AI

MDPI

Review

Navigating the Cyber Threat Landscape: An In-Depth Analysis of Attack Detection within IoT Ecosystems

Samar AboulEla [1], Nourhan Ibrahim [1,2], Sarama Shehmir [1], Aman Yadav [1] and Rasha Kashef [1,*]

[1] Electrical, Computer, and Biomedical Engineering, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada; samar.g.aboulela@torontomu.ca (S.A.); nourhan.ibrahim@torontomu.ca (N.I.); sarama.shehmir@torontomu.ca (S.S.); aman.yadav@torontomu.ca (A.Y.)
[2] Faculty of Engineering, Alexandria University, Alexandria 5424041, Egypt
* Correspondence: rkashef@torontomu.ca

Abstract: The Internet of Things (IoT) is seeing significant growth, as the quantity of interconnected devices in communication networks is on the rise. The increased connectivity of devices has heightened their susceptibility to hackers, underscoring the need to safeguard IoT devices. This research investigates cybersecurity in the context of the Internet of Medical Things (IoMT), which encompasses the cybersecurity mechanisms used for various healthcare devices connected to the system. This study seeks to provide a concise overview of several artificial intelligence (AI)-based methodologies and techniques, as well as examining the associated solution approaches used in cybersecurity for healthcare systems. The analyzed methodologies are further categorized into four groups: machine learning (ML) techniques, deep learning (DL) techniques, a combination of ML and DL techniques, Transformer-based techniques, and other state-of-the-art techniques, including graph-based methods and blockchain methods. In addition, this article presents a detailed description of the benchmark datasets that are recommended for use in intrusion detection systems (IDS) for both IoT and IoMT networks. Moreover, a detailed description of the primary evaluation metrics used in the analysis of the discussed models is provided. Ultimately, this study thoroughly examines and analyzes the features and practicality of several cybersecurity models, while also emphasizing recent research directions.

Keywords: cybersecurity; cyberattacks; intrusion detection; Transformers; deep learning (DL); machine learning (ML); Internet of Things (IoT)

Citation: AboulEla, S.; Ibrahim, N.; Shehmir, S.; Yadav, A.; Kashef, R. Navigating the Cyber Threat Landscape: An In-Depth Analysis of Attack Detection within IoT Ecosystems. *AI* **2024**, *5*, 704–732. https://doi.org/10.3390/ai5020037

Academic Editor: Arslan Munir

Received: 16 April 2024
Revised: 12 May 2024
Accepted: 13 May 2024
Published: 15 May 2024

1. Introduction

Nowadays, the Internet of Things (IoT) is experiencing significant growth. With advanced technology, the number of connected devices in communications systems is increasing [1] as the interconnected devices become more vulnerable to cyberattacks [2]. To safeguard sensitive data and uphold device integrity, securing IoT devices is crucial. The applications of IoT technologies cover various fields, such as smart healthcare systems and connected vehicles.

The cybersecurity of the Internet of Medical Things (IoMT) is the focus of this work. In IoMT environments, various healthcare-related devices are connected. These devices include wearable health devices such as smart inhalers and medical sensors, implantable medical devices such as insulin pumps and pacemakers, digital health records, smart beds, monitoring systems, and medical lab equipment. Regulatory agencies such as the Food and Drug Administration (FDA) participate in medical device security by enforcing rigorous certification processes for medical device manufacturers, including cybersecurity checks. Securing medical devices is essential for many reasons. Ensuring the safety of patients and protecting their health records are primary goals. Moreover, it is essential to prevent the malicious use of medical devices and secure healthcare systems' infrastructure. Network attacks on the IoMT pose high risks to patient well-being, information confidentiality,

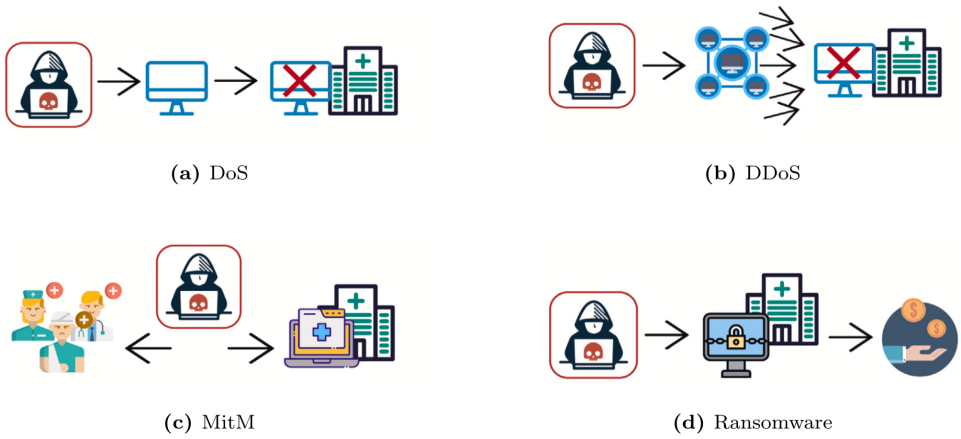
and the overall reliability of healthcare services. Cyberattacks can endanger patients' lives and disrupt hospital operations [3].

One well-known attack in the medical field is the "WannaCry" ransomware. This attack compromised 230,000 devices in the UK in 2017 [3,4]. The attack infected computers in 150 countries and resulted in substantial financial losses [4]. Another popular attack occurred in Germany in 2000 [3,5]. The attack compromised 30 servers, and the hospital had to redirect many emergency patients [5].

Ayoub et al. [6] classified IoMT attacks into three categories. The first category represents attacks at the level of data collection. Data modification is an example of an attack in this category. The second category is transmission-level attacks. Denial of Service (DoS), spoofing, and Man-In-The-Middle (MITM) attacks fall within this category. The third category comprises attacks targeting the storage level, with examples including malware and social engineering attacks.

This section briefly elaborates on sample types of IoMT attacks. In data modification attacks, the attacker aims to tamper with the data, which compromises their integrity. An attacker tries to impersonate real users in a spoofing attack, which violates the authenticity aspect of security. Social engineering attacks are also very common nowadays. Attackers attempt to trick victims into sharing personal information. This violates data confidentiality because the system's sensitive data can be revealed. DoS attacks occur when the system becomes overwhelmed by network traffic so that the service may be unreachable or slow. The system's availability is affected by DoS attacks. Distributed Denial of Service (DDoS) attacks involve multiple sources overwhelming a system with traffic, which also results in unavailability, as in DoS attacks. In MITM attacks, the attacker can intercept communication channels within the network. This attack can compromise the confidentiality aspect if the attacker steals the data. It can also affect the integrity of the data, if the attacker modifies them before forwarding them to the recipient. A malware, or malicious software, attack is a common cyberattack that executes unauthorized actions on the victim's system. Viruses and worms are examples of malware attacks. The attacker aims to corrupt or steal the data (integrity violation). The intruder can also illicitly access the system (violating the confidentiality rule). Ransomware is a type of malware that encrypts data and demands a ransom for their release, compromising data availability and potentially confidentiality if the data are sensitive. Figure 1 illustrates examples of the mentioned security threats [1].

After discussing the various network attacks, this paper explores state-of-the-art directions to address these threats. The subsequent subsection summarizes related surveys within the field of cybersecurity.



(a) DoS **(b)** DDoS **(c)** MitM **(d)** Ransomware

Figure 1. Examples of security threats [1].

1.1. Related Surveys

The emerging importance of cybersecurity in safeguarding the IoT network has led researchers to focus on implementing machine learning (ML) and deep learning (DL)

techniques to enhance the methods for the detection of cyberattacks in IoT networks. This subsection presents a summary of the recent surveys in the field.

Alyazia et al. [7] reviewed recent studies focusing on cybersecurity intrusion detection systems (IDS) in IoT networks. Many DL techniques for attack detection within an IoT network were investigated. The methods include deep belief networks (DBN), autoencoders (AE), and generative adversarial networks (GANs). Additionally, long short-term memory (LSTM) networks, neural network synthesis (NNS), graph neural networks (GNNs), and deep neural networks (DNN) are examples of the discussed DL techniques. Moreover, the authors explored the use of hybrid DL models to enhance the detection accuracy. Recurrent neural networks (RNNs) based on LSTM, RNNs combined with convolutional neural networks (CNNs), and LSTM are examples of the hybrid DL techniques explored. A detailed description of the publicly available benchmark datasets recommended for IDS in IoT networks was given. The authors explained the most important evaluation metrics used to assess the surveyed DL models. Finally, the key challenges facing cybersecurity in IoT networks were summarized, including the requirement of labeled datasets for IoT networks and the real-time model deployment issues.

Due to the IoT's technological advancements, cybersecurity is vital in various fields, like smart grids, vehicle communication systems, smart cities, and healthcare applications. The authors in [8] provided an overview of the current state of cybersecurity, the challenges faced, and the future research directions. This review addressed emerging cybersecurity techniques like artificial intelligence (AI) and machine learning (ML) for the detection of cyber threats and to automate their responses. Sophisticated cyberattacks utilizing methods such as multi-vector attacks, polymorphic and fileless malware, zero-day exploits, advanced persistent attacks, and AI-driven attacks are challenges facing the cybersecurity domain. The progress in AI has led to significant advancements in cybersecurity. However, it has also enabled a breakthrough in the development of cyberattacks, resulting in artificial intelligence-based attacks such as botnet attacks. Moreover, the growing reliance on cloud services has led to the emergence of evolving threat types. The new threats include data breaches, unauthorized access, insecure application programming interfaces, and shared infrastructures. These attacks pose high security risks. They can also result in data loss or the disruption of services. Finally, the authors pointed out future research directions in cybersecurity, including quantum computing, biometric authentication, advanced AI, and ML models.

The work in [9] thoroughly examined the integration of databases and DL technologies in cybersecurity, specifically intrusion detection systems (IDS). This review paper examined benchmark cybersecurity datasets, describing the steps involved in data collection, the features, and the attack types found in these datasets. Moreover, the authors explored various DL techniques, including DBN, AE, CNNs, LSTMs, and GANs. They investigated their applications in different domains, such as malware detection, phishing detection, and network intrusion detection, assessing their advantages and disadvantages. Furthermore, the survey identified a potential research gap in the current studies: the present features in the available benchmark datasets are insufficient in obtaining high attack detection rates as cyberattacks evolve.

The objective of the review paper in [10] was to comprehensively summarize the relevant literature in the field related to the use of AI in cybersecurity for IoT networks. The authors examined various attack types: initial reconnaissance, physical attacks, MITM attacks, false data injection, botnets, and DoS attacks. They also discussed methods of attacking IoT networks: the device's hardware and software, the connected network, and the interfacing application. Additionally, the paper explored the AI field, examining AI-based models used for cyberattack detection, including decision trees (DT), K-nearest neighbors (KNN), support vector machines (SVMs), and artificial neural networks (ANNs). Attackers can utilize AI techniques to attack the IoT network. They can also manipulate AI cybersecurity models to work against their systems. During AI model training, the authors

investigated attacks involving input manipulation, data poisoning, and false data injection. This included dataset poisoning, model poisoning, and algorithm poisoning.

1.2. Paper Contributions

Many research papers focus on the field of cybersecurity, specifically exploring the integration of artificial intelligence (AI) methods. Nevertheless, there is a scarcity of research papers that specifically focus on AI-driven cybersecurity for ecosystems. The primary emphasis of this research study is healthcare systems in IoT contexts. An extensive survey was conducted on cutting-edge artificial intelligence (AI) methods to safeguard healthcare systems from cyber threats. The paper furthermore offers an elaborate depiction of the benchmark datasets for both IoT and IoMT systems. The survey presents a classification system that is based on artificial intelligence approaches and offers security solutions specifically designed for the healthcare industry. The evaluation metrics used to analyze these techniques are then described. Finally, the paper examines the areas of study that have not been addressed in healthcare cybersecurity and provides suggestions for future directions.

1.3. Paper Organization

The rest of the paper is structured as follows. Section 2 shows the methodology used in this survey. Section 3 is dedicated to presenting the related work. The methodology, including the analytical models, the cybersecurity datasets, and the performance metrics, is described in Section 4. Section 6 presents the conclusions.

2. Survey Methodology

This section outlines the methodology that was used in conducting this survey. The main objective was to enhance the security of IoMT systems in order to protect them from cyberattacks. The research analyzed relevant scholarly articles on the cybersecurity of IoMT systems that use artificial intelligence (AI) techniques. The articles included were published during the last four years, up to the year 2023. The original research questions are presented in Table 1. The first phase of data collection included searching several academic databases, including Google Scholar, Scopus, and IEEE Xplore, using specific keywords like "cybersecurity", "IoMT", "healthcare", "ecosystems", "artificial intelligence", "machine learning", and "deep learning" to identify relevant publications. The collected data were then examined and refined to determine their relevance to the survey's purpose. The filtering procedure consisted of three steps, first based on the title, followed by an evaluation of the abstract and the conclusion. Ultimately, the filtration process was conducted according to the scholarly contributions. Figure 2 depicts the technique that has been used for the proposed review. In summary, this study examined a total of 33 research studies and 4 survey papers. The pie chart in Figure 3 illustrates the distribution of articles chosen from various types of journals. The bar chart in Figure 4 displays the publication years of the works considered in this study.

Table 1. Proposed research questions.

RQ	Research Question
1	What is the current status of IoMT cybersecurity in the recent literature?
2	What are the cyberattacks targeting the cybersecurity of the IoMT systems?
3	What are the most common techniques used recently in addressing the cybersecurity of IoMT systems?
4	How can AI be incorporated in addressing the cybersecurity problems in IoMT systems?
5	What are the benchmark datasets used for the AI modeling of IoMT systems?
6	What are the evaluation metrics used to evaluate the current models in the literature?
7	What are the research gaps and future directions in safeguarding IoMT systems?

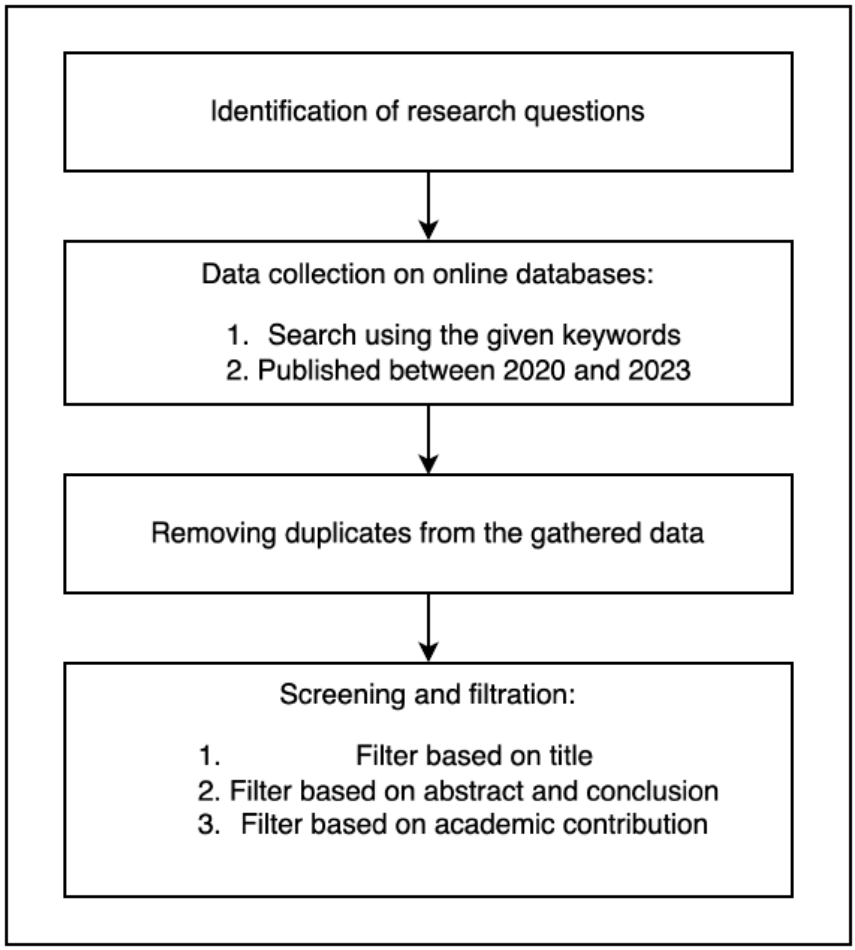


Figure 2. Survey methodology.

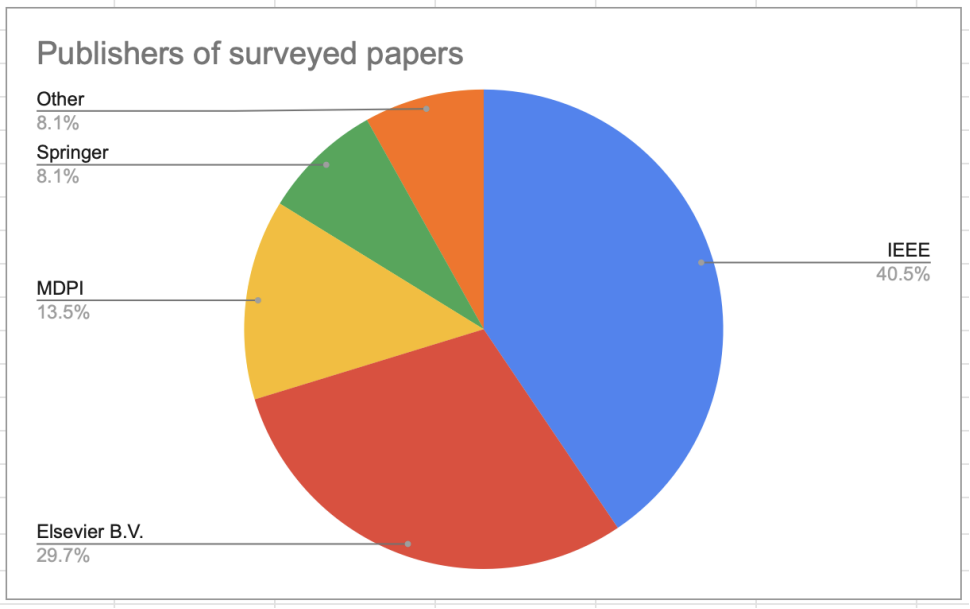


Figure 3. Representation of surveyed papers.

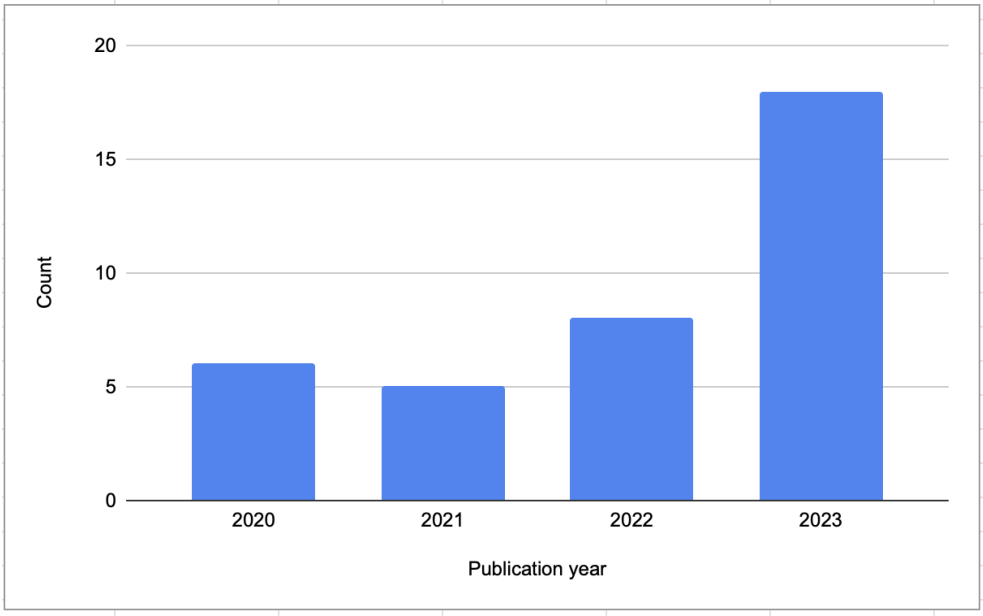


Figure 4. Representation of publication years of surveyed papers.

3. Related Work

In this section, the related work is categorized into ML-based methods, DL-based models, combined ML and DL approaches, Transformer-based approaches, and others, as discussed in the following sections.

3.1. Machine Learning Methods

In [11], the authors produced a novel healthcare IoT dataset (WUSTL-EHMS) [12]) for an enhanced healthcare monitoring system. The database contains 28 features related to network traffic data and eight biometric characteristic features. For intrusion detection, four machine learning algorithms were evaluated: random forest (RF), KNN, SVM, and ANN. The best results (lowest prediction time and highest area under the curve) were achieved using the ANN model. The experiments confirmed the positive impact of combining network features with features gathered from patients' biometrics. The authors planned to enhance their work by tuning the model's hyperparameters and improving the data quality using feature engineering. One possible limitation of the work in [11] is the assumption that the data collected using medical sensors are transmitted in plain text to avoid high processing power.

The work in [13] addressed three main challenges: designing a distributed security framework, ensuring security while dealing with big data, and designing a robust anomaly-based IDS. The proposed IDS [13] uses a fog cloud architecture and ensemble learning. The first-level learners in the model are decision trees (DT), Naive Bayes (NB), and RF. Using stacking, the output of the ML classifiers is input to XGBoost to determine the final classification of the system. The model was investigated using the ToN-IoT database. The reported evaluation metrics were the accuracy, precision, detection rate, false alarm rate, and F1 score.

The model has the following strengths: it is simple, it relies on few parameters, and it can be updated in real time. A possible limitation of this approach is that it tackles only binary classification. The authors planned to extend their work so that it could detect different network attacks. Another future direction that they mentioned was to adopt various techniques in the feature selection stage.

In the framework of the IoMT, the paper [14] tackles the crucial cybersecurity problem. The authors aimed to create efficient techniques for the identification and cessation of cyberattacks in IoMT environments. The study used the WUSTL-EHMS 2020 dataset, which includes biometric and network information. Data cleaning and feature selection were

the two preparatory procedures the authors used. Several performance metrics, including the accuracy, precision, recall, F1 score, and mean-squared error loss, were employed to evaluate the ML models. The RF method produced accuracy of 96.9% and achieved values above 96% in terms of precision, recall, and F1 score. Gradient boosting (GB) produced comparable outcomes in terms of precision, recall, and F1 score, with accuracy of 96.5%. The SVM's accuracy was 95.85% compared to the other two models, but its precision, recall, and F1 score were marginally lower. The recommended machine learning models were evaluated against the current methods in this research. It was seen that the suggested random forest and GB models performed better than the conventional techniques. In contrast, the SVM model produced results that were competitive with those of earlier research.

The research in [15] presented an investigation into creating an ML intrusion detection system (IDS) for the IoMT. The authors examined several ensemble learning strategies, such as GB, extreme GB, bagging, RF, and ensemble voting classifiers. These ensemble approaches enhance intrusion detection by combining the predictions of several models. For every classification model, the hyperparameters were optimized to guarantee optimal performance. By selecting critical features for intrusion detection, the authors carried out feature selection. Considerations included the source and destination IP bytes, protocol, connection state, etc. The AdaBoost (ADB) classifier outperformed the other examined classification models regarding all performance measures. It recorded the lowest false discovery rate (FDR), F1 score, accuracy, and precision. Two current models (Model 1 and Model 2) were compared to the proposed ADB-based IDS for the IoMT. The proposed model performed better than the other compared models in terms of the false positive rate (FPR), FDR, accuracy, and precision.

To provide an efficient and effective security solution while considering the limitations of Internet of Medical Things (IoMT) networks, one work [16] offered an anomaly intrusion detection system (AIDS) explicitly designed for IoMT networks. The authors provided an all-inclusive AIDS framework for IoMT networks that included modules for dataset generation, feature normalization, data collection, and central detection, using ML methods to detect intrusions. The network's core gateway was the target of data gathering, which included disc and Wi-Fi bandwidth utilization, CPU and memory utilization, and energy consumption data. It also contained network data, such as the protocol details, packet sizes, and source and destination IP addresses. CSV datasets containing gateway-, network-, and device-specific sets were created from the processed data. By balancing the feature values, feature normalization prevented dominance problems. The central detection module used machine learning methods to find irregularities and intrusions in the IoMT network. Regarding binary classification tasks, DT, RF, and KNN performed better than other popular machine learning methods. They demonstrated great recall, accuracy, precision, and F1 score, which qualified them for IoMT intrusion detection. Future work, including the installation of hardware prototypes, multi-class support, hyperparameter optimization, and the investigation of deep learning for cloud-based solutions, was also outlined in the study.

The authors in [17] addressed the challenge of the lack of openly accessible datasets on the Internet of Healthcare Things (IoHT). They contributed by designing the ECUIoHT database, thus encouraging more researchers to develop robust models for IoHT security. The authors launched different types of network attacks, such as network mapper (Nmap), address resolution protocol (ARP) spoofing, DoS, and smurf attacks. Numerous anomaly detection methods were investigated, with six variations of nearest neighbor algorithms, three clustering algorithms, two statistical-based methods, and one kernel-based algorithm. Specifically, the list of tested techniques included KNN, the approximate local correlation integral (aLOCI), the local outlier probability (LoOP), influenced outlierness (INFLO), the cluster-based local outlier factor (CBLOF), and the clustering-based multi-variate Gaussian outlier score (CMGOS). Additionally, the list included the local density cluster-based outlier factor (LDCOF), robust principal component analysis (RPCA), and the histogram-based

outlier score (HBOS). Lastly, the one-class support vector machine (LIBSVM) method was also evaluated. Possible limitations for the work in [17] included the following. The class imbalance problem was not addressed. At the same time, it was clear from the distribution of benign versus attack instances that some attacks represented minority classes compared to normal network traffic. In addition, the DoS attacks appeared to be artificial and could not be detected with good performance (as was noticed from the F1 score bar graph in [17]). Moreover, each attack type was tested independently (i.e., the system used binary, anomaly-based detection). In other words, the authors used four different subsets of the data and tackled a single type of attack in each test.

In [18], the authors' approach showed effectiveness in reducing cyberattacks compared to other machine learning approaches. A framework using algorithms for task scheduling using blockchain and a combination of deep reinforcement learning was developed to enhance the performance of healthcare applications in a distributed IoMT environment. The proposed framework utilized a temporal LSTM deep neural network for disease detection and anticipation. The Bayesian optimization algorithm was used to optimize the parameters of an EML-based model for IoT security attack detection. The proposed approach showed superior precision, recall, F1 score, and receiver operating characteristic–area under the curve (ROC-AUC) performance compared to other approaches. The suggested approach was found to achieve better performance overall, with a 32 percent time complexity reduction and a 15 percent increase in current accuracy values when evaluated against several ML methods, such as LR, RF, Naive Bayes, decision trees, extreme machine learning, and ensemble learning approaches, such as extreme machine learning with genetic algorithms and EML with RS. These resulted in the successful classification and prediction of attacks in the Internet of Medical Things environment. EML works for some patterns but may not be suitable for large, nonlinear datasets. Deep learning neural networks are recommended for untrained features.

Wazid et al. [19] reported the effectiveness of a new model, EID-HS—Envisioned Intrusion Detection in Industry 5.0-driven Healthcare Applications—which ensembles SVM, DT, and KNN with custom weights to detect new malware using traffic analysis on a large-scale network. Industry 5.0 healthcare systems focus on delivering personalized products for patients given their unique needs. This study demonstrated that ensemble deep learning yields promising results in such systems. The EIDHS system was robust against cyberattacks and was shown to outperform existing approaches. The experimental results on the NSL-KDD dataset, with 81,161 intrusion instances, indicated accuracy of 95.12%.

Recent studies exploring machine learning methods for cybersecurity within IoT and IoMT environments have shown notable advancements but have also revealed several key areas in need of enhancement. In the study conducted by Hady et al. [11], a novel dataset integrating both biometric and network features was introduced. However, the research assumed that data collected from medical sensors are transmitted in plain text, potentially compromising the data security. This assumption reveals a critical need for more robust data handling protocols that enhance the security without overwhelming the processing capabilities. Moreover, Kumar et al. [13] utilized a fog cloud architecture and ensemble learning, primarily handling binary classification. This approach may be inadequate against more complex, multi-class cyber threats, which are becoming increasingly common in modern networks. This limitation suggests a need for models capable of efficiently differentiating among a broader array of attack vectors. Additionally, the study by Tauqeer et al. [14] aimed to address sophisticated cyberattacks in IoMT settings. However, the effectiveness of these machine learning models could be limited by the current approaches to data preprocessing and feature selection. This indicates the potential for improvements in feature engineering techniques to better capture and utilize the nuances of cybersecurity data.

To address these identified challenges, the following enhancements could be beneficial. First, for research like that of Hady et al. [11], integrating advanced encryption methods during data transmission could significantly mitigate the risk of security breaches. Employing

lightweight cryptographic algorithms might provide an optimal balance between security and operational efficiency. Second, in response to the gaps identified in Kumar et al.'s work [13], it is crucial to develop machine learning models capable of effective multi-class classification. Incorporating sophisticated algorithms could improve the system's ability to manage diverse cyber threats. Third, to augment the performance of the models discussed in Tauqeer et al.'s study [14], implementing more advanced feature engineering methods, including automated feature learning through deep learning techniques, could enhance both the accuracy and detection capabilities. Finally, integrating federated learning could enhance the scalability and robustness of intrusion detection systems by allowing multiple decentralized devices to train models collaboratively, without compromising data privacy.

Table 2 compares cutting-edge IDS techniques, including the methodologies, classification types, datasets, evaluation measures, and constraints. Table 2 lists the ML-based approaches. The table provides useful information and aids in identifying research gaps, which will drive future research into network intrusion detection systems.

Table 2. A summary of ML-based methods for cyberattack detection.

Model	Classification Type	Dataset	Evaluation Metrics	Limitations
RF, KNN, SVM, ANN [11]	Binary	WUSTL-EHMS	Accuracy, area under the ROC curve (AUC), average training time, average prediction time	Medical sensor data are transmitted in plain text
Fog computing, ensemble learning [DT, NB, RF] + XGBoost [13]	Binary	ToN-IoT	Precision, F1 score, false alarm rate, detection rate, and accuracy	—
RF, GB, SVM [14]	Binary	WUSTL EHMS 2020	Accuracy, precision, recall, F1 score, loss (mean-squared error—MSE)	Lack of generalization of the proposed models to real-world IoMT environments
MNB, LR, LRSGD, LSVC, EVC [15]	Not mentioned	ToN-IoT	F1 score, accuracy, precision, recall, false positive and false discovery rates	Lacks detailed information about the dataset's source, size, and characteristics
LR, RF, DT, NB, KNN, and SVM [16]	Binary	Custom dataset	Accuracy, precision, F1 score, recall	Limited dataset
LOF, COF, aLOCI, LoOP, INFLO, CBLOF, CMGOS, LDCOF, RPCA, HBOS, LIBSVM, and KNN [17]	Binary	ECU-IoHT	True positive, false positive, F1 score	Class imbalance was not considered so the method could not detect the minority class (DoS attack)
EML and Bayesian optimization [18]	Binary	ToN-IoT	Recall, precision, ROC-AUC, F1-, F2-, and F-beta scores	Privacy and security issues in dynamic cloud/fog systems with lots of devices
EID-HS [19]	Binary	NSL-KDD	Accuracy	—

3.2. Deep Learning Methods

Marwa et al. [20] presented a recent anomaly detection technique built on deep learning and deep clustering. The paper addressed two main challenges, namely feature randomness and feature drift. The first challenge, feature randomness, occurs when training a neural network encoder without a decoder, based on hypothetical similarities. This method may result in the encoder producing features that do not accurately represent the distinguishing characteristics of the data. On the other hand, feature drift arises when combining clustering and reconstruction objectives in the use of autoencoders. Clustering aims to simplify data by removing unimportant details, whereas reconstruction strives to preserve all information. Consequently, feature drift occurs when there is a failure to balance these conflicting objectives. The proposed algorithm utilized the concept of deep

subclass dispersion within a one-class support vector machine (deep SDOSVM). The main steps of the algorithm were feature mapping, feature selection, clustering using a dynamic autoencoder (DynAE), feature normalization, subclass matrix calculation, model training, model testing, and a performance assessment. The authors used performance metrics such as the false positive rate, true positive rate, number of support vectors (SVs), ROC curve, AUC, probability values (p-values), and training time. For future work, the authors planned to implement an incremental IDS to overcome the batch learning model limitation. The upgraded version should effectively manage sequential and large-scale datasets, while learning using the limited available data samples.

The study in [21] introduced an ensemble deep learning technique for the classification of network attacks. The authors built a robust generative adversarial network based on ensemble convolutional neural networks (GANsECNN). The model was used to generate synthetic data for each type of network attack. Experiments were performed using two publicly available datasets, the NSL-KDD and the UNSWNB15 datasets. The performance was measured using the following metrics: accuracy, precision, recall, and generator and discriminator loss. The experiments indicated that the suggested method could enhance multi-class classification by around 10% using the generated samples. The proposed method presented a stable architecture, and the model converged rapidly. However, the reported results were not superior to related results from experiments on the same datasets.

A new deep learning method was adopted in [22] to apply to medical cyber-physical systems. The authors proposed a federated learning (FL) architecture that utilized generative adversarial networks (GANs). The GAN models were trained on two categories of data: medical and network traffic data. The CHARIS [23,24] clinical dataset and the UNSW-NB15 dataset were used for medical anomaly detection and network traffic data detection, respectively. Data modification and scrambling attacks were launched on the medical data. At the same time, the algorithm detected several types of attack on the network traffic, including backdoors, Denial of Service attacks, shellcodes, and worms. Five performance metrics were reported: accuracy, recall, precision, F1 score, and AUC. The authors concluded that the federated models achieved better results than non-federated models. However, the results were not very high for network flow anomaly detection. For example, the F1 scores were 0.77 and 0.78 for non-federated versus federated network flow models. As part of their future work to enhance their model, the authors planned to augment a range of deep learning methods with privacy prevention policies.

Intrusion detection using a cloud-based model was introduced in [25]. The authors implemented a hierarchical federated learning (HFL) algorithm. In contrast, the proposed hierarchical long short-term memory (HLSTM) model was used to distinguish between health records and detect intrusions in the incoming network traffic. The proposed model was reported to require minimal training while safeguarding IoMT networks against various network attacks. The IDS was tested using the TON-IoT and NSL-KDD datasets. Various metrics, including the accuracy, precision, recall, and F1 score, were utilized to assess the model's performance. The experimental outcomes demonstrated the effectiveness of the proposed model. The authors suggested including the Gurobi optimization solver for future extensions to optimize the performance. In addition, they planned to explore how the model performed concerning heterogeneity, interoperability, and scalability [25].

Two multi-class classification models, namely DenseNet and Inception Time, were proposed in [26]. The models were used to identify cyberattacks on an IoT network. The proposed models were trained on three publicly available benchmark datasets: ToN-IoT, Edge-IIoT, and UNSW2015. The evaluation measures used were the accuracy, recall, precision, and F1 score. The DenseNet model achieved a remarkable 99.9% accuracy for the ToN-IoT dataset. However, when using the Inception Time architecture, the results reached a perfect 100% accuracy. In the case of the Edge-IIoT dataset with the Inception Time architecture deployed, the accuracy reached 94.94%.

The necessity of an IDS in the IoMT is emphasized in the paper [27], seeking to identify and alert administrators to potentially dangerous activity. Federated learning (FL), a method

of fitting machine learning models across distributed platforms without the need for data exchange, was introduced in this work. The authors described how their suggested model, which used deep neural network (DNN) methods, operated. The model was composed of a global model disseminated to local edge devices after being trained on a source domain. Using local datasets for training, the local models' expertise was fed back into the global model without jeopardizing the integrity of the local datasets. This procedure enabled rapid, safe, customized intrusion detection on edge devices. The learning method, including layer freezing and CORAL loss minimization, was described in the study. This procedure aimed to enhance the model performance with each local dataset and fine tune the global model. The model demonstrated greater accuracy compared to classic machine learning and deep learning techniques, underscoring its efficacy in intrusion detection. It maintained realistic prediction times for real-time detection on edge devices without regular connectivity to cloud servers.

In recent years, the use of DNNs for the detection of cyberattacks in IoT networks has been on the rise. However, this technique for cyberattack detection brings challenges, as it is computationally complex to apply and vulnerable to adversarial samples. The study in [28] aimed to address these challenges by enhancing the accuracy of DNN models while reducing the computational complexity, especially in resource-constrained environments. The fully connected neural network (FCNN) model was presented in the paper as the baseline model for cyberattack detection. The authors then proposed a performance enhancement technique that integrated pruning, simulated micro-batching, and parameter optimization to handle the computational complexity problems of the DNN models.

By integrating the proposed optimization method into the baseline model, the authors proposed a refined model, namely Robust Effective and Resource-Efficient DNN (REDNN). Three publicly available benchmark datasets—N-BaIoT, Kitsune, and WUSTL—were used to test the performance of the newly suggested model. The robustness of the proposed model was also presented. The robustness was tested against various factors, including the number of epochs, clipped perturbation samples, and model variations. The efficiency of the REDNN model was then compared against that of the baseline model and state-of-the-art techniques. The REDNN model, as proposed, exhibited robustness against adversarial attacks and achieved an unconventionally high level of accuracy in detecting cyberattacks within IoT networks. It also demonstrated the significant conservation of resources. Notably, the suggested model demonstrated considerable decreases in memory and time utilization compared to the benchmark in simulated virtual worker environments. Additionally, its effectiveness was demonstrated in a federated learning (FL) setting, highlighting its robustness and efficiency in real-world scenarios.

The primary focus of the work in [29] was to reduce the complexity and classification time, which improved the accuracy when using DL-based techniques in a cybersecurity IDS for IoT networks. The authors proposed three different models using various deep learning techniques. The deep learning techniques used for the three models were a feed-forward neural network (FFNN), LSTM, and a random neural network (RandNN). Each model was trained on the CIC IoT 2022 dataset. The proposed framework consisted of five stages. First, features were extracted using CICFlowMeter 4.0. Second, the data preprocessing stage took place, including data cleaning, encoding, and scaling. Then, data balancing, feature selection using principal component analysis (PCA), and data splitting were performed. The proposed models aimed to classify instances into "Normal" or "Attack" for binary classification problems. However, for multi-class problems, the proposed models classified instances as "Normal" or identified their specific attack types. These newly suggested models were then compared with one another and with the traditional ML IDS models and state-of-the-art IDS models. The RandNN model showed promising performance as it could capture complex dependencies. The LSTM model also showed promising performance because it captured the time-based dynamics within IoT data. The newly proposed FFNN model demonstrated enhanced performance compared to the proposed LSTM, the RanDNN, and other ML and DL-based models.

Recent advancements in deep learning methods have significantly improved anomaly detection and cyberattack classification within IoT and IoMT environments. However, several studies highlight persistent research gaps that could hinder their broader application and effectiveness. Notably, Marwa et al. [20] and other subsequent studies reveal issues such as feature randomness and feature drift, where deep learning models struggle to balance data simplification with accurate information preservation. This challenge points to an inherent limitation in the current autoencoder architectures used for cybersecurity purposes. Furthermore, while methods like those proposed by Raha et al. [21] for the generation of synthetic data to train robust models show promise, they often do not outperform existing benchmarks, indicating a gap in the efficacy of such generative approaches. Similarly, the use of federated learning in medical cyber-physical systems, as discussed in Ilias et al. [22], although improving the performance over non-federated models, still shows sub-optimal results in certain key areas like network flow anomaly detection.

To address these gaps, this paper proposes several solutions aimed at enhancing the current state of deep learning techniques in cybersecurity. First, to tackle feature randomness and drift, an advanced deep learning architecture that integrates enhanced regularization techniques could be developed. This would involve sophisticated training regimes that more effectively capture the nuances of cybersecurity data, thereby producing features that better represent the underlying patterns without oversimplification. Second, to improve the performance of generative adversarial networks in cybersecurity, it is essential to integrate novel adversarial training frameworks that can generate more diverse and challenging synthetic datasets. This approach will ensure that the models are not only robust against known types of attacks but are also prepared for zero-day exploits. Lastly, the application of federated learning models in cybersecurity could be enhanced by incorporating multimodal learning strategies that leverage both structured and unstructured data from various IoT devices. This method would help in better understanding the context of the data, thus improving the detection accuracy of network anomalies. Additionally, exploring advanced optimization algorithms could significantly reduce the computational overhead, making these models feasible for deployment in resource-constrained environments.

Table 3 summarizes the DL-based methods mentioned in this section.

Table 3. A summary of DL-based methods for cyberattack detection.

Model	Classification Type	Dataset	Evaluation Metrics	Limitations
Deep SDOSVM [20]	Binary	ToN-IoT	False positive rate, true positive rate, ROC, AUC, *p*-values, number of SVs, training time	Batch learning model
GAN-ECNN [21]	Multi-class	NSL-KDD, UNSW-NB15	Accuracy, precision, sensitivity, F1 score	The reported results were not superior to those of other related work
FL, GAN [22]	Binary	CHARIS, UNSW-NB15	Accuracy, recall, precision, F1 score, AUC	Results for network flow data were not promising
Dew-cloud-based HFL-HLSTM [25]	Binary and multi-class	ToN-IoT, NSL-KDD	Accuracy, precision, recall, F1 score	Hierarchical model results in increased latency. Delays should be minimized in real-time scenarios
DenseNet, Inception Time [26]	Multi-class	ToN-IoT, Edge-IIoT, UNSW2015	Accuracy, precision, recall, F1 score	Partial dataset
DNN [27]	Binary and multi-class	CICIDS2017	Accuracy, detection rate, average training time, average prediction time	Long training time

Table 3. *Cont.*

Model	Classification Type	Dataset	Evaluation Metrics	Limitations
REDNN [28]	Binary	N-BaIoT, Kitsune, WUSTL IIOT 2018	Memory saving, test accuracy, train time, train mem, test set acc, test time, test mem	No improvements in accuracy compared to other related work
FFNN, LSTM, RandNN [29]	Binary and multi-class	CIC IoT 2022	Accuracy, precision, recall, F1 score	It could be time-consuming

3.3. Combined Machine Learning and Deep Learning Methods

The primary goal of the study in [30] was to develop an effective IDS to safeguard IoMT networks against cyberattacks. The author highlighted the growing significance of the IoMT in healthcare, but he also drew attention to the vulnerabilities brought about by medical devices' interconnectedness. The paper recommended using a fog cloud architecture to solve the security concerns related to the IoMT. The ensemble learning technique used by the suggested IDS system integrates several long short-term memory (LSTM) networks. The author presented a deployment methodology that offers Infrastructure as a Service (IaaS) in the cloud and Software as a Service (SaaS) in the fog. The paper also covered several data preprocessing methods, such as feature mapping, data imputation, and feature selection, to prepare the dataset for intrusion detection. Learning curves and misclassification errors were used to assess the performance of the proposed technique, which demonstrated that the ensemble approach performed much better than a decision tree. The ROC curve was used to evaluate the classifier's performance; the AUC showed that the proposed method performed better than the baseline. The work in [31] aimed to provide a reliable approach for the detection of anomalies and attacks in IoMT devices used in healthcare. The study used four real IoMT datasets gathered from actual healthcare devices: WUSTL-EHMS, TON-IoT, ICU, and ECU-IoHT. The suggested approach used machine learning techniques to perform multiple phases of dataset cleaning, feature selection, feature extraction, and classification. The study used the recursive feature elimination (RFE) technique to choose the most crucial characteristics. The first method used was the KNN classifier. Then, a multi-layer perceptron (MLP) classifier with hyperparameters adjusted was employed to improve the classification. The efficacy of the suggested approach in identifying abnormalities and cyberattacks was demonstrated by its excellent accuracy rates across all IoMT datasets. Better performance was obtained by combining the hyperparameter-tuned MLP with XGBRegressor-based feature selection. The authors intended to set up an IoMT laboratory to improve the attack detection accuracy and investigate potential new research avenues.

The work in [32] focused on intrusion detection in the context of the IoMT, recognizing two forms of attacks: data spoofing and data alteration. The primary goal was to develop an effective intrusion detection model to secure healthcare systems that handle sensitive information. The study used a range of assessment metrics to assess the intrusion detection model's performance. These measures included the ROC-AUC and the following: prediction time, F1 score, accuracy, precision, false acceptance rate (FAR), and recall (detection rate). To improve the precision and effectiveness of intrusion detection, the suggested model combined several machine learning methods, feature scaling strategies, data augmentation, and class weight ratios. Noteworthy average testing accuracy of 94.23%, indicating the model's superiority over an existing method, was one of the most important findings. The model's efficiency was mainly ascribed to the shorter prediction times attained in feature, algorithm, and data preparation selection. However, there were also acknowledged drawbacks, such as the model's narrow focus on only two types of attacks and its assessment in a simulated network context. In further research, the author suggested including more attack types to create a more comprehensive intrusion detection model, looking at deep learning models with minimum complexity to increase the AUC and detection rates.

In [33], network traffic and patient biometric data were combined into a dataset using an ARGUS tool to improve intrusion detection in the IoMT. There were 44 features in the dataset, comprising 9 biometric features and 35 network traffic features. The dataset was initially composed of 2046 attack samples and 14,272 normal samples. When attacks were infrequent, 1400 attack samples were chosen at random to replicate real-time networks. A CNN, DNN, and LSTM were utilized for intrusion detection. AdaBoost performed the best among all machine learning models, with accuracy of 91.6%. All ML models displayed high recall, F1 score, and precision. The DNN achieved maximum accuracy of 96%, surpassing both the CNN and LSTM in performance. The precision, recall, and F1 score of the DL models were consistently good. However, the DNN obtained the best overall accuracy. The suggested particle swarm optimization deep neural network (PSO-DNN) algorithm achieved accuracy of 96%, which was 3.2% better than that in previous studies, outperforming cutting-edge techniques. To improve IoMT attack categorization in the future, the author proposed integrating particle swarm optimization (PSO) for feature selection and DNNs for intrusion detection.

Developing a strong IDS to safeguard sensitive medical data against attacks and breaches was the main goal of the paper [34]. The authors used a Kaggle intrusion detection dataset that is globally benchmarked and covers a variety of attack methods along with typical network behavior. PCA was used as a dimensionality reduction approach to solve the dataset's high dimensionality problem. By reducing the number of attributes, this strategy increased the efficiency. The Grey Wolf Optimization (GWO) method makes this research distinctive. After PCA, GWO was employed as a second-level optimization method. GWO aids in further dimensionality reduction while maintaining crucial characteristics. The dataset was subjected to various categorization models, such as NB, RF, SVM, KNN, and DNN. These models were designed to be used for intrusion detection. According to the paper's findings, the suggested classifier model regularly performed better than alternative models with respect to sensitivity, specificity, and accuracy. The classification model became more efficient and required less training time as the dimensionality was reduced.

By highlighting the possible dangers and repercussions of security holes or online attacks in these systems, the authors of the paper [35] sought to address the security weaknesses in IoMT contexts. Their primary objective was to create a reliable method of identifying malicious activity in IoMT networks. The authors set up 100 IoT nodes on a fictitious square field using an Intel Xeon system with particular hardware configurations. Throughout the studies, several DDoS assaults were simulated. Wireshark was used to collect data packets. A Python script was developed to extract IoT end-level layer characteristics from packet capture (.pcap) files, which were then transformed into CSV files for analysis. Using a label encoder to transform categorical elements into numerical values and managing missing values are two examples of the data preprocessing steps applied. The authors employed numerous optimization approaches, including Spider Monkey Optimization, Salp Swarm Optimization, Whale Optimization, and a hybrid of Lion and Salp Swarm Optimization (LSSOA). These methods were used to improve the detection of malicious traffic. Several metrics, including the accuracy, precision, recall, F1 score, invalid positive rate (IPR), and invalid negative rate (INR), were used in the research to assess the effectiveness of these optimization strategies. The efficacy of the detection techniques was evaluated using these metrics. The suggested Lion and Salp Swarm Optimization Algorithm (LSSOA), according to the authors, had a recall F1 score of 98.0% and could be applied to a variety of tasks, such as resource allocation, network security, hybrid optimization, the management of numerous variables, and scalability.

This section, with studies on combined machine learning and deep learning methods for cybersecurity in the IoMT, reveals significant advancements and also exposes critical gaps that need to be addressed. In the study by Khan [30], while the fog cloud architecture and the use of LSTM networks indicate a robust approach to safeguard IoMT networks, the research lacks details on the real-world application and scalability of the proposed system. Similarly, Kilincer et al. [31] demonstrate improved classification through machine

learning techniques and feature selection, but the reliance on conventional methods like KNN and MLP might not be sufficient against more sophisticated or evolving cyber threats. Furthermore, Gupta's work [32] points out the limitations of focusing only on two specific types of cyberattacks and conducting assessments in a simulated environment, which might not translate effectively into real-world settings. This highlights a broader issue in the current research: a narrow focus on limited attack types and a lack of comprehensive testing across diverse operational conditions. In addition, the study by Chaganti [33] shows promising results using a CNN, DNN, and LSTM for intrusion detection, with high accuracy rates. However, the best performance is limited to a DNN model, which suggests the need to explore more integrated or hybrid approaches that can leverage the strengths of various machine learning and deep learning models more effectively.

For systems like those proposed by Khan [30], it is critical to extend the testing beyond controlled or simulated environments to real-world applications. This would involve deploying the proposed IDS in actual IoMT settings to observe its performance under real operational pressures and attack scenarios. Considering the limitations in the studies by Kilincer et al. [31] and Chaganti [33], there is a clear need to develop hybrid models that integrate multiple machine learning and deep learning techniques. Such models could utilize the strengths of different algorithms to enhance their detection capabilities, especially for complex and evolving attack vectors. In response to the narrow focus observed in Gupta's study [32], future research should incorporate a wider array of attack types and test the IDS models against a broader spectrum of cyber threats. This would ensure that the IDS is robust and versatile enough to handle various types of cyberattacks. To improve the efficacy of the IDS, as observed across these studies, the implementation of more advanced feature selection techniques such as deep learning-based feature extraction could be explored. Techniques like autoencoders or deep belief networks might offer better feature representation and thus enhance the model's predictive accuracy.

Table 4 summarizes the methods based on both ML and DL discussed in this section.

Table 4. A summary of combined (ML and DL) methods for cyberattack detection.

Model	Classification Type	Dataset	Evaluation Metrics	Limitations
LSTM networks, DT [30]	Binary	ToN-IoT	Accuracy, false alarm rate, detection rate, detection of binary anomalies	Limited detail, dataset not well defined
MLP, KNN, Recursive Feature Elimination (RFE), XGBoost Regressor (XGBRegressor) [31]	Binary and multi-class	ECU-IoHT, ToN-IoT	Precision, recall, accuracy and F1 score	Limited features, time-consuming
LR, DT, RF, Extra Tree Classifier, Artificial Neural Network [32]	Not mentioned	Custom dataset	ROC curve, AUC, accuracy, precision, recall, F1 score	Limited attacks, simulated environment
LR, KNN, Decision Tree, AdaBoost, Random Forest, SVM, Long Short-Term Memory (LSTM) [33]	Binary	Custom dataset	Accuracy, precision, F1 score, recall	Limited scope, scalability
DNN, SVM, KNN, RF, NB [34]	Not mentioned	Custom dataset	Accuracy, recall	Limited experimental details
Lion and Salp Swarm Optimization (LSSOA) [35]	Binary	Custom dataset	Accuracy, precision, F1 score, invalid positive rate (IPR), invalid negative rate (INR)	High computational resource consumption

3.4. Transformer-Based Methods

The author in [3] introduced a framework to enhance the security of medical systems. The author built a hybrid security system consisting of two components. The first compo-

nent of the IoMT system was an intrusion detection system, which aimed to monitor the system for any unauthorized access or breaches. Another element was a malware detection system designed to protect the computers used by medical professionals. The approach used a BERT-based Transformer and a light gradient boosting machine (LightGBM). The recommended method consisted of three main phases, as outlined in [3]. First, the network flow was derived from the recorded activities. Subsequently, the collected data underwent preprocessing. Subsequently, the classification of each network's activity as either benign or an assault was performed using the two machine learning algorithms. The model was assessed using four datasets: ECU-IoHT, ToN-IoT, Edge-IIoTset, and EMBER [36]. The proposed model was found to be capable of detecting many types of assaults, regardless of the specific equipment being targeted. An identified constraint of the model was its intricate deployment process. In addition, a correlation calculation was required to combine the obtained data. In further research, the author intended to include other sophisticated malware families and investigate the use of an analytical approach to merge the system's outcomes and expedite decision-making in the IoMT setting.

A research study [37] was published on a modified Transformer neural network (MTNN) designed for the detection of intrusions in IoT systems. The authors proposed a unique approach to identifying cybersecurity vulnerabilities in IoT devices using the MTNN model. The MTNN model, with its smaller parameter count, utilizes the information gain for feature selection and achieves acceptable accuracy. This makes it suitable for implementation in distributed IoT systems, distinguishing it from RNN and LSTM models. The experimental findings on the Ton-IoT dataset [38] showed large improvements in accuracy, precision, recall, and F1 score. The article examined the use of Transformers in detecting cyberattacks and intrusions in IoT systems and the possibility of using GANs to generate false data injection. The authors further emphasized the need for hyperparameter optimization to enhance the efficacy of Transformer-based models. They suggested using a grid search or Bayesian optimization (BO) as potential approaches. The authors discussed the possibility of using generative adversarial networks and federated learning to improve distributed learning in IoT systems in the future.

The authors in [39] presented a novel method for intrusion detection systems called the robust Transformer-based intrusion detection system (RTIDS). This innovative method significantly improved the classification accuracy compared to many present detection techniques. RTIDS demonstrated superior performance compared to SVMIDS, with an improvement of 4.56%; RNN-IDS, with an improvement of 1.67%; LSTM-IDS, with an improvement of 0.81%; and FNN-IDS, with an improvement of 3.03%. The system's performance was further confirmed by comprehensive assessments conducted on two datasets, namely CICIDS2017 and CIC-DDoS2019. Regarding CICIDS2017, RTIDS exhibited remarkable accuracy of 98.45%, precision of 98.32%, recall of 98.73%, and an F1 score of 98.02%. In the case of the CIC-DDoS2019 dataset, the system achieved accuracy of 98.58%, precision of 98.82%, recall of 98.66%, and an F1 score of 98.45%. The underlying robustness of RTIDS resided in its ability to accurately identify network abnormalities and traffic violations, exceeding the capabilities of traditional and DL-based IDS. Further exploring the architecture of the suggested system, the authors emphasized the importance of self-attention mechanisms and strategic data preparation strategies. The comprehensive examination of a dataset including more than 30 million records highlighted the potential of RTIDS in practical applications. A potential area for future research would be optimizing the effectiveness of the Transformer algorithm used in the intrusion detection system to enhance its speed and better address the consequences of abnormal occurrences. In addition, the authors anticipated that incorporating meta-learning would be a viable approach to address the difficulties presented by few-shot categorization situations.

A recent study [40] developed a new intrusion detection model that combined multi-head attention with bidirectional long short-term memory (BiLSTM). This proposed model employed an embedding layer to transform the intrusion data into a vector format, improving the data representation. The process of embedding converted the initial vectors

into two-dimensional vectors. Using the multi-head attention mechanism enabled the model to focus specifically on crucial characteristics within the vector, improving its interpretability. This method was seamlessly integrated with BiLSTM, which, despite not being intended for time series data, can discern connections between distant characteristics, hence linking various features together for predictive purposes. The research used datasets like KDDCUP99, NSLKDD, and CICIDS2017 for training and testing purposes. Optimal model performance was ensured by using data processing methods such as normalization and one-hot encoding. The SMOTE algorithm, also known as the Synthetic Minority Oversampling Technique, was used to tackle the issue of imbalanced class distributions. When compared to other models, the recommended model demonstrated greater performance in terms of accuracy and F1 score. The researchers highlighted specific constraints, such as the model's inability to precisely detect or report new forms of infiltration. Nevertheless, these invasions might still be categorized for further examination.

The study conducted in [41] showed that an IDS using a hierarchical attention model obtained detection accuracy of 98.76% and a false alarm rate of 1.49% when the timestep was set to 10. Prior research has suggested the use of ML methods for IDS, which include approaches such as feature selection and the utilization of DNNs. The use of the attention mechanism in the model facilitates the capturing of relevant characteristics and offers the potential for advancements in feature selection and parallel computing. The proposed model exhibited commendable performance on the UNSW-NB15 dataset, with accuracy above 98.76% and a false alarm rate below 1.2%. The suggested model demonstrated a 3.05% enhancement in comparison to the BiLSTM model. A total of 82,332 records were used in the investigation. The experts suggested that future research should prioritize categorizing various forms of attacks using the presented approach. The proposed system does not yet have a second-phase detection capability. In [42], the authors proposed an intrusion detection method for IoT networks that utilizes an attention mechanism and a bidirectional gated recurrent unit (BiGRU). The authors tackled the issues of unbalanced datasets and insufficient feature information learning in state-of-the-art DL models. The paper introduced SEW-MBiGD, a hybrid intrusion detection model that integrates the SEW model with a BiGRU fusion neural network and an attention mechanism. The SEW model can detect the characteristics of minority groups within a dataset. Furthermore, the data quality was enhanced using model balancing techniques. The studies conducted on NSL-KDD [43] showed that the SEW model effectively addressed the problem of dataset imbalance. Therefore, the suggested method successfully achieved minority-class learning. In addition, the MBiGD model enhanced its feature acquisition by including multi-head self-attention (MHSA) in the BiGRU. This improvement allowed the model to better evaluate the connections between features and enabled attention to be focused on temporal class information. The SEW-MBiGD model was found to outperform and had superior data comprehension capabilities compared to other models. As an example, it enhanced the precision of the support vector machine (SVM) from 77.7% to 81.2% and resulted in around a 1% improvement for K-nearest neighbors (KNN) and decision trees (DT). The inclusion of the BiGRU model with the MHSA layer resulted in a notable improvement in accuracy, with a 5.3% increase for binary classification and a 4.7% increase for multi-classification. The accuracy was improved by training on a balanced dataset.

In the framework introduced by Abdallah [3], namely a hybrid system combining BERT-based Transformers and LightGBM for intrusion detection and malware prevention, the complexity of deployment and the need for correlation calculations to integrate data streams highlight significant operational challenges. These issues could impede the method's scalability and real-world applicability. The research by Ahmed [37] on a modified Transformer neural network (MTNN) demonstrates improvements in precision and recall using Transformers. However, the reliance on traditional feature selection methods like information gain might limit the model's ability to process more complex or subtle patterns in IoMT environments. Additionally, the use of generative adversarial networks (GANs) to simulate attack scenarios raises questions about the model's performance

against real-world, novel cyber threats. Wu et al.'s study [39], which developed a robust Transformer-based intrusion detection system (RTIDS), shows impressive performance metrics. Nevertheless, the system's focus on known datasets like CICIDS2017 and CIC-DDoS2019 means that it may not fully represent the dynamic nature of cyberattacks in IoMT contexts, suggesting a gap in the adaptability and ongoing learning capabilities of the model. Zhang's approach [40] to integrating multi-head attention with BiLSTM to enhance the data interpretability and predictive accuracy is promising but highlights an ongoing challenge in machine learning-based IDS: the detection of new, previously unreported types of cyber threats. This limitation underscores the need for models that can evolve and adapt to new threats dynamically. Liu's application of a hierarchical attention model [41] demonstrated high accuracy and low false alarm rates, but the research suggests potential overspecialization to specific dataset characteristics, meaning that the model might not generalize well across different IoMT platforms or attack vectors.

For complex systems like the one proposed by Abdallah [3], developing streamlined deployment processes and automated data integration tools could reduce the operational complexity and enhance the scalability. This could involve creating modular frameworks that allow for easier customization and integration into existing IoMT infrastructures. To address the limitations noted in Ahmed's MTNN model [37], incorporating deep learning approaches such as autoencoders or deep belief networks for feature learning could uncover more nuanced data patterns and improve the model's efficacy in detecting sophisticated cyber threats. Regarding adaptive and evolving models, for systems like RTIDS [39], integrating continuous learning mechanisms, such as online learning or reinforcement learning, could allow the system to adapt to new threats dynamically. This would help to maintain high performance even as the attack strategies evolve. Zhang's use of multi-head attention with BiLSTM [40] could be enhanced by hybridizing these models with unsupervised learning techniques to detect anomalies that do not fit any known patterns, thereby improving the system's ability to identify novel threats. Regarding cross-platform validation and testing, ensuring that models like Liu's hierarchical attention system [41] are tested across diverse IoMT environments and against a variety of attack simulations could improve their generalizability and robustness.

Table 5 summarizes the Transformer-based methods discussed in this section.

Table 5. A summary of Transformer-based (DL) methods for cyberattack detection.

Model	Classification Type	Dataset	Evaluation Metrics	Limitations
LightGBM, Transformer [3]	Binary	Edge-IIoTset, ECU-IoHT, ToN-IoT, EMBER dataset	MCC, ROC-AUC, F1 score, recall, accuracy, and precision	Model is complex to deploy
MTNN [37]	Multi-class	ToN-IoT	Recall, precision, accuracy, and F1 score	False data injection performed using GANs
RTIDS [39]	Multi-class	CICIDS2017, CIC-DDoS2019	Precision, recall, accuracy, and F1 score	Refining the Transformer algorithm's efficiency is needed, along with integration of meta-learning to overcome few-shot occurrences
Multi-head attention and BiLSTM [40]	Multi-class	KDD-CUP99, NSL-KDD, and CICIDS2017	Accuracy, F1 score	Cannot accurately identify novel intrusion types
Hierarchical Attention Mechanism [41]	Binary	UNSW-NB15	Accuracy, false alarm rate	Cannot identify misclassified attacks
SEW-MBiGD [42]	Binary	NSL-KDD	F1 score, accuracy, precision, recall	—

3.5. Other Methods

The paper [44] proposed an innovative framework, namely the IoT Security Simulator (IoTSecSim). Graphical security modeling (GSM) was utilized to create IoTSecSim. This framework focuses on modeling IoT networks with diverse IoT devices and various network protocols. It could help researchers to simulate different cyberattacks and cybersecurity defenses in IoT networks. Additionally, the effectiveness of these defenses could be assessed using various security metrics embedded in the software. To evaluate the performance of the software, the authors utilized Botnet malware, such as the Mirai virus, seeking to assess the effectiveness of their framework. Three defense methods were tested to demonstrate the framework's effectiveness: firewall, NIDS, and vulnerability patching. The security generator produced a two-layered hierarchical attack representation model (HARM) to capture malware propagation data. Several security metrics were utilized to assess the computational time for malware infection and its spread across four stages: scanning, accessing, reporting, and installation. Additionally, the authors presented four permutations of attacker behaviors that could impact the spread of malware within a network. The paper provided evidence of the simulator's correctness through a simulation and sensitivity analysis. The suggested software offered versatile and intricate functionalities for the modeling of existing and upcoming cyberattacks targeting IoT networks. Nevertheless, it exhibited certain constraints. IoTSecSim lacked real-time simulation capabilities for packet flows, and the proposed defense methods could not identify anomalies.

The authors in [45] proposed a new edge-directed graph multi-head attention network model (EDGMAT) for NIDS. This contemporary framework applied a multi-head attention transformation mechanism to perform weighted aggregation on nodes and edges. The model used traffic directionality and utilized a graph attention network. The evaluation findings demonstrated that the EDGMAT model performed better in multi-class classification, with higher accuracy, recall, and F1 score than state-of-the-art techniques. The model was assessed using four publicly available NIDS. The model was compared to other methods and showed excellent performance. A limitation of the model is that it uses large amounts of GPU memory and requires a long period of time for training to provide comparable levels of accuracy in intrusion detection.

Rayan et al. [46] proposed a security framework for IoMT devices. The method used machine learning and blockchain technology. The authors used a tri-layered feed-forward neural network (TNN) to classify network traffic into normal traffic or attacks. Anomaly detection was implemented using the TNN, while the blockchain helped to secure the data. The proposed blockchain architecture guaranteed the privacy and integrity of the dataset. For performance evaluation, the ICUDatasetProcessed [47,48] dataset was used. It contains 42 features and around 187K records. The presented performance parameters were the confusion matrix, classification accuracy, precision, recall, and F1 score. The method was found to exhibit superior performance. However, when comparing the approach with other cutting-edge techniques, the dataset used appeared to have certain limitations, because the results for most of the baseline methods approached 99%, so the suggested method could only slightly improve the results.

The exploration of diverse methods in cybersecurity for IoT and IoMT devices, as described in recent studies, unveils several research gaps that require attention for enhanced security solutions. The study by Chee et al. [44] introduces IoTSecSim, a security simulator utilizing graphical security modeling (GSM) to simulate cyberattacks and defenses. Despite its capabilities, the simulator lacks real-time simulation for packet flows, which is critical for dynamic network environments. Additionally, the defense methods proposed do not include anomaly detection, a key component in identifying unforeseen or zero-day attacks. Li's research [45] on the edge-directed graph multi-head attention network model (EDGMAT) for network intrusion detection systems (NIDS) demonstrates superior classification performance. However, the model's strong reliance on GPU memory and extended training times could hinder its practical deployment, especially in resource-constrained environments. Rayan et al. [46] present a novel framework combining machine learning

with blockchain technology to enhance IoMT security. While the blockchain architecture ensures data integrity and privacy, the study reveals a potential overfitting issue or dataset limitations, as indicated by the unusually high performance metrics close to 99 percent for the baseline methods. This raises questions about the robustness and generalizability of the proposed model.

To address the limitations of IoTSecSim noted in Chee et al.'s study [44], incorporating real-time data processing capabilities could significantly enhance its utility. Integrating more advanced real-time simulation engines and developing capabilities to monitor live network traffic could provide more accurate and timely insights into network security vulnerabilities. For the EDGMAT model presented by Li [45], optimizing the model to reduce its dependency on extensive GPU resources and training time is crucial. Techniques such as model pruning, quantization, and efficient training algorithms like federated learning could be explored to improve the efficiency without compromising the model's performance. To strengthen the framework proposed by Rayan et al. [46], conducting extensive validation against a broader set of attacks and in more diverse network environments would be beneficial. Enhancing the dataset's diversity and complexity could help to ascertain the true efficacy of the combined blockchain and machine learning approach and identify any overfitting issues. Given the absence of effective anomaly detection in the IoTSecSim framework, incorporating sophisticated anomaly detection algorithms such as unsupervised learning or semi-supervised learning models could fill this gap. These methods could potentially identify novel attack vectors that are not part of the existing threat models used for training.

By addressing these gaps, future research can significantly enhance the effectiveness of cybersecurity measures in IoT and IoMT environments. Improved real-time simulation capabilities, resource-efficient models, robust validation methods, and sophisticated anomaly detection are pivotal in developing resilient security solutions that can adapt to the evolving landscape of cyber threats.

Table 6 summarizes the other surveyed methods discussed in this section.

Table 6. A summary of other surveyed methods for cyberattack detection.

Model	Category	Classification Type	Dataset	Evaluation Metrics	Limitations
GSM, two-layered HARM model [44]	Graph-based	Not mentioned	Botnet (Mirai malware and its variants)	Security metrics (average time taken to compromise a node, average number of compromised nodes)	Lacks real-time simulation capabilities, the proposed defense methods are unable to identify anomalies
EDGMAT [45]	ML + graph-based	Binary	NIDS, 4 dataset benchmark, ToN-IoT, Bot-IoT	Accuracy, recall, F1 score	High GPU memory usage during training, prolonged training times, challenging to maintain high accuracy
TNN + blockchain [46]	ML + blockchain	Binary and multi-class	ICUDatasetProcessed	Accuracy, precision, recall, F1 score	Dataset limitation

4. Methodology

4.1. Analytical Models

Artificial intelligence (AI) has a subset called machine learning (ML). Its main goal is to create algorithms that enable a program to recognize patterns in data and forecast outcomes based on training. The following approaches have used ML techniques in their

cybersecurity IDS: [11,13–19]. The following research has combined ML algorithms with other methods: [30–35,45,46].

A unique subset of machine learning is deep learning. Deep learning models involve layered architectures, which can learn more complex data patterns. They can be applied to more sophisticated tasks like image processing and natural language processing. The following state-of-the-art works have adopted DL (non-Transformer-based) methods: [20–22,25–29]. The following works have combined DL with ML methods: [30–35].

One class of deep learning models based on the self-attention process is Transformers. They have been recently introduced in the paper "Attention is All You Need" [49]. Transformers have shown encouraging improvements in several domains, including machine translation and natural language processing. The studies [3,37,39–42] have adopted Transformer-based methods in the field of cybersecurity.

Graphical security modeling is an approach that relies on graphical representations to analyze the security aspects of computer systems. It involves creating visual models representing the system's components and their relationships. The visual model helps to identify vulnerabilities in the software. This can assist in implementing robust security strategies in the IoT network. The work in [44,45] considers graph-based approaches.

Blockchain is a technology that relies on cryptographic methods. It allows a group of computers to securely work together in a decentralized fashion. Blockchain resembles a super-secure digital record book that keeps track of data. Its safety is maintained because many computers work together to monitor it. The work in [46] adopts blockchain technology.

4.2. Datasets

The related cybersecurity datasets have been classified into three main categories, with the first category being IoMT datasets. Table 7 contains a description of these medical datasets. Other IoT datasets can be found in Table 8. Other non-IoT datasets used in the surveyed papers are outlined in Table 9.

The WUSTL-EHMS dataset [11,12] was created in 2020. It contains 16k data records, including network flow features and patients' biometric features. It contains Man-In-The-Middle attacks, including spoofing and data injection. The ECU-IoHT dataset [50] contains 111k records. It has a greater variety of cyberattacks on the IoMT, but the number of features is much smaller than those in other IoMT datasets. The ICUDatasetProcessed dataset [47,48] contains 187k records and 42 features. To the best of our knowledge, it can be considered the largest publicly available dataset for the IoMT.

Additionally, seven datasets commonly used in the cybersecurity domain of IoT are identified. The IoT datasets are Ton-IoT [38,51], BoT-IoT [52], CIC IoT 2022 [53,54], N-BaIoT [55], Kitsune [56], WUSTL IIOT 2018 [57], and Edge-IIoT [58]. These datasets contain a wide variety of features and network attacks, as shown in Table 8. Furthermore, other datasets frequently utilized in the security field are listed. These include the UNSW-NB15 [59], CICIDS2017 [60], NSL-KDD [43], CSE-CIC-IDS2018 [61], CHARIS [23,24], and EMBER [36] datasets.

Table 7. IoMT datasets.

Dataset	Number of Records	Number of Features	Types of Attack
WUSTL-EHMS [11,12]	16,318	36 features	Man-In-The-Middle attacks
Ecu-IoHT [50]	111,207	6 features	ARP spoofing, Nmap port scan, smurf attack, DoS attack
ICUDatasetProcessed [47,48]	187,643	42 features	Message Queuing Telemetry Transport (MQTT) DDoS, MQTT flood attack, brute force attack, SlowITE attack

Table 8. IoT datasets.

Dataset	Number of Records	Number of Features	Types of Attack
Ton-IoT [38,51]	41,043	43 features	Brute force passwords, ransomware, injection, MITM, DDoS, and backdoors
BoT-IoT [52]	72,000,000	45 features	DDoS, DoS, keylogging, data exfiltration, OS, and service scans. Based on the protocol in use, DDoS and DoS assaults were more common
CIC IoT 2022 [53,54]	–	48 features	DOS (HTTP, UDP, and TCP flooding), brute force and camera RTSP URL attacks
N-BaIoT [55] (sub-divided)	7,062,606	115	BASHLITE or Mirai attacks
Kitsune [56]	27,170,754	7	Reconnaissance attacks, DoS attacks, and Mirai attacks
WUSTL IIOT 2018 [57]	7,037,983	6	Port scanner, address scan attack, device identification attack, device identification attack (aggressive mode), exploit
Edge-IIoT [58]	20,952,648	1176 (61 are highly correlated)	Attacks using malware, Man-In-The-Middle, injection attacks, DoS, DDoS, and information gathering

Table 9. Other datasets.

Dataset	Number of Records	Number of Features	Types of Attack
UNSW-NB15 [59]	2,540,044	49 features	Analysis, fuzzers, backdoors, DoS, exploits, generic, shellcode, reconnaissance, and worms
CICIDS2017 [60]	2,830,743	77 features	DDoS, web-based, Mirai, spoofing, recon, DoS, and brute force
NSL-KDD [43]	125,973 training, 22,544 testing	41 features	DOS, probing, R2L, and U2R
CSE-CIC-IDS2018 [61]	–	80 features	Brute force attacks, DoS, DDoS, web attacks, infiltration, Botnet attacks, port scanning
CHARIS [23,24]	–	–	Generated attack types in [22]: data modification and data scrambling attacks
EMBER [36]	–	–	–

4.3. Performance Metrics

This section describes the main performance measures applied by the studies surveyed in this work. The performance metrics are summarized in Table 10.

1. **Precision (P)**
   Precision measures a model's accuracy in making positive predictions. Its usage is mainly in binary classification problems, where the goal is to distinguish between two classes as '1' or '0'.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (1)$$

where
true positives (TP) = number of '1's correctly predicted as '1's by the model.
false positives (FP) = number of '0's incorrectly predicted as '1's by the model.
A machine learning model with a greater precision value is more accurate in producing positive predictions and has a lower rate of false positives.

2. **Recall (R)**
A model's recall, also known as sensitivity, quantifies its capacity to accurately identify every real positive among the total number of real positives (true positives + false negatives).

$$\text{Recall (or Sensitivity)} = \frac{\text{TP}}{\text{TP + FN}} \tag{2}$$

where
false negatives (FN) = number of actual '1's incorrectly predicted as '0's by the model.
A high recall value indicates that the ML model correctly recognizes all relevant instances belonging to a certain class, even if it may also generate some incorrect positive identifications. Conversely, poor recall indicates that the model has failed to identify a significant number of true positive instances.

3. **F1 score**
The F1 score may be defined as the mathematical average of the precision and recall, specifically calculated using the harmonic mean. The evaluation approach provides a fair assessment by considering the presence of both false positives and false negatives. The method is used to conduct an intermediate assessment where datasets exhibit imbalances.

$$\text{F1 score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{3}$$

4. **Accuracy**
The accuracy score is a machine learning assessment statistic that estimates the percentage of correct predictions generated by a model compared to the total predictions. It is calculated by dividing the number of accurate predictions by the total number of forecasts.

$$\text{Accuracy} = \frac{\text{TP + TN}}{\text{TP + TN + FP + FN}} \tag{4}$$

where
true negatives (TN) = number of actual '0's correctly predicted as '0's by the model.

5. **Receiver Operating Characteristic Curve**
The receiver operating characteristic (ROC) curve is a visual depiction of the performance of a binary classification model. It evaluates the balance between the model's sensitivity (true positive rate) and 1-specificity (false positive rate).
The ROC curve, as seen in Figure 5 [62], often represents the true positive rate (TPR) or sensitivity on the vertical axis. In contrast, the false positive rate (FPR) or 1-specificity is displayed on the horizontal axis. The ideal ROC curve is characterized by its positioning in the upper-left corner of the graph, indicating a high level of sensitivity and a low number of false positives, which are desirable qualities for a classification model.

6. **Area Under the Curve (AUC)**
As shown in the ROC graph, the area under the curve signifies the comprehensive efficacy of a classifier. The AUC of a perfect classifier is 1, whereas the AUC of a random classifier is 0.5. A greater AUC indicates the more effective discriminatory capabilities of the model.

7. **False Alarm Rate**
The false alarm rate (FAR) is a statistic used to assess system performance, particularly in the context of signal detection, anomaly detection, and security systems. It counts the number of false alarms or false positives generated by the system.

8. **Invalid Positive Rate**
The invalid positive rate is used when the rate of positive results, typically in the context of medical tests or diagnostic procedures, is not valid or reliable. This can occur for various reasons, such as issues with the test, improper administration, or a small sample size. It is usually the true negative rate in terms of intrusions.

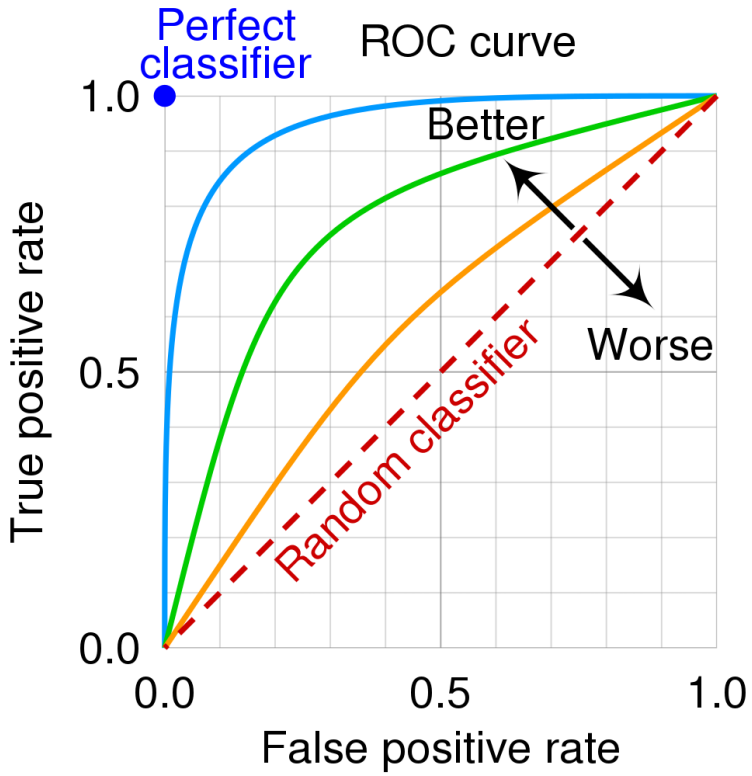


Figure 5. Receiver operating characteristic (ROC) curve [62].

Table 10. Performance metrics.

Metric	Description	Note
Precision	Measures a model's accuracy in positive predictions	Between 0 and 1
Recall	Measures how specific the model is in terms of finding the true positives among actual positives	Values between 0.0 and 1.0
F1 score	Measures how accurate a model is: goodness of fit	Higher is better, values between 0 and 1, used when datasets are imbalanced
Accuracy	Measures the number of correct predictions out of all predictions made	Higher is better, values between 1 and 100 in percentage
ROC Curve	An illustration of how well a binary classification model performs. It assesses how well the model's true positive rate (sensitivity) and false positive rate (specificity) are balanced. Moreover, the upper-left corner of the graph, which denotes a high degree of sensitivity and few false positives, is where the ideal ROC curve is located	Better performance is indicated by values closer to the upper-left corner
AUC	Measures the overall performance of a binary classifier	Values between 0.0 and 1.0
False Alarm Rate (FAR)	Measures the rate at which the system generates false alarms or false positives.	Lower is better, values between 0 and 1
Invalid Positive Rate	Measures true negative rate	Lower is better, values between 0 and 1

5. Discussion

A wide range of techniques and strategies for cyberattack detection are presented in the reviewed literature, with an emphasis on intrusion detection systems (IDS) in the context of the Internet of Medical Things (IoMT). In order to identify similarities, differences, and potential topics for further research, the results and approaches of the examined studies are compared and contrasted in this section.

Several studies improve cyberattack detection in IoMT networks by utilizing machine learning (ML) and deep learning (DL) approaches. To achieve better interpretability and accuracy, Zhang et al. [40] suggest a model that combines multi-head attention with bidirectional long short-term memory (BiLSTM). Similar to this, Rayan et al. [46] classify network traffic and secure data by combining blockchain technology with a tri-layered feed-forward neural network (TNN). By utilizing graph-based methods and multi-head attention transformation mechanisms, Li [45] present the edge-directed graph multi-head attention network model (EDGMAT) for network intrusion detection systems (NIDS).

These studies show that ML and DL techniques are effective in detecting cyberattacks, but they also emphasize the value of interdisciplinary cooperation. In order to detect intrusions, Abdallah [3] combines LightGBM and BERT-based Transformers. This highlights the difficulty in implementing such systems and the requirement for correlation computations in order to successfully integrate data streams. Ahmed [37] delves into the application of a modified Transformer neural network (MTNN) for enhanced precision and recall. The study highlights the dependence on conventional feature selection techniques and the possible constraints of GANs in replicating actual cyber threats.

A collection of standardized performance criteria, such as the accuracy, precision, recall, F1 score, area under the curve (AUC), false alarm rate, and invalid positive rate, are used to evaluate cybersecurity models. There are differences in the performance of various models, although the majority of studies claim good accuracy and detection rates. For example, Zhang's model [40] outperforms other models in terms of predicted accuracy, achieving remarkable accuracy and F1 score. Surprisingly high performance measures for the baseline approaches point to potential overfitting problems or dataset restrictions in Rayan et al.'s architecture [46].

This study outlines a number of exciting prospects in the field of cybersecurity for IoT and IoMT applications, in addition to pointing out current obstacles and research gaps. These opportunities include exploring blockchain-based security solutions to improve data integrity and trust; fostering interdisciplinary collaboration to address complex security challenges; integrating artificial intelligence techniques for adaptive threat detection; harnessing real-time threat intelligence feeds for proactive threat identification; and ensuring compliance with cybersecurity standards and regulatory requirements to establish robust security frameworks. By seizing these new opportunities, organizations may reduce the cyber risks, improve the security of IoT and IoMT systems, and create robust healthcare infrastructures that can survive growing cyber attacks.

6. Conclusions

In conclusion, this study provides a thorough survey and analysis of cyberattack detection techniques, emphasizing intrusion detection systems (IDS). This research focuses on the cybersecurity of the Internet of Medical Things (IoMT). The survey covers a wide range of methodologies identified in the recent literature for the safeguarding of IoMT networks, including blockchain technology, Transformer-based models, deep learning (DL), machine learning (ML), and graph-based techniques.

A clear pattern suggests combining ML and DL techniques to improve the detection performance, frequently by building hybrid models to solve certain drawbacks. Transformer-based models demonstrate possible uses in cyberattack detection, drawing inspiration from developments in natural language processing. Furthermore, graph-based methods, such as graphical security modeling (GSM), provide valuable insights into com-

plex systems such as Internet of Things networks, making it easier to create strong security plans and vulnerability detection systems.

By using decentralized consensus methods and cryptographic techniques, blockchain technology can potentially improve the data security in Internet of Things networks. Despite progress, challenges persist, including the need for more diverse datasets, scalability issues, and the ongoing evolution of cyber threats. Interdisciplinary collaboration is crucial in addressing these challenges and developing robust defense mechanisms.

This survey highlights the various methods used to identify cyberattacks and emphasizes the importance of interdisciplinary collaboration in solving cybersecurity issues. Several research gaps are highlighted in relation to intrusion detection for IoT and IoMT applications, emphasizing the need for more effective and lightweight models, improved methods of detecting new threats and anomalies, and further investigation into edge device deployment and federated learning.

This study evaluates the effectiveness of cybersecurity models using a detailed set of performance metrics, listed in Table 10. These metrics include precision, which emphasizes the accuracy of positive predictions, and recall, which assesses the model's capability to correctly identify all actual positives. The F1 score offers a balanced perspective by considering both false positives and false negatives. Additionally, the overall accuracy provides an estimate of the correct predictions made. The receiver operating characteristic (ROC) curve and the area under the curve (AUC) provide both visual and quantitative evaluations of the model performance. The results demonstrate that these metrics can be used together to create a comprehensive evaluation framework that highlights the strengths and weaknesses of the current cybersecurity solutions. The application of these metrics has pinpointed critical areas for improvement, especially in enhancing the precision and recall, which are vital in detecting cyberattacks effectively in IoMT environments.

There are several limitations that should be noted despite the thorough survey and analysis that this study presents. Firstly, given the rapid development of this area, the study might not include all recent developments and approaches in cyberattack detection for IoT and IoMT applications. Furthermore, the quality and accessibility of datasets can have a significant impact on the generalizability of the results and the assessment of the performance measures and approaches. Moreover, although the importance of multidisciplinary cooperation in tackling cybersecurity issues is emphasized, the study's depth and breadth restrictions prevented it from delving thoroughly into any particular interdisciplinary strategy.

Further investigation is necessary in areas such as creating lighter and more efficient models, especially for IoT and IoMT applications, since existing models might not be sufficiently scalable or resource-efficient. Better techniques for the identification of novel risks and abnormalities are also required, particularly in the quickly changing cyber threat landscape. To guarantee the efficient deployment of intrusion detection systems in dispersed and resource-constrained contexts, more research on edge device deployment and federated learning is necessary. In order to provide a thorough security framework for healthcare systems, research should also look into how intrusion detection may be integrated with other security measures like firewalls and intrusion prevention systems.

Significant challenges and gaps in knowledge remain despite advances in cyberattack detection for IoMT networks. Incorporating advanced measures such as the false alarm rate and invalid positive rate, improving the models' accuracy, and creating intrusion detection systems that are resistant to adversarial attacks should be the top priorities for future research. In order to strengthen cybersecurity protection in IoMT scenarios, more research into federated learning and edge device deployment is required, along with better scalability and dataset variety. The creation of a safer digital healthcare environment that is capable of successfully resisting cyber threats depends on these initiatives.

Author Contributions: Conceptualization, S.A., N.I., S.S., A.Y. and R.K.; methodology, S.A., N.I., S.S., A.Y. and R.K.; validation, S.A., N.I., S.S., A.Y. and R.K.; formal analysis, S.A., N.I., S.S. and A.Y.; investigation, S.A., N.I., S.S. and A.Y.; writing—original draft preparation, S.A., N.I., S.S. and A.Y.; writing—review and editing, R.K.; visualization, R.K.; supervision, R.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Toronto Metropolitan University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Hernandez-Jaimes, M.L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K.A.; Feregrino-Uribe, C. Artificial Intelligence for IoMT Security: A Review of Intrusion Detection Systems, Attacks, Datasets, and Cloud-Fog-Edge Architectures. *Internet Things* **2023**, *23*, 100887. [CrossRef]
2. Soleymanzadeh, R.; Kashef, R. The Future Roadmap for Cyber-Attack Detection. In Proceedings of the International Conference on Cryptography, Security and Privacy (CSP), Tianjin, China, 14–16 January 2022.
3. Ghourabi, A. A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks. *IEEE Access* **2022**, *10*, 48890–48903. [CrossRef]
4. WannaCry Ransomware. Available online: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed on 11 May 2024).
5. Cyber Attack Suspected in German Woman's Death. Available online: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (accessed on 11 May 2024).
6. Si-Ahmed, A.; Al-Garadi, M.A.; Boustia, N. Survey of Machine Learning based Intrusion Detection Methods for Internet of Medical Things. *Appl. Soft Comput.* **2023**, *140*, 110227. [CrossRef]
7. Aldhaheri, A.; Alwahedi, F.; Ferrag, M.A.; Battah, A. Deep learning for cyber threat detection in IoT networks: A review. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 110–128. [CrossRef]
8. Admass, W.S.; Munaye, Y.Y.; Diro, A.A. Cyber security: State of the art, challenges and future directions. *Cyber Secur. Appl.* **2024**, *2*, 100031. [CrossRef]
9. Gümüşbaş, D.; Yıldırım, T.; Genovese, A.; Scotti, F. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. *IEEE Syst. J.* **2021**, *15*, 1717–1731. [CrossRef]
10. Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
11. Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access* **2020**, *8*, 106576–106584. [CrossRef]
12. WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research. Available online: https://www.cse.wustl.edu/~jain/ehms/index.html (accessed on 1 November 2023).
13. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Comput. Commun.* **2021**, *166*, 110–124. [CrossRef]
14. Tauqeer, H.; Iqbal, M.; Ali, A.; Zaman, S.; Chaudhry, M.U. Cyberattacks Detection in IoMT using Machine Learning Techniques. *Comput. Biomed. Inform.* **2022**, *4*, 13–20. [CrossRef]
15. Kulshrestha, P.; Kumar, T.V. Machine learning based intrusion detection system for IoMT. *Int. Syst. Assur. Eng. Manag.* **2023**, 1–13 [CrossRef]
16. Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.; Rodriguez, J. An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks. *Electronics* **2021**, *10*, 2562. [CrossRef]
17. Ahmed, M.; Byreddy, S.; Nutakki, A.; Sikos, L.F.; Haskell-Dowland, P. ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. *Ad Hoc Netw.* **2021**, *122*, 102621. [CrossRef]
18. Nayak, J.; Meher, S.; Souri, A.; Naik, B.; Vimal, S. Extreme Learning Machine and Bayesian Optimization-Driven Intelligent Framework for IoMT Cyber-Attack Detection. *J. Supercomput.* **2022**, *78*, 14866–14891. [CrossRef]
19. Wazid, M.; Singh, J.; Das, A.K.; Rodrigues, J.J.P.C. An Ensemble-Based Machine Learning-Envisioned Intrusion Detection in Industry 5.0-Driven Healthcare Applications. *IEEE Trans. Consum. Electron.* **2023**, *1*, 1903–1912. [CrossRef]
20. Fouda, M.; Ksantini, R.; Elmedany, W. A Novel Intrusion Detection System for Internet of Healthcare Things Based on Deep Subclasses Dispersion Information. *IEEE Internet Things J.* **2023**, *10*, 8395–8407. [CrossRef]
21. Soleymanzadeh, R.; Kashef, R. A Stable Generative Adversarial Network Architecture for Network Intrusion Detection. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Virtual, 27–29 July 2022; pp. 9–15. [CrossRef]

22. Siniosoglou, I.; Sarigiannidis, P.; Argyriou, V.; Lagkas, T.; Goudos, S.K.; Poveda, M. Federated Intrusion Detection In NG-IoT Healthcare Systems: An Adversarial Approach. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Xiamen, China, 28–30 July 2021; pp. 1–6. [CrossRef]
23. PhysioNet. CharisDB. Available online: https://www.physionet.org/content/charisdb/1.0.0/ (accessed on 1 November 2023).
24. Kim, N.; Krasner, A.; Kosinski, C.; Wininger, M.; Qadri, M.; Kappus, Z.; Danish, S.; Craelius, W. Trending Autoregulatory Indices During Treatment for Traumatic Brain Injury. *J. Clin. Monit. Comput.* **2016**, *30*, 821–831. [CrossRef]
25. Singh, P.; Gaba, G.S.; Kaur, A.; Hedabou, M.; Gurtov, A. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 722–731. [CrossRef]
26. Tareq, I.; Elbagoury, B.M.; El-Regaily, S.; El-Horbaty, E.S.M. Analysis of ToN-IoT, UNSW-NB15, and Edge-IIoT Datasets Using Deep Learning in Cybersecurity for IoT. *Appl. Sci.* **2022**, *12*, 9572. [CrossRef]
27. Otoum, Y.; Wan, Y.; Nayak, A. Federated Transfer Learning-Based IDS for the Internet of Medical Things (IoMT). In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7 –11 December 2021; pp. 1–6. [CrossRef]
28. Zakariyya, I.; Kalutarage, H.; Al-Kadri, M.O. Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring. *Comput. Secur.* **2023**, *133*, 103388. [CrossRef]
29. Bakhsh, S.A.; Khan, M.A.; Ahmed, F.; Alshehri, M.S.; Ali, H.; Ahmad, J. Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet Things* **2023**, *24*, 100936. [CrossRef]
30. Khan, F.; Jan, M.A.; Alturki, R.; Alshehri, M.D.; Shah, S.T.; ur Rehman, A. A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT. *IEEE Trans. Ind. Inform.* **2023**, *19*, 10125–10132. [CrossRef]
31. Kilincer, I.F.; Ertam, F.; Sengur, A.; Tan, R.S.; Acharya, U.R. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybern. Biomed. Eng.* **2023**, *43*, 30–41. [CrossRef]
32. Gupta, K.; Sharma, D.K.; Gupta, K.D.; Kumar, A. A tree classifier based network intrusion detection model for Internet of Medical Things. *Comput. Electr. Eng.* **2022**, *102*, 108158. [CrossRef]
33. Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. [CrossRef]
34. Priya R.M., S.; Maddikunta, P.K.R.; Parimala, M.; Koppu, S.; Gadekallu, T.R.; Chowdhary, C.L.; Alazab, M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput. Commun.* **2020**, *160*, 139–149. [CrossRef]
35. Kumar, S.; Goswami, N. Preserving Security in Internet-of-Things Healthcare System with Metaheuristic-Driven Intrusion Detection. *Eng. Sci.* **2023**, *25*, 933.
36. Anderson, H.S.; Roth, P. EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. *arXiv* **2018**, arXiv:1804.04637.
37. Ahmed, S.W.; Kientz, F.; Kashef, R. A Modified Transformer Neural Network (MTNN) for Robust Intrusion Detection in IOT Networks. In Proceedings of the 2023 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 18–20 July 2023. [CrossRef]
38. TON_IoT Datasets. Available online: https://research.unsw.edu.au/projects/toniot-datasets (accessed on 11 May 2024).
39. Wu, Z.; Zhang, H.; Wang, P.; Sun, Z. RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System. *IEEE Access* **2022**, *10*, 64375–64387. [CrossRef]
40. Zhang, J.; Zhang, X.; Liu, Z.; Fu, F.; Jiao, Y.; Xu, F. A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism. *Electronics* **2023**, *12*, 4170. [CrossRef]
41. Liu, C.; Liu, Y.; Yan, Y.; Wang, J. An Intrusion Detection Model With Hierarchical Attention Mechanism. *IEEE Access* **2020**, *8*, 67542–67554. [CrossRef]
42. Song, Y.; Zhang, D.; Li, Y.; Shi, S.; Duan, P.; Wei, J. Intrusion Detection for Internet of Things Networks using Attention Mechanism and BiGRU. In Proceedings of the 2023 5th International Conference on Electronic Engineering and Informatics (EEI), Wuhan, China, 30 June–2 July 2023. [CrossRef]
43. NSL-KDD Dataset. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed on 14 May 2024).
44. Chee, K.O.; Ge, M.; Bai, G.; Kim, D.D. IoTSecSim: A framework for modelling and simulation of security in Internet of things. *Comput. Secur.* **2024**, *136*, 103534. [CrossRef]
45. Li, X.; Zhang, J.; Yuan, Y.; Zhou, C. Network Intrusion Detection with Edge-Directed Graph Multi-Head Attention Networks. *arXiv* **2023**, arXiv:2310.17348.
46. Alsemmeari, R.A.; Dahab, M.Y.; Alsulami, A.A.; Alturki, B.; Algarni, S. Resilient Security Framework Using TNN and Blockchain for IoMT. *Electronics* **2023**, *12*, 2252. [CrossRef]
47. Malicious-Traffic-Detection-in-IoT-Healthcare-Environment. Available online: https://github.com/ThingzDefense/Malicious-Traffic-Detection-in-IoT-Healthcare-Environment (accessed on 11 May 2024).
48. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. *Sensors* **2021**, *21*, 3025. [CrossRef] [PubMed]
49. Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A.N.; Kaiser, Ł.; Polosukhin, I. Attention is all you need. *Adv. Neural Inf. Process. Syst.* **2017**, *30*, 5998–6008.
50. Ecu-IoHT. Available online: https://ro.ecu.edu.au/datasets/48/ (accessed on 11 May 2024).

51. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
52. Bot-IoT Dataset. Available online: https://research.unsw.edu.au/projects/bot-iot-dataset (accessed on 11 May 2024).
53. IoTdataset-2022. Available online: https://www.unb.ca/cic/datasets/iotdataset-2022.html (accessed on 11 May 2024).
54. Dadkhah, S.; Mahdikhani, H.; Danso, P.K.; Zohourian, A.; Truong, K.A.; Ghorbani, A.A. Towards the Development of a Realistic Multidimensional IoT Profiling Dataset. In Proceedings of the 2022 19th Annual International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 22–24 August 2022; pp. 1–11. [CrossRef]
55. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
56. Kitsune Network Attack Dataset. Available online: https://archive.ics.uci.edu/dataset/516/kitsune+network+attack+dataset (accessed on 11 May 2024).
57. WUSTL-IIOT-2018 Dataset for ICS (SCADA) Cybersecurity Research. Available online: https://www.cse.wustl.edu/~jain/iiot/index.html (accessed on 11 May 2024).
58. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, 10, 40281–40306. [CrossRef]
59. UNSW-NB15 Dataset. Available online: https://research.unsw.edu.au/projects/unsw-nb15-dataset (accessed on 11 May 2024).
60. CIC-IDS2017 Dataset. Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 11 May 2024).
61. CSE-CIC-IDS2018 Dataset. Available online: https://www.unb.ca/cic/datasets/ids-2018.html (accessed on 11 May 2024).
62. ROC Curve Image. Available online: https://en.wikipedia.org/wiki/File:Roc_curve.svg (accessed on 11 May 2024).