, such as Decision Trees and Random Forests, combined with filter-based feature selection methods to improve the efficiency and effectiveness of the detection process. Despite the advancements in anomaly-based IDS for IoMT, challenges still exist, such as the need for large amounts of labeled data for training and the potential for high false positive rates due to the dynamic nature of IoMT environments.

e. Statistical Anomaly Detection

Anomaly-based Intrusion Detection Systems (IDS) play a vital role in securing the Internet of Medical Things (IoMT) by identifying unusual patterns and deviations from normal behavior. These systems rely on various statistical models, such as Gaussian Distribution, Markov Models, Time Series Analysis, Chi-Square Test, and Correlation Analysis, to capture normal behavior patterns and detect anomalies based on deviations from these patterns [29] [30]. Building accurate profiles of normal behavior is crucial for effective anomaly-based IDS in IoMT, which involves selecting relevant features, applying data preprocessing techniques, and using machine learning algorithms like Support Vector Machines (SVM) and Artificial Neural Networks (ANN) to learn and model normal behavior profiles from historical data [29] [30] [31].

Determining appropriate thresholds for anomaly detection is essential to balance detection accuracy and false positive rates. Statistical measures, such as p-value and significance level, are used to set thresholds that determine the boundary between normal and anomalous behavior [29] [30]. Cross-validation techniques and receiver operating characteristic (ROC) curves are employed to optimize threshold values for maximizing detection accuracy while minimizing false positives [31]. Achieving high detection accuracy and low false positive rates is a significant challenge in anomaly-based IDS for IoMT, and the performance is evaluated using metrics such as precision, recall, and F1-score [29] [30] [31].

The choice of statistical technique depends on the specific characteristics of the data and the nature of the anomalies to be detected. Gaussian Distribution and Threshold-Based Detection are suitable for point anomalies, while Time Series Analysis and Markov Models are better suited for contextual and collective anomalies. Chi-Square Test and Correlation Analysis are useful for detecting anomalies in multivariate data. The effectiveness of these techniques also depends on the quality and representativeness of the training data used to build the normal behavior profiles [29] [30] [31].

f. Machine Learning Anomaly Detection

Machine Learning (ML) anomaly-based Intrusion Detection Systems (IDS) have become pivotal in securing Internet of Medical Things (IoMT) networks against cyber-attacks. These systems utilize ML algorithms to identify deviations from normal network behavior, effectively detecting previously unknown threats. For instance, a study by Ghaida Balhareth and Mohammad Ilyas (2024) [3] proposed an optimized IDS for IoMT networks, employing tree-based machine learning classifiers combined with advanced feature

selection methods to enhance detection accuracy and minimize false alarm rates [3].

Similarly, Jamshed Ali Shaikh et al. (2024) [32] introduced RCLNet, an anomaly-based IDS for IoMT, integrating Convolutional Neural Networks and Long Short-Term Memory models with a Self-Adaptive Attention Layer Mechanism. This approach demonstrated significant improvements in the security and confidentiality of patient data within IoMT healthcare systems.

Furthermore, Georgios Zachos et al. (2021) [33]proposed an efficient and effective anomaly-based IDS for IoMT networks, leveraging host-based and network-based techniques to reliably collect log files and traffic data. They utilized machine learning algorithms to detect abnormalities and identify malicious incidents in the IoMT network [34].

These studies underscore the critical role of ML anomaly-based IDS in enhancing the security of IoMT networks, offering innovative solutions to detect and mitigate cyber threats effectively. The integration of advanced ML techniques, such as deep learning models and feature selection methods, has proven effective in improving detection accuracy and reducing false positives. However, challenges remain, including the need for large, labeled datasets for training, the computational complexity of advanced models, and the necessity for real-time processing capabilities to ensure timely threat detection. Addressing these challenges is essential for the development of robust IDS solutions that can effectively safeguard IoMT networks against evolving cyber threats.

g. Deep Learning Anomaly Detection

Deep learning has emerged as a powerful approach for anomaly-based Intrusion Detection Systems (IDS) in the Internet of Medical Things (IoMT). Alghamdi and Bellaiche (2023) propose an ensemble deep learning-based IDS using a combination of Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and AutoEncoders (AE) to capture different aspects of network traffic and improve detection accuracy [22]. Bhavsar et al. (2023) [35] explore various deep learning architectures, such as Deep Neural Networks (DNN), CNN, and Recurrent Neural Networks (RNN), to model the normal behavior of IoT devices and detect anomalies [35].

Alsoufi et al. (2021) [36] conduct a systematic literature review on anomaly-based IDS in IoT using deep learning, categorizing existing approaches based on techniques like AE, Deep Belief Networks (DBN), and Generative Adversarial Networks (GAN) [36]. The review highlights the effectiveness of deep learning in detecting novel and sophisticated attacks but also identifies challenges related to the scarcity of labeled IoT security datasets and the computational complexity of deep learning models.

[32] presents a deep learning-based anomaly detection framework for IoMT security, leveraging unsupervised learning (AE and DBN) to learn normal behavior and supervised learning (CNN and LSTM) to classify detected anomalies. Alalhareth and Hong (2024) [37] propose a meta-learning approach for enhancing the performance of ensemble IDS in IoMT, dynamically selecting and combining multiple deep learning models

based on their performance on different attack types and network conditions [37].

[38] presents a deep learning-driven anomaly detection system for IoMT-based smart healthcare systems, utilizing a hierarchical architecture combining CNN and LSTM layers to capture spatial and temporal dependencies in IoMT data. The system achieves high detection accuracy and low processing overhead, enabling real-time anomaly detection in resource-constrained IoMT environments.

The reviewed literature highlights the potential of deep learning in enhancing the detection accuracy and adaptability of anomaly-based IDS in IoMT. However, challenges related to the availability of representative training datasets, the computational complexity of deep learning models, and the real-time processing requirements of IoMT environments remain to be addressed.

IV. HYBRID-BASED DETECTION APPROACHES

a. Integration Approaches

Hybrid-based Intrusion Detection Systems (IDS) for IoMT leverage a combination of signature-based and anomaly-based detection methods to address the limitations of standalone approaches. Signature-based methods excel at identifying known attacks by matching patterns with pre-defined signatures, while anomaly-based methods detect deviations from normal behavior, making them effective against zero-day attacks. For instance, RCLNet integrates Random Forest for feature selection with Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models to capture spatial and temporal patterns in IoMT data, achieving a remarkable accuracy of 99.78% [32]. Multi-layer detection frameworks, such as those combining CNNs and LSTMs, enhance the ability to identify complex attack patterns by analyzing both sequential and grid-structured data [39]. Fusion techniques, like weighted decision-making and alert correlation, further improve detection performance by combining outputs from multiple detection layers, ensuring a robust defense against diverse cyber threats *[40]*.

b. Decision Making Process

The decision-making process in hybrid IDS involves sequential and parallel processing to optimize detection efficiency. Sequential processing allows for step-by-step analysis, where initial detection layers filter out benign traffic, reducing the computational load on subsequent layers. Parallel processing, on the other hand, enables simultaneous analysis of multiple data streams, improving response times. Weighted decision-making assigns varying importance to different detection outputs, ensuring that critical alerts are prioritized. For example, SafetyMed employs a unique classification algorithm that dynamically adjusts detection thresholds based on the trade-off between detection rates and false positives, enhancing decision accuracy [39]. Alert correlation techniques aggregate and analyze alerts from multiple sources, reducing false positives and providing a comprehensive view of potential threats *[40]*.

c. Performance Analysis

Hybrid IDS systems are evaluated based on detection accuracy, false alarm rates, processing overhead, resource usage, and response time. Advanced models like RCLNet achieve high accuracy (99.78%) and low false alarm rates by leveraging focal loss to handle imbalanced datasets [32]. However, processing overhead remains a

challenge, especially in resource-constrained IoMT environments. Techniques such as feature selection and lightweight algorithms help mitigate this issue. For instance, optimized tree-based models like Random Forest and XGBoost demonstrate high accuracy (99.82%) with minimal detection times (0.02–0.15 seconds) [3]. Response time is critical in healthcare settings, where delays can compromise patient safety, making real-time detection capabilities a key performance metric [41].

d. Implementation Aspects

The implementation of hybrid IDS in IoMT requires careful consideration of architecture design, integration complexity, resource requirements, and deployment strategies. Distributed architectures, such as fog-to-cloud computing, enable efficient data processing by distributing detection tasks across local fog nodes and centralized cloud servers. This approach reduces latency and enhances scalability, as demonstrated by a fog-based IDS that achieved a 37.07% reduction in execution time compared to centralized methods [41]. Integration complexity is addressed through modular designs that allow for the seamless incorporation of new detection techniques. Resource requirements are minimized by employing lightweight algorithms and optimizing feature selection, ensuring compatibility with IoMT devices [3].

e. IoMT-Specific Considerations

Hybrid IDS solutions for IoMT must address healthcare-specific challenges, including real-time requirements, device constraints, and protocol support. Real-time detection is crucial for ensuring timely responses to cyber threats, as delays can have life-threatening consequences in healthcare settings. Device constraints, such as limited computational power and memory, necessitate the use of lightweight algorithms and efficient data processing techniques. For example, federated learning-based IDS models train locally on IoMT devices, preserving data privacy while minimizing resource usage [42]. Protocol support is another critical consideration, as IoMT networks rely on diverse communication protocols that must be seamlessly integrated into the IDS framework. Solutions like SafetyMed are designed to handle sequential and grid-structured data, ensuring compatibility with IoMT-specific protocols [39].

V. Ensemble Machine Learning Algorithms

Ensemble learning has emerged as a critical approach in enhancing the security of the Internet of Medical Things (IoMT), leveraging the combination of multiple machine learning models to improve predictive accuracy and robustness. Its importance lies in addressing the dynamic and heterogeneous nature of IoMT environments, where traditional security measures often fall short due to the complexity of interconnected medical devices and evolving cyber threats. Current applications include intrusion detection systems (IDS) that utilize ensemble techniques like stacking, bagging, and boosting to detect anomalies and cyberattacks in real-time, ensuring the confidentiality and integrity of sensitive patient data [37]. However, major challenges persist, such as the resource constraints of IoMT devices, the need for lightweight and efficient algorithms, and the difficulty in maintaining low false positive rates while ensuring high detection accuracy [43] [44].

a. Algorithm Types

Ensemble learning methods are diverse, each offering unique advantages for IoMT security.

Bagging, or Bootstrap Aggregating, is a widely used technique that reduces overfitting and variance by training multiple models on different subsets of the data and averaging their predictions. A prime example is the Random Forest algorithm, which constructs numerous decision-trees and aggregates their outputs to improve stability and accuracy. Random Forest is *particularly* effective in IoMT security due to its ability to handle high-dimensional data and its inherent resistance to overfitting [37] [45].

Boosting methods, on the other hand, focus on improving model performance by sequentially correcting errors. Algorithms like AdaBoost (Adaptive Boosting) and Gradient Boosting assign higher weights to misclassified instances, allowing subsequent models to learn from past mistakes. This iterative approach makes boosting highly effective for detecting rare or subtle attack patterns in IoMT systems. For instance, Gradient Boosting has been shown to achieve high precision in identifying zero-day attacks, which are particularly challenging in healthcare environments [37] [45].

Stacking takes a different approach by combining the predictions of multiple base models using a meta-learner. This method leverages the strengths of diverse algorithms, such as decision trees, support vector machines, and neural networks, to create a more robust and accurate final model. Stacking is particularly useful in IoMT security, where the complexity of data and the variety of attack types require a multifaceted approach. Additionally, voting mechanisms, such as majority or weighted voting, provide a simpler yet effective way to aggregate predictions from multiple models. These techniques are often used in real-time IoMT applications where computational efficiency is critical [37] [45].

b. Feature Engineering:

Feature engineering is pivotal in IoMT security, involving selection methods like Intriguing Group Teaching Optimization (IGTO) to identify relevant features and reduce dimensionality. Data preprocessing steps, including normalization, transformation, and handling missing values, ensure that the input data is clean and balanced, which is essential for effective model training. IoMT-specific considerations include handling heterogeneous data from medical devices, addressing data imbalance, and ensuring compliance with healthcare regulations like HIPAA. For example, preprocessing techniques like Synthetic Minority Over-sampling Technique (SMOTE) can be used to balance datasets, improving the detection of rare but critical cyber threats. [43] [44] [46].

VI. PERFORMANCE AND IMPLEMENTATION

Ensemble learning models have demonstrated exceptional performance in IoMT security, with studies reporting accuracy rates exceeding 98% in some cases. Metrics such as precision, recall, and F1-score are commonly used to evaluate these models, with boosting and stacking techniques often achieving the highest scores. However, reducing false alarm rates remains a significant challenge, as high false positives can lead to alarm fatigue among healthcare professionals. Processing efficiency is another critical factor, with lightweight ensemble models like bagging and stacking being preferred for real-time applications.

For instance, Random Forest has been shown to strike a balance between accuracy and computational efficiency, making it a popular choice for IoMT security al [37] [46].

Integrating ensemble learning into IoMT systems requires careful consideration of resource requirements, as many medical devices have limited computational power and memory. To address this, researchers are developing lightweight models that can operate on edge devices, ensuring real-time threat detection without compromising performance. Healthcare adaptations include tailoring algorithms to handle the unique characteristics of medical data, such as its high variability and sensitivity. Frameworks like the Kappa Architecture enable continuous data processing, making them suitable for IoMT environments where delays can have serious consequences. Additionally, real-time capabilities are essential for timely threat detection, with ensemble methods like stacking and voting being particularly effective in this regard [44] [46].

VII. COMPARATIVE ANALYSIS

Comparative studies have consistently shown that ensemble learning methods outperform single-model approaches in IoMT security. For example, stacking and boosting techniques often achieve the highest accuracy and lowest false positive rates, making them ideal for detecting sophisticated cyber threats. However, implementation complexity varies, with stacking requiring more computational resources and expertise compared to bagging or boosting. The strengths of ensemble methods include improved generalization, robustness, and the ability to handle complex and heterogeneous data. On the other hand, limitations such as scalability challenges and the need for extensive hyperparameter tuning must be addressed [37] .

Looking ahead, future directions in ensemble learning for IoMT security include integrating meta-learning for adaptive decision-making, leveraging federated learning to preserve data privacy, and developing lightweight models for resource-constrained devices. These advancements will be critical in addressing the evolving challenges of IoMT security and ensuring the safe and efficient operation of healthcare systems [37] .

The analysis of various detection techniques reveals distinct characteristics and performance metrics for each approach in IoMT environments. Table X presents a comprehensive comparison of five key detection techniques: Signature-Based, Anomaly-Based, Hybrid, ML-Based, and Ensemble Learning approaches. Each technique demonstrates unique strengths and limitations, with accuracy rates ranging from 98% to 99.78%. While Signature-Based detection excels in identifying known attacks with up to 99% accuracy, Anomaly-Based detection achieves the highest accuracy rate of 99.78% in detecting novel threats. The ML-Based and Ensemble Learning approaches offer balanced solutions, with accuracies of 99.5% and 98.47% respectively, particularly suitable for real-time and adaptive threat detection in IoMT environments. as shown in Table (1)

Table (1): Comprehensive Comparison of Detection Techniques for IDS in IoMT

Detection Technique	Mechanism	Strengths	Weaknesses	Accuracy	Key Applications
Signature-Based	Predefined patterns and signatures	High accuracy for known threats	Ineffective against zero-day attacks	Up to 99%	DDoS and malware detection
Anomaly-Based	Behavioral deviation analysis (RCLNet)	Detects novel and zero-day attacks	High false positives; computationally intensive	Up to 99.78%	Zero-day attack detection
Hybrid	Combined signature and anomaly (SafetyMed)	Balanced detection with low false positives	Complex implementation; high maintenance	Up to 98%	Comprehensive threat detection
ML-Based	Tree-based models (RF, XGBoost)	High accuracy and adaptability	Requires large datasets; adversarial vulnerabilities	Up to 99.5%	Real-time threat detection
Ensemble Learning	Multiple ML model combination	Enhanced robustness and generalization	High computational overhead	Up to 98.47%	Adaptive threat detection

VIII. CONCLUSION AND FUTURE WORK

This comprehensive review underscores the critical importance of intrusion detection systems (IDS) in safeguarding the Internet of Medical Things (IoMT) from evolving cyber threats. The analysis reveals a concerning escalation in the impact and sophistication of major attack types, emphasizing the urgent need for advanced detection mechanisms tailored to IoMT environments.

A comparative examination of signature-based, anomaly-based, and hybrid detection techniques highlights their unique strengths and limitations. While signature-based methods excel in identifying known attacks, anomaly-based approaches, particularly those leveraging machine learning and deep learning algorithms, demonstrate superior performance in detecting novel and sophisticated threats. Hybrid models, combining the benefits of both approaches, emerge as promising solutions for IoMT security.

Ensemble learning methods, such as bagging, boosting, and stacking, consistently outperform single-model approaches in terms of accuracy, robustness, and adaptability. However, challenges related to resource constraints, real-time processing requirements, and the need for lightweight algorithms must be addressed to ensure their practical implementation in IoMT systems.

Future research directions should focus on developing efficient and scalable IDS solutions that can operate effectively on resource-constrained IoMT devices. The integration of advanced techniques, such as meta-learning, federated learning, and lightweight models, holds promise for enhancing the security and privacy of sensitive healthcare data.

Moreover, the development of standardized datasets and evaluation frameworks specific to IoMT security is crucial for facilitating meaningful comparisons and advancements in the field. Collaborative efforts between healthcare providers,

device manufacturers, and cybersecurity experts are essential to create comprehensive and representative datasets that capture the unique characteristics of IoMT environments.

REFERENCE

[1] A. Naghib, F. Gharehchopogh and A. Zamanifar, "A Comprehensive and Systematic Literature Review on Intrusion Detection Systems in the internet of Medical Things: current status, Challenges, and opportuniters," Artif Intell, vol. 58, no. 114, 2025.

[2] S. Ahmed and F. Qamar, "Satellite based IoT Networks unsing high performance computing architecture," Scientific Reports, vol. 14, no. 1, 2024.

[3] G. Balhareth and M. Ilyas, "Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection," Sensors, vol. 24, 2024.

[4] J. Abigail, G. J. W. Kathrine, S. Silas and A. Jeyabose, "Efficient Deep Learning-Based Cyber-Attack Detetion for Internet of Medical Things Devices," Sci. Rep, vol. 14, 2024.

[5] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramirez-Gutierrez and C. Feregrino-Uribe, "Artificial Intelligence for IoMT Secuirty: A review of Intrusion Detection Systems, Attacks, Datasets and Cloud-Fog-Edge Architectures,," Internet of Things, vol. 23, p. 33, 2023.

[6] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, pp. 45-67, 2019.

[7] R. Doriguzzi-Corin and D. Siracusa, "FLAD: Adaptive Federated Learning for DDoS Attack Detection," Computer & Secuirty , 2024.

[8] S. F. Ahmed, M. Sahib Bin Alam, S. Afrin, S. J. Rafa, N. Rafa and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," Information Fusion, vol. 102, 2024.

[9] S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras and N. Doulamis, "Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review," Computer in Biology and Medicine, vol. 170, 2024.

[10] M. Iddrisu, K. Takyi, R.-M. Mensah, K. Peasah and L. Banning, "An improved man-in-the-middle (MITM) attack detections using convolutional neural networks," Multidisciplinary Science Journal, vol. 7, 2024.

[11] M. Alqhtani, D. Alghazzawi and S. Alarifi, "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," Journal of Cybersecurity and Privacy, 2022.

[12] A. Jatain and M. Narang, "A Study on Cyber-Attack Detection in IoMT using Machine Learning Techniques," Social Science Research Network, 2023.

[13] A. A. Alharbi, "Federated Transfer Learning for Attack Detection for Internet of Medical Things," International Journal of

Information Security, vol. 23, no. 1, pp. 81-100, 2024.

[14] H. Sahu, N. K. Joshi and S. V. Chande, "Design of Secure IoMT Networks using a Federated Learning Approach," Springer, Singapore, p. 1075, 2024.

[15] G. Dupont, D. dos Santos, S. Dashevskyi, S. Vijayakumar, . S. P. Murali, E. Costante, J. den Hartog and S. Etalle, "Demonstration of new attacks on three healthcare network protocols in a lab environment," Journal of Comput Virology and Hacking Techniques, vol. 20, 2024.

[16] C. M. Mejia-Granda, J. L. Frenandes-Aleman, J. M. Carrillo-de-Gea and J. A. Carcia-Berna, "Security vulnerabilities in healthcare: an analysis of medical devices and software," Medical & Biological engineering & Computing, vol. 62, 2023.

[17] D. C. Munoz and A. d. C. Valiente, "A novel botnet attack detection for IoT networks based on communication graphs.," Cybersecurity., vol. 6, 2023.

[18] S. Almeghlef, A. Al-Gamdi, M. Ramzan and M. Ragab, "Appliction Layer-Bsed Denial-of-Service Attcks Detection against IoT-CoAP," Electronics, vol. 12, 2023.

[19] H. Asad, S. Adhikari and I. Gashi, ". A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems.," International Journal of Information Security, vol. 23, pp. 1331-1346, 2024.

[20] B. Bhushan, A. Kumar, A. K. Agarwal, P. Bhattacharya and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," Sustainability, vol. 15, 2023.

[21] L. N. Zlatolas, T. Welzer and L. Lhotska, "Data breaches in healthcare: security mechanisms for attack mitigation," Cluster Computing, vol. 27, pp. 8639-8654, 2024.

[22] R. Alghamdi and M. Bellaiche, "An ensemble deep learning based IDS for IoT using Lambda architecture," Cybersecurity, vol. 6, 2023.

[23] E. M. Mustafa, M. M. Saad and L. W. Rizkallah, "Building an enhanced case-based reasoning and rule-based systems for medical diagnosis," Journal of Engineering and Applied Science, vol. 70, 2023.

[24] A. Benamira and T. P. Guerand, "A New Interpretable Neural Network-Based Rule Model," Cornell University, 2023.

[25] Pritika, B. Shanmugam and S. Azam, "Risk Evaluation and Attack Detection in Heterogeneous IoMT Devices Using Hybrid Fuzzy Logic Analytical Approach," Sensors, vol. 24, no. 10, 2024.

[26] M. A. Kumaar, D. Samiayya, D. R. Vincent and K. Srinivasan, "A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning," Frontiers in Public Health, vol. 9, 2022.

[27] M. Tabassum, S. Mahmoud, A. Bukhari, B. Alshemaimri, A. Daud and F. Khalique, "Anomaly-based threat detection in smart health using machine learning," BMC Medical Informatics and Desision Making, vol. 24, 2024.

[28] A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro and A. Alnajim, "Deep Learning-Driven Anomaly Detection for IoMT-Based Smart," Computer Modeling in Engineering & Sciences, vol. 141, 2024.

[29] K. Elleithy, S. Bell, B. Plaag and D. Stone, "Implementation and Comparison of a Rules-Based Approach and a Statistical Approach Intrusion Detection Systems," in 2nd International Information and Telecommunication, Technologies Symposium., Florianópolis, Brazil, 2003.

[30] A. Dehlaghi-Ghadim, M. H. Moghadam, A. Balador and H. Hansson, "Anomaly Detection Dataset for Industrial Control System," IEEE Access, 2023.

[31] N. Belhadj Aissa and M. Guerroumi, "Semi-supervised Statistical Approach for Network Anomaly Detection," Procedia Computer Science., vol. 83, 2016.

[32] J. A. Shaikh, C. Wang, W. U. S. Muhammed, M. Arshad, M. Owais, R. O. Alnashwan, S. A. Chelloug and M. S. A. Muthanna, "RCLNet: an effective anomaly-based intrusion detection for securing the IoMT system," Front Digit Health, vol. 6, 2024.

[33] G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro and J. Rodriguez, "An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks," Electronics, vol. 10, 2021.

[34] M. Bhavsar, K. Roy, J. Kelly and et al., "Anomaly-Based Intrusion Detection system for IoT application," Discov. Internet Things, vol. 3, 2023.

[35] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb , F. Saeed and M. Nasser, "Anomaly-Based Intrusion Detection Systems in IoT using Deep Learning: A Systematic Literature Review," Appl. Sci., vol. 11, 2021.

[36] M. Alalhareth and S. C. Hong, "Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems," Sensors, vol. 24, 2024.

[37] A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro and A. Alnajim, "Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems," Comput. Model. Eng. Sci., vol. 141, 2024.

[38] N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. K. M. Azad, S. A. Alyami, P. Lio, M. A. Kabir and M. A. Moni, "SafetyMed: A novel IoMT Intrusion Detection System using CNN-LSTM Hybridization," Elextronics, vol. 12, 2023.

[39] S. Kushal, B. Shanmugam, J. Sundaram and et al., "Self-healing hybrid instrusion detection system: an ensemble machine learning approach," Discov. Artif. Intell., vol. 4, 2024.

[40] D. Mohamed and O. Ismael, "Enhancement of an IoT Hybrid Intrusion Detection System based on fog-to-cloud computing," J. Cloud Comput., vol. 12, 2023.

[41] K. Begum, M. A. I. Mozumder, M. I. Joo and H. C. Kim, "BFLIDS: Blockchain-driven federated learning for intrusion detection in IoMT networks," Sensors, vol. 24,

2024.

[42] A. Manoharan and M. Thathan, "Enhanced IoMT Security Framework Using Group Teaching Optimized Probabilistic Deep Auto-Encoder (GTPDA)," Sci. Rep., vol. 14, 2024.

[43] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub and M. Ilyas, "Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Enviroments," Sensors, vol. 25, 2025.

[44] T. Alsolami, B. Alsharif and M. Ilyas, "Enhanced Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet if Medical Things," Sensors, vol. 24, 2024.

[45] M. A. Arasi, H. N. AlEisa and A. A. Alneil, "Artificial Intelligence-driven ensemble deep learning models for smart monitoring of indoor activities in IoT environment for people with disabilities," Sci. Rep. , vol. 15, 2025.