Article

A Deep Learning-Based Framework for Strengthening Cybersecurity in Internet of Health Things (IoHT) Environments

Sarah A. Algethami and Sultan S. Alshamrani *

Department Information Technology, College of Computers and Information Technology Taif University, Taif 21944, Saudi Arabia; s44480555@students.tu.edu.sa
* Correspondence: susamash@tu.edu.sa

Abstract: The increasing use of IoHT devices in healthcare has brought about revolutionary advancements, but it has also exposed some critical vulnerabilities, particularly in cybersecurity. IoHT is characterized by interconnected medical devices sharing sensitive patient data, which amplifies the risk of cyber threats. Therefore, ensuring healthcare data's integrity, confidentiality, and availability is essential. This study proposes a hybrid deep learning-based intrusion detection system that uses an Artificial Neural Network (ANN) with Bidirectional Long Short-Term Memory (BLSTM) and Gated Recurrent Unit (GRU) architectures to address critical cybersecurity threats in IoHT. The model was tailored to meet the complex security demands of IoHT and was rigorously tested using the Electronic Control Unit ECU-IoHT dataset. The results are impressive, with the system achieving 100% accuracy, precision, recall, and F1-Score in binary classifications and maintaining exceptional performance in multiclass scenarios. These findings demonstrate the potential of advanced AI methodologies in safeguarding IoHT environments, providing high-fidelity detection while minimizing false positives.

Keywords: IoHT; deep learning; intrusion detection systems; healthcare; cybersecurity

1. Introduction

The Internet of Things (IoT) is an innovative technology that facilitates data collection, analysis, and dissemination for intelligent applications [1]. Its distinctive attributes have captured the interest of urban planners and healthcare experts, as it has the potential to revolutionize real-time applications like eHealth and smart cities [2]. IoT is an internet of three types of relationships: human-to-human, human-to-machine, and machine-to-machine, all communicating over the internet [3]. AI enhances IoT applications by obtaining useful features from the vast data generated by IoT devices, leading to innovative solutions that provide value to individuals and businesses [4]. The integration of AI with IoT strengthens security and drives efficiency, customization, and automation across various sectors.

On the other hand, IoHT specifically targets healthcare, integrating medical devices and sensors to enhance patient care through real-time data collection and remote monitoring. IoHT addresses challenges, including patient safety, data security, and regulatory compliance, setting it apart from general IoT applications.

Cybersecurity measures must be prioritized to secure information and networks. To achieve this, intrusion detection systems (IDSs) are used to monitor network traffic, detect suspicious activity, and mitigate the harmful effects of cyber-attacks on IoHT networks and nodes [5]. IDSs may not be effective in detecting new and unknown adversarial attacks, especially with the increasing number of IoT devices [6]. The emergence of machine learning (ML) has greatly influenced the field of cybersecurity, enabling the creation of intelligent systems that can effectively prevent network attacks [7].

Among these systems, IDS, which uses deep learning (DL) techniques, has demonstrated exceptional performance compared to other methods [8]. Through their data-driven approach, these solutions have successfully addressed numerous cybersecurity obstacles.

Study [9] proposed a novel intrusion detection system designed specifically for IoT networks. The system successfully identified various types of assaults by using a hybrid approach that included the Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) models. The suggested approach demonstrated its suitability for a diverse array of IoT applications. The UNSW NB15 dataset was used, with a validation ratio of 70% for training and 30% for test validation. The proposed model was experimentally shown to achieve an accuracy of 98% across various IoT scenarios.

Undetected attacks on the IoT may lead to significant service disruptions, causing substantial financial losses. Furthermore, it presents the potential risk of compromising one's identity. The real-time detection of intrusions on IoT devices is crucial for ensuring the reliability, security, and profitability of IoT-enabled services. A study proposed a novel intrusion detection system for IoT devices using DL techniques [10].

The system utilized a four-layer deep Fully Connected (FC) network architecture to identify malicious traffic that could launch assaults on interconnected IoT devices. The system under consideration was designed to be independent of communication protocols to mitigate the challenges associated with deployment. The system under consideration exhibited consistent and dependable performance when subjected to simulated and actual intrusions, as shown by the experimental performance study. The system had a mean accuracy of 93.74% in identifying and detecting several types of cyber assaults, including Blackhole, Distributed Denial of Service (DDOS), Opportunistic Service, Sinkhole, and Workhole attacks. On average, the suggested intrusion detection system's precision, recall, and F1-Score were 93.71%, 93.82%, and 93.47%, respectively. That study's deep learning-based intrusion detection system (IDS) demonstrated a commendable average detection rate of 93.21%. This performance level is deemed suitable for enhancing the security of IoT networks. Conventional IDSs for advanced network-based attack detection encounter difficulties in network environments that employ typical IoT protocols and operate on a centralized network architecture, such as a software-defined network (SDN). In [11], the authors proposed a methodology that utilizes LSTM to identify network assaults inside IoT networks, with IDS enabled by SDN. The authors provided a comprehensive assessment of the performance of ML and DL models using two datasets designed explicitly for Software-Defined Networking in the Internet of Things (SDNIoT) applications. The authors also proposed an architecture based on LSTM to classify network assaults in IoT networks efficiently using several classes. The assessment of the suggested model demonstrated its efficacy in accurately detecting assaults and categorizing them, with a classification accuracy of 0.971. Furthermore, various visualization techniques were used to get insights into the dataset's properties and visually represent the embedding features.

Identifying and differentiating such threats pose significant challenges, necessitating a sophisticated IDS. ML has emerged as a promising methodology for developing intelligent IDSs across several domains, including the IoT. Nevertheless, it is crucial to note that the input for ML models must be derived from the IoT environment via feature extraction models. These models have considerable importance in determining the detection rate and accuracy of the ML models. Hence, the primary objective of study [12] was to investigate the implementation of machine learning-based IDSs in the IoT. The investigation specifically focused on evaluating several feature extraction methods with many machine learning models. That work evaluated several feature extractors, including image filters, and transfer learning models such as VGG-16 and DenseNet. Furthermore, considering all the feature extraction approaches studied, a comprehensive evaluation was conducted on several machine learning techniques, such as random forest, K-nearest neighbors, support vector machine (SVM), and different stacked models. The research comprehensively assessed the collective models using the IEEE Dataport dataset. The study's findings revealed that utilizing VGG-16 with stacking techniques yielded the most noteworthy accuracy rate, reaching 98.3%.

An advanced approach to enhancing the security of the IoT involves using deep learning techniques. This approach presents a coherent solution for anomaly-based detection.

The research by the authors of [13] introduced a convolutional neural network (CNN) technique for anomaly-based IDSs in the field of IoT. The proposed approach leveraged the capabilities of IoT to analyze the whole network traffic inside the IoT ecosystem effectively. The model under consideration could identify and classify instances of intrusion and anomalous patterns in network traffic. The model underwent training and testing procedures using the NID Dataset and BoT-IoT datasets, yielding accuracy rates of 99.51% and 92.85%, respectively.

The authors of [14] developed a novel framework based on Explainable Artificial Intelligence (XAI) to detect intrusions in IoT networks. The proposed framework incorporates a deep neural network model as the first component for real-time intrusion detection. Once the model has been determined, their framework incorporated three distinct ways of Explainable Artificial Intelligence (XAI) to enhance the model's decision-making process with increased levels of explainability, transparency, and trust. Furthermore, the framework was designed to cater to two distinct user groups: users of the deep learning model who seek to comprehend and have confidence in the model's outputs to enhance their decision-making, and cybersecurity experts who also desire to comprehend the model's outputs to provide appropriate recommendations, particularly in the event of an intrusion being detected. The feasibility and performance of the framework were demonstrated using the NSL-KDD and UNSWNB15 datasets. The experimental results indicated the effectiveness of the proposed XAI-based framework in detecting attacks in IoT systems. Furthermore, their framework provided additional insights and explanations regarding the deep neural network model's decision-making process, enhancing the interpretation of the detection outcomes. The researchers' findings indicated that the XAI framework yielded 88% and 99% accuracy when applied to the NSL−KDDTest and UNSW-NB15 datasets.

Article [15] presented the implementation of an intelligent intrusion detection system designed to identify and detect assaults against IoT devices. A deep learning system was used to identify fraudulent network traffic inside the Internet of Things. The identification solution guaranteed operational security and facilitated interoperability across connection protocols in the Internet of Things. IDS is a widely used network security technology for network protection. Based on the findings obtained from their experimental analysis, the suggested architecture for intrusion detection exhibited a high level of proficiency in accurately identifying genuine global intrusions. Using a neural network to detect assaults demonstrated a high level of effectiveness. Furthermore, there is a growing emphasis on providing cybersecurity solutions that prioritize the needs and preferences of users. This requires collecting, processing, and analyzing substantial data traffic volumes and connections inside 5G networks. After rigorous testing, the autoencoder model exhibited superior performance by significantly reducing detection time and enhancing detection accuracy. A remarkable accuracy rate of 99.76% was attained using the suggested methodology.

As the volume of sensitive data transmitted in IT infrastructures increases, healthcare individuals and businesses that generate supplementary data for users have become attractive targets for cybercriminals. IoHT devices must be protected to preserve electronic healthcare data. Researchers have attempted to develop a robust IDS to secure healthcare environments.

The authors of [16] presented a hybrid deep learning methodology for IoT botnet malware detection that incorporates CNN-BLSTM-GRU to facilitate efficient multiclass malware family detection. Accuracy, detection rate, and receiver operating characteristic area under the curve (ROC AUC) were performance metrics used to evaluate the hybrid deep learning model proposed by the authors. IoT-based botnet attack detection attained 98.34% accuracy and the suggested hybrid CNN-BLSTM-GRU deep learning-based botnet attack detection system obtained 99.25% accuracy.

Study [17] proposed a new cybersecurity method using deep learning to facilitate the detection of intrusions in the social Internet of Things. The performance of the deep model was compared to that of the conventional machine learning approach, and the performance of the distributed attack detection system was compared to that of the centralized detection

system. Using the NSL-KDD dataset, the experiments demonstrated that the overall detection accuracy increased from 96% to over 99%.

The healthcare industry increasingly applies IoT and artificial intelligence (AI) technologies to enhance services. IoT-enabled hospital devices improve patient safety, reduce costs, and increase healthcare accessibility [18]. AI and IoT play vital roles in medical diagnostics, real-time patient monitoring, medical image analysis, treatment planning, drug discovery, and personalized healthcare [19]. Smart healthcare systems leverage wearable devices, IoT, and AI to access medical information, enhancing efficiency and personalization in healthcare services [20]. ML in IoT allows for pattern recognition and predictive capabilities, benefiting healthcare through automated patient monitoring and data management [21]. The combination of AI and IoT in healthcare is revolutionizing decision-making and resource management but also presents challenges, including cybersecurity, energy consumption, and privacy concerns. Researchers are looking to enhance cyber-attack detection in IoT by utilizing artificial intelligence, machine learning, and deep learning methods to identify new and evolving threats while minimizing false positive detections.

IoHT is a network combining various hardware platforms, software, and medical devices to support healthcare information technology [22]. In this environment, smart medical devices such as glucometers and blood pressure monitors are interconnected, enabling seamless communication and the sharing of vital medical data [23]. Healthcare practitioners and facilities then use this information to provide top-quality care and support. However, it is essential to remember that IoHT devices collect sensitive health data, which makes security and privacy protection critical [24]. With intelligent monitoring and data transmission to an IoHT server, these devices transform how we care for patients. Protecting IoT devices from cyber threats is paramount, as hardware and software can be vulnerable to attacks [25].

In [26], a deep neural network-based cyber-attack detection system is developed using artificial intelligence on the ECU-IoHT dataset to detect cyber-attacks in the Internet of Health Things ecosystem. The proposed deep neural network system obtained an improved performance accuracy of 99.85 percent, a mean area under the receiver operator characteristic curve of 0.99, and a false positive rate of 0.01.

Paper [27] suggested a deep neural network in federated learning (DNN-FL) to detect security-threatening anomalies in IoHT data. The authors evaluated their proposal's detection effectiveness using metrics such as accuracy and precision. Using the wustl-ehms-2020 and ECU-IoHT datasets, the proposed DNN-FL was validated. It detected attacks with 91.40% accuracy in the wustl-ehms-2020 dataset and 98.47% in the binary classification on the ECU-IoHT dataset.

In [28], the authors proposed a framework for developing IoT context-aware security solutions to detect malicious traffic in IoT healthcare environments. The proposed framework consisted of an IoT traffic generator utility that generated standard and malicious traffic using an IoT-based Intensive Care Unit (ICU) use case. Six commonly used ML classifiers were trained and evaluated on the generated dataset for malicious and traditional traffic detection in the IoT healthcare environment. They examined the efficacy of every trained ML classifier. The random forest classifier performed the best among the six ML classifiers, with 99.7068% precision, 99.79% recall, 99.51% accuracy, and 99.65% F1-Score. The main contribution of this work involves building an intrusion detection model in the IoHT model, which covers a range of cyber-attack scenarios while maintaining the confidentiality of medical information. We explore different intrusion detection techniques, including deep learning. Deep learning is a powerful option for intrusion detection in IoHT because of its ability to self-learn, adapt, and generalize.

Our work is based on leveraging the ECU-IoHT dataset [29] for evaluation. This dataset enables us to assess our model's effectiveness in detecting a wide range of cyber-attack scenarios while ensuring the confidentiality of sensitive medical information. A comparative analysis systematically evaluates our approach against existing methods to

highlight its advantages and unique contributions. This comparison can be performed using various standard metrics, which provide quantitative proof of our model's superior performance. Explicitly remarking on the limits of current approaches, such as their inability to detect new and unknown adversarial attacks effectively, sets the stage for showcasing the innovative aspects of our solution. Our proposed model, which integrates a hybrid deep learning model, addresses these limitations, and we can clearly articulate the improvements. Emphasizing our model's robust performance on a realistic ECU-IoHT dataset and its adaptability to various IoHT scenarios highlights its practical applicability and relevance.

2. Materials and Methods

The methodology used in this study is designed to investigate and evaluate the effectiveness of deep learning-based cyber-attack detection systems in the IoHT environments. The study starts with a thorough review of the existing literature, which offers a theoretical analysis of diverse intrusion detection approaches focused on deep learning methodologies. Key aspects, such as overall cyber-attacks in IoHT networks, existing IDS, and the challenges associated with cybersecurity in healthcare, are extensively examined. The theoretical framework lays the foundation for understanding the complexities of IoHT cyber threats.

The study then flows into the experimental phase, which involves developing and implementing a deep learning network-based cyber-attack detection system. The novel ECU-IoHT dataset, known for reflecting various cyber-attacks in the medical field, is chosen for experimentation. Using this dataset ensures relevance to real-world scenarios while mitigating potential risks associated with sensitive healthcare data. The research methodology integrates artificial intelligence techniques, leveraging deep learning capabilities for anomaly detection within the IoHT environment.

2.1. Data Source and Collection

Our deep learning model is evaluated using the ECU-IoHT dataset, which includes both normal network activity and cyber-attacks in the healthcare domain. The dataset's generation involves an environment equipped with specific components, notably a Windows 10 operating system, Kali Linux, a mobile Wi-Fi hotspot, a wireless network adapter, and a Bluetooth adapter, all interconnected to enable internet access for the hosts. In addition, the environment incorporates a healthcare kit named MySignals, equipped with multiple sensors designed for monitoring and recording patients' physiological data, encompassing metrics like body temperature, blood pressure, and heart rate. These sensor-generated data are subsequently transmitted to users' cloud storage. The ECU-IoHT dataset encompasses seven key network data features: source, destination, protocol, and specific attack types. Within the dataset, 23,453 instances represent normal network activity, while other instances correspond to cyber-attack instances. These attacks are classified into four distinct types: Address Resolution Protocol (ARP) spoofing, Denial-of-Service (DoS) attacks, Network Mapper (Nmap) port scans, and Smurf attacks. ARP spoofing involves sending false Address Resolution Protocol messages to associate the attacker's MAC address with the IP address of a legitimate network device, leading to data interception. DoS attacks aim to overwhelm a target system with excessive requests, rendering it unavailable to legitimate users. Nmap port scans involve probing a network to identify open ports and services, aiding in vulnerability assessment. Smurf attacks exploit IP broadcast addressing to flood a target system with ICMP echo requests, causing network congestion and disruption. The ECU-IoHT dataset is used to train and evaluate the model, ensuring its suitability for healthcare applications. Notably, this method significantly improves detection accuracy by analyzing a substantial volume of data, with the ECU-IoHT dataset comprising a total of 111,207 samples, as presented in Figure 1.
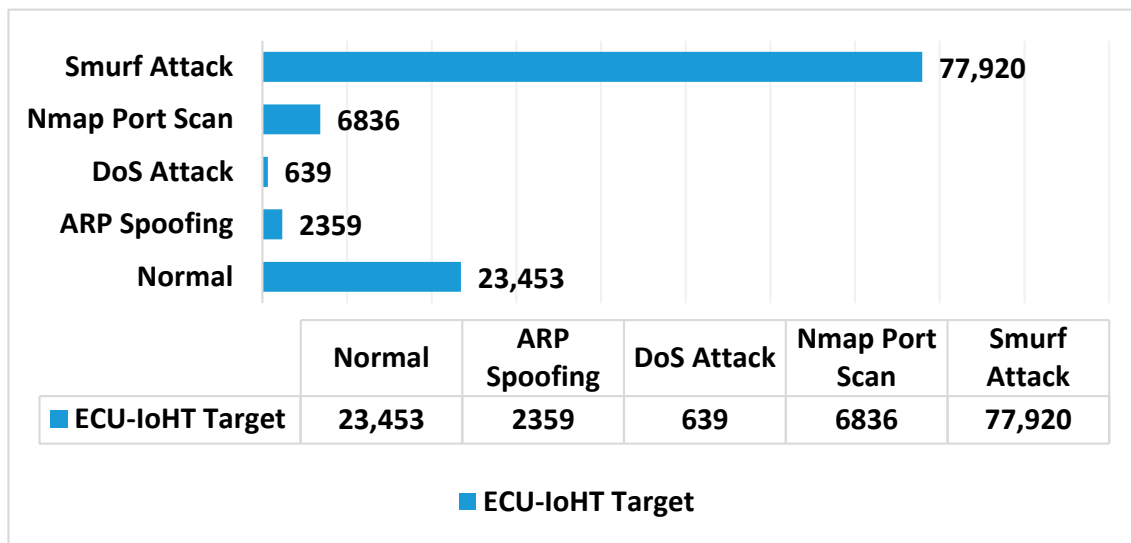
Figure 1. Proposed ECU-IoHT target data distribution.

A comprehensive multi-stage quality assurance protocol is crucial for maintaining the integrity and reliability of a dataset used in deep learning for cyber-attack detection in IoHT environments. The process starts by gathering and combining data from public sources, then cleaning missing data and standardizing it for accuracy and consistency. A thorough relevance assessment is conducted on the dataset, consistency checks are performed on network data features, and validation is carried out to verify its appropriateness for model training. Recognizing the importance of iterative data preprocessing, the protocol mandates regular evaluations and adjustments to optimize the dataset's contribution to building a robust detection system.

The performance requirements for the deep learning-based cyber-attack detection system in the IoHT environment are crucial to achieving our research objectives. The model must exhibit exceptional accuracy, recall, and precision performance to effectively identify and classify a wide range of cyber-attacks while minimizing false detections. Efficiently handling a dataset of 111,207 samples is essential. Additionally, the system's performance should be reliable and consistently effective across different scenarios and data variations. Moreover, the strategy must achieve a low false positive rate in detecting and responding to cyber threats, reflecting the real-time requirements of the IoHT environment where timely action is critical.

Achieving performance requirements is vital to ensure the proposed deep learning approach contributes significantly to strengthening cybersecurity in IoHT, enhancing the security of sensitive medical data, and ultimately guaranteeing the well-being of patients.

2.2. Hybrid Deep Learning Model

This study introduces an innovative hybrid deep learning-based IoHT attack detection model that combines an ANN with BLSTM and GRU architectures. The hybrid model integrates the ANN's ability to process intricate patterns, BLSTM's capacity to capture sequential dependencies in both directions, and GRU's efficiency in handling long-term dependencies. This integrated architecture aims to improve cyber-attack detection in the IoHT environment by leveraging the complementary strengths of these neural network components. The proposed system is designed to be adaptable and efficient, providing a comprehensive solution to cyber threats' dynamic and evolving nature in IoHT, as presented in Figure 2. Trained on an extensive dataset of IoHT, this model is specifically designed to detect four distinct types of attacks. These include ARP spoofing, DoS, Nmap port scans, and Smurf attacks. The ANN component efficiently processes complex patterns inherent in IoHT data. The BLSTM layer captures bidirectional dependencies, while the

GRU layer excels in handling long-term sequential features. This integrated architecture enables the model to discern and classify diverse cyber threats within IoHT. As a result, it contributes to the security and integrity of healthcare data and services.
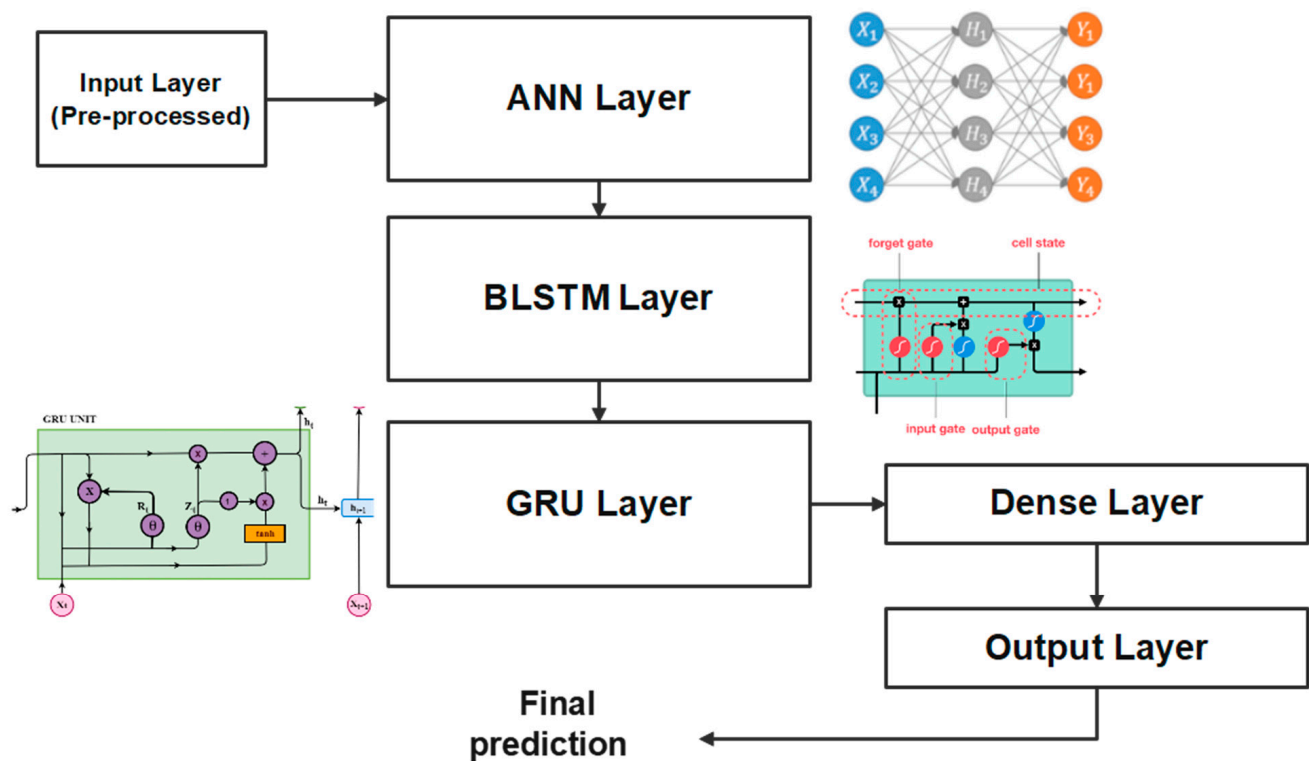

Figure 2. Hybrid deep learning-based IoHT attack detection model architecture.

The hybrid deep learning model outlined in the provided architecture incorporates multiple layers to harness the strengths of different types of neural networks, creating a comprehensive approach to classification tasks. The model starts with an input layer to receive pre-processed data, explicitly shaped based on the dimensions of the training data. It then splits into three separate paths: an ANN, a GRU, and an LSTM architecture.

The ANN layer consists of a dense layer with 256 neurons activated by ReLU, introducing non-linearity and allowing the network to capture complex patterns. The GRU layer includes a bidirectional GRU layer, which processes data in both forward and backward directions, improving the model's ability to learn long-term dependencies by considering past and future contexts. The LSTM layer begins with a reshaping layer to adjust the input dimensions, followed by a bidirectional LSTM layer to capture dependencies similar to GRUs, and includes a dropout layer to prevent overfitting by randomly omitting neurons during training.

The outputs from these layers are then combined and passed through a final dense layer with a softmax activation function, which generates a probability distribution over five classes suitable for multiclass classification tasks. This architecture leverages the strengths of both ANN and RNN components, aiming to effectively capture spatial and sequential features within the data, potentially enhancing performance in complex classification scenarios.

Table 1 summarizes the key parameters for setting up the hybrid deep learning model. Different parameter values are tested to find the best performance.

Table 1. The model setup.

Parameter	Value
Batch Size	256
Number of Epochs	100
Output Activation	Softmax
Loss Function	Categorical Cross Entropy
Optimizer	Adam
Learning Rate	0.001
Activation Function	ReLU

2.3. Performance Metrics

To assess the performance of the deep learning-based cyber-attack detection system in the IoHT environment, several key performance metrics are employed to measure its effectiveness. These metrics include the following:

Accuracy (ACC): Accuracy represents the ratio of correctly classified instances to the total number of instances and is a fundamental measure of overall system performance. It is calculated using the following equation:

$$\text{ACC} = (\text{TP} + \text{TN})/(\text{TP} + \text{TN} + \text{FP} + \text{FN}), \tag{1}$$

where:

- True positives (TP) are the instances correctly classified as attacks.
- True negatives (TN) are the instances correctly classified as normal.
- False positives (FP) are the instances incorrectly classified as attacks.
- False negatives (FN) are the instances incorrectly classified as normal.

Recall quantifies the system's ability to detect actual attacks correctly. It is computed as follows:

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}), \tag{2}$$

Precision measures the accuracy of the system in classifying detected attacks. The following formula determines it:

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}), \tag{3}$$

The F1-Score is the harmonic mean of precision and recall and provides a balanced measure of the system's performance:

$$\text{F1-Score} = (2 \times \text{Precision} \times \text{Recall})/(\text{Precision} + \text{Recall}), \tag{4}$$

Specificity is a critical metric in the context of classification problems, particularly in assessing the performance of a model in identifying negative cases for each category. Defined mathematically, specificity for a given class is expressed as:

$$\text{Specificity} = \text{TN}/(\text{TN} + \text{FP}), \tag{5}$$

The weighted average mean adjusts for class imbalances by assigning weights proportional to the class frequencies. The weighted average $\overline{X}$ is computed as:

$$\overline{X} = \frac{\sum_{i=1}^{n} W_i \cdot X_i}{\sum_{i=1}^{n} W_i}, \tag{6}$$

where x_i represents t the performance metric, including accuracy, precision, and recall for each class i, and W_i denotes the weight assigned to class i. The weights W_i is typically determined based on class frequencies relevant to the classification task, ensuring that each class contributes proportionally to the overall performance assessment.

Finally, we can compute the overall error rate for classification, which is related to accuracy.

$$\text{Error Rate} = 1 - ((TP + TN)/(TP + TN + FP + FN)). \tag{7}$$

These performance metrics are essential in evaluating the system's ability to detect cyber-attacks and assess their effectiveness in the IoHT environment. High accuracy, recall, precision, specificity, error rate, weighted average results, and F1-Score values indicate that the system can efficiently identify and classify attacks while minimizing false detections.

3. Results

This research introduces an innovative approach to address cyber threats against IoHT. The proposed IoHT attack detection model combines an ANN with BLSTM and GRU architectures to create a reliable defense mechanism. The integrated system is adaptable and efficient, capable of combatting cyber threats' dynamic and sophisticated nature within the IoHT environment. The model was extensively trained on IoHT data to detect four cyber-attack types: ARP spoofing, DoS attacks, Nmap port scans, and Smurf attacks. The ANN component efficiently processes intricate patterns in IoHT data, while the BLSTM layer captures bidirectional dependencies, and the GRU layer manages long-term sequential features. Together, this architecture empowers the model to identify and categorize various cyber threats accurately, safeguarding the integrity of healthcare data and services.

3.1. Multi-Classification Result Scenario

The multiclass classification results demonstrate great accuracy in detecting and classifying different types of attacks.

As detailed in Table 2, it is clear that our model has achieved outstanding results in detecting various cyber-attacks. For multiclass classification scenarios, the model achieved 100% specificity and accuracy while achieving a precision of 99.365%, a recall of 99.957%, and an F1-Score of 99.6604%, crucial for preventing unnecessary alarms and ensuring the seamless operation of IoHT devices.

Table 2. Multi-classification results for each class.

Class	Accuracy (%)	Specificity (%)	Precision (%)	Recall (%)	F1-Score
No Attack	100	100	99.365	99.957	99.6604
ARP Spoofing	100	100	100	100	100
Nmap Port Scan	100	100	100	100	100
Smurf Attack	99.86	99.55	99.987	99.807	99.897
DoS Attack	0.9944	99.44	100	100	100

As represented in Figure 3, the confusion matrix represents the true positive and false positive rates across different classifications. A noteworthy observation is the model's success in distinguishing between 'No Attack' instances and 'Smurf Attack' scenarios, with only 15 cases misclassified from a substantial dataset. It indicates the model's high sensitivity and specificity in operational environments.

The weighted average results in Table 3 show the model's overall performance with accuracy, precision, recall, and F1-Score above 0.9985, 0.997 specificity and 0.001439 error rate. The aggregate analysis ensures the model's consistent strength across various attack vectors, solidifying its role as a comprehensive solution for cybersecurity in the IoHT landscape.
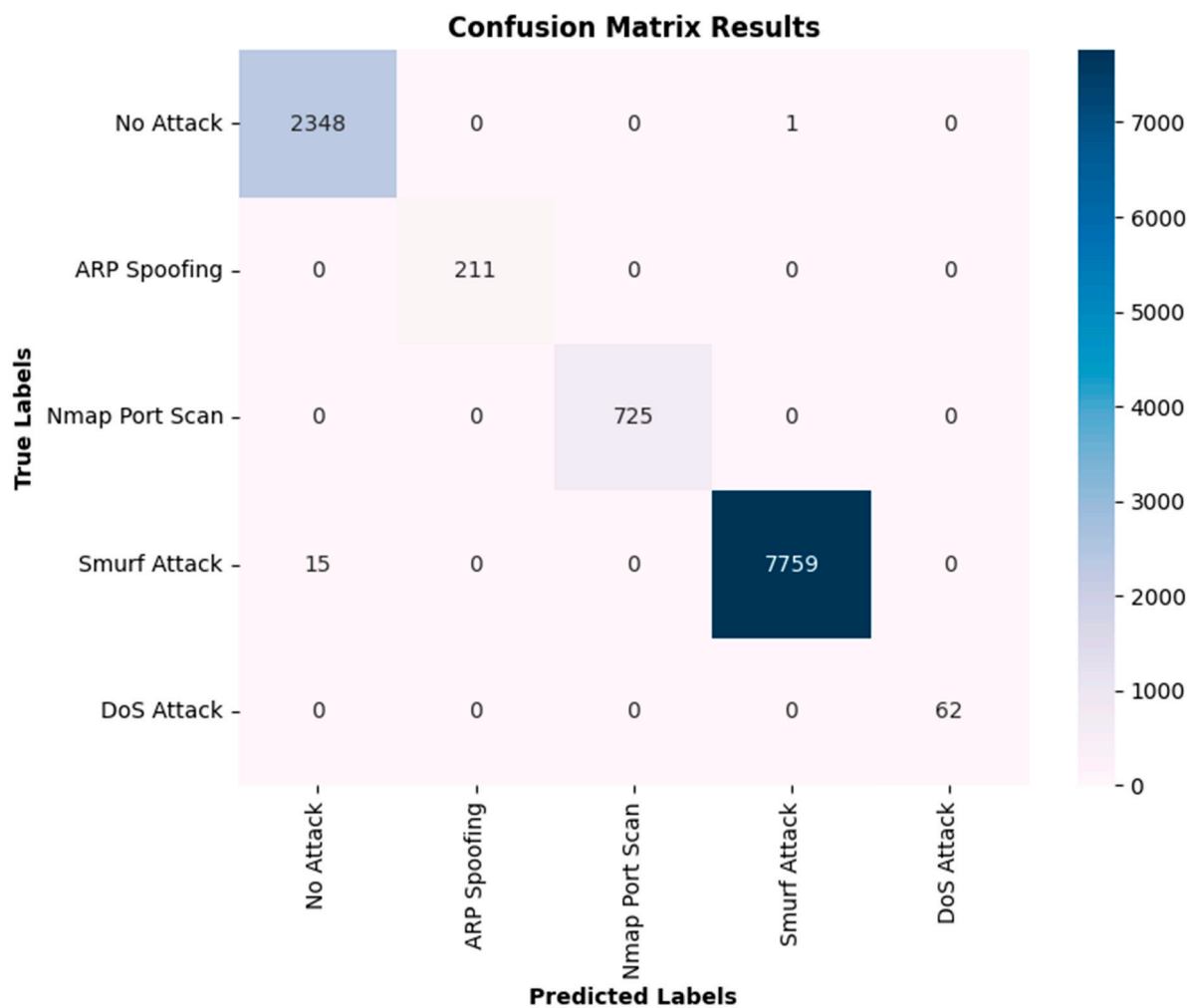
Confusion Matrix Results

Figure 3. Analysis of the confusion matrix multi-classification results.

Table 3. Weighted average multiclass classification results.

Metric	Value
Accuracy	0.998561
Specificity	0.996823
Precision	0.998569
Recall	0.998561
F1-Score	0.998563
Error Rate	0.001439

3.2. Binary Classification Result Scenario

Noteworthy progress in IoHT cybersecurity is the binary deep learning-based IoHT attack detection model. This innovative model provides a highly accurate method for identifying cyber threats within the IoHT infrastructure. While it employs a binary classification paradigm, which is less detailed than its multiclass equivalent, it is equally vital in preserving security. The model's primary function is to verify the existence or absence of cyber threats within the IoHT system. Table 4 details that the model's recall metric is significant, boasting a perfect 100% for both classes. Recall is a critical measure of the model's capacity to identify all genuine positives within the dataset. This achievement is most important for IoHT security, as the model identifies all legitimate threats.

The F1-Score of the model for both the 'No Attack' and 'Attack' classes achieved the optimal value of 100%. Since the F1-Score is a balanced average of precision and recall,

this indicates a perfect balance between avoiding false positives and detecting all true positives. This is an essential feature for security models, as the costs of false negatives can be significant.

The binary classification results, as shown in Table 5, demonstrate the model's exceptional performance. The model achieved 100% accuracy, specificity, precision, recall, and F1-Score, an excellent detection capability and 0 error rate. This consistency across all metrics indicates that the model is proficient in identifying the correct class labels and maintains this accuracy uniformly throughout the proposed dataset.

Figure 4 displays the binary classification confusion matrix, indicating a highly accurate predictive model for both 'Attack' and 'No Attack' scenarios. The dataset is composed of 11,121 instances, 2349 were classified as 'No Attack', and 8772 were classified as 'Attack'. The model performed correctly, with zero false positives or false negatives. The absence of off-diagonal values in the matrix confirms this. The model accurately predicted all 'Attack' instances (true positive rate) and all 'No Attack' instances (true negative rate). The scenario presented here demonstrates a binary classification framework with unparalleled perfection in cybersecurity for IoHT. It achieved a 100% success rate in detecting true threats and ensuring non-threat conditions, setting a theoretical benchmark for cybersecurity applications.
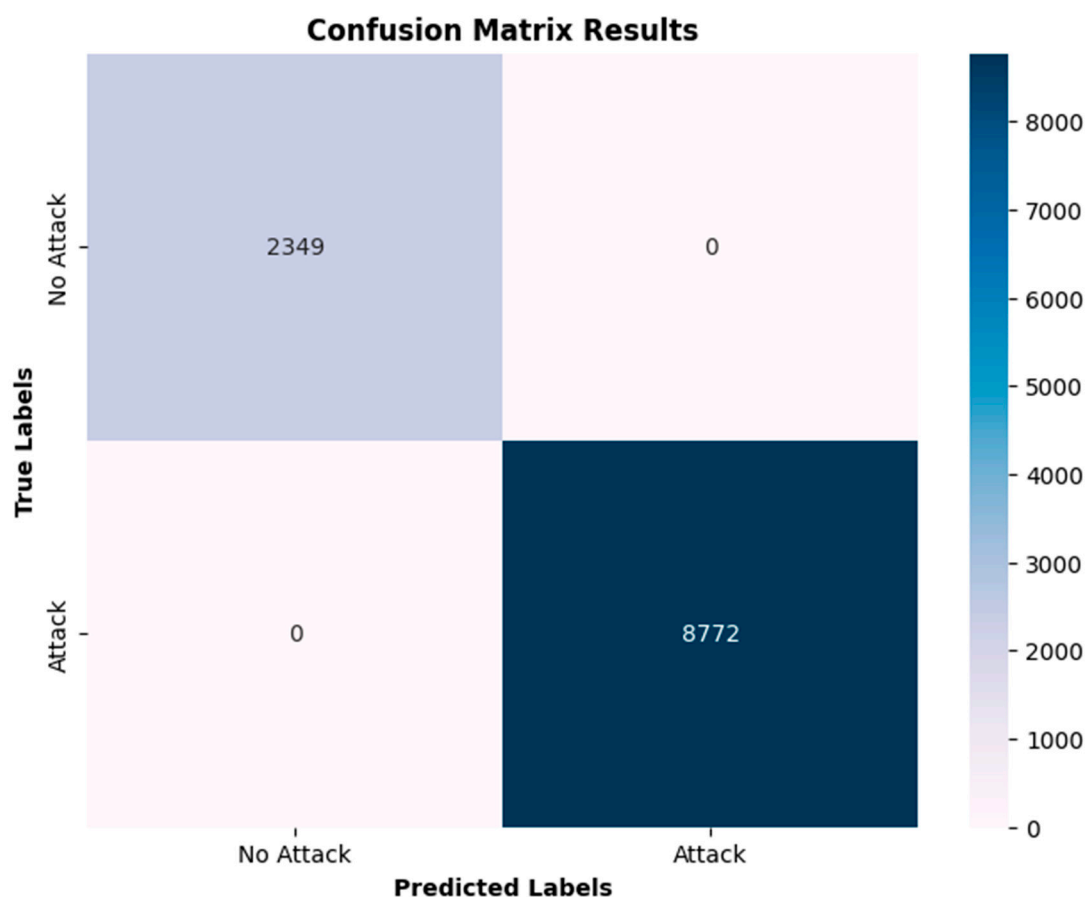

Figure 4. Analysis of the confusion matrix binary classification results.

Table 4. Binary classification results for each class.

Class	Accuracy (%)	Specificity (%)	Precision (%)	Recall (%)	F1-Score
No Attack	100	100	100	100	100
Attack	100	100	100	100	100

Table 5. Weighted average binary classification results.

Metric	Value
Accuracy	100
Specificity	100
Precision	100
Recall	100
F1-Score	100
Error Rate	0.0

4. Discussion

The results of our experimental evaluation of the hybrid IoHT attack detection model demonstrate a highly effective defense mechanism against cyber threats in IoHT. By integrating ANN with BLSTM and GRU architectures, our model achieved impressive results in both multiclass and binary classification scenarios, as evidenced by near-perfect accuracy, precision, recall, and F1-Score scores.

Our proposed model performed better than existing IDSs in the IoHT and IoT domains. While methodologies like LSTM with CNNs and various feature extraction methods combined with machine learning models offer high accuracy, they often need to provide complete coverage against many attacks, as shown in Table 6. For instance, the model in [10] has a mean accuracy of 93.74%, which, is notably lower than the 100% accuracy achieved by our model in a binary classification scenarios. Similarly, the hybrid approach employing CNN-BLSTM-GRU architectures, as reported in reference [16], achieves an accuracy of 99.25%, which is still lower than our model's multiclass accuracy of 99.86%.

Table 6. Comparative analysis of various existing IDSs based on the IoT and IoHT networks.

Ref.	Dataset Used	Methodology	Results
[9]	UNSW NB15	Hybrid approach (LSTM + CNN)	98% accuracy
[10]	25,000 instances	Four-layer deep Fully Connected network	Accuracy: 93.74%; precision: 93.71%
[11]	SDNIoT	LSTM for network assaults in IoT networks	Accuracy: 0.971
[12]	IEEE Dataport	Various feature extraction methods with ML models	VGG-16 with stacking: 98.3% accuracy
[13]	NID Dataset, BoT-IoT	CNN for anomaly-based IDS	Accuracy: 99.51% (NID), 92.85% (BoT-IoT)
[16]	IoT-based botnet	Hybrid deep learning (CNN-BLSTM-GRU) for IoT botnet detection	Accuracy: 98.34% (IoT-based botnet), 99.25% (CNN-BLSTM-GRU)
[17]	NSL-KDD	Deep learning for intrusion detection in social IoT	Accuracy from 96% to over 99%
[26]	ECU-IoHT	Deep neural network for cyber-attack detection ANN	Accuracy: 99.85%; Nmap port scan and DDOS recall: 92%,
[27]	wustl-ehms-2020, ECU-IoHT	DNN-FL for anomaly detection in IoHT data	Accuracy: 91.40% (wustl-ehms-2020), 98.47% (ECU-IoHT)
Proposed	ECU-IoHT	Hybrid IoHT detection model	Multiclass accuracy: 99.86; Binary class accuracy: 100. ARP spoofing, Nmap port scan, and DDOS recall: 100%.

The proposed model excels in its robustness and dynamic adaptability. The ANN component is critical in processing complex patterns in IoHT data, effectively filtering and identifying potential threats. Additionally, the BLSTM layer enhances the model's ability to understand bidirectional dependencies within the data, which is particularly useful for capturing evolving patterns. Moreover, including GRU layers helps manage long-term dependencies, enabling the model to maintain high performance even with extended data sequences typical in IoHT environments.

The model's high precision and recall metrics across all classifications demonstrate its accuracy and reliability, minimizing the risk of false positives and negatives. Such reliability is crucial in healthcare settings where patient data integrity and confidentiality are paramount. By accurately detecting and classifying cyber-attacks, the model supports the continuous availability and reliable performance of healthcare services, safeguarding sensitive health data against unauthorized access and potential tampering.

As shown in Figure 5, the proposed model obtained the best recalls, which confirms that it better detects abnormal instances of actual attacks compared to recent works.
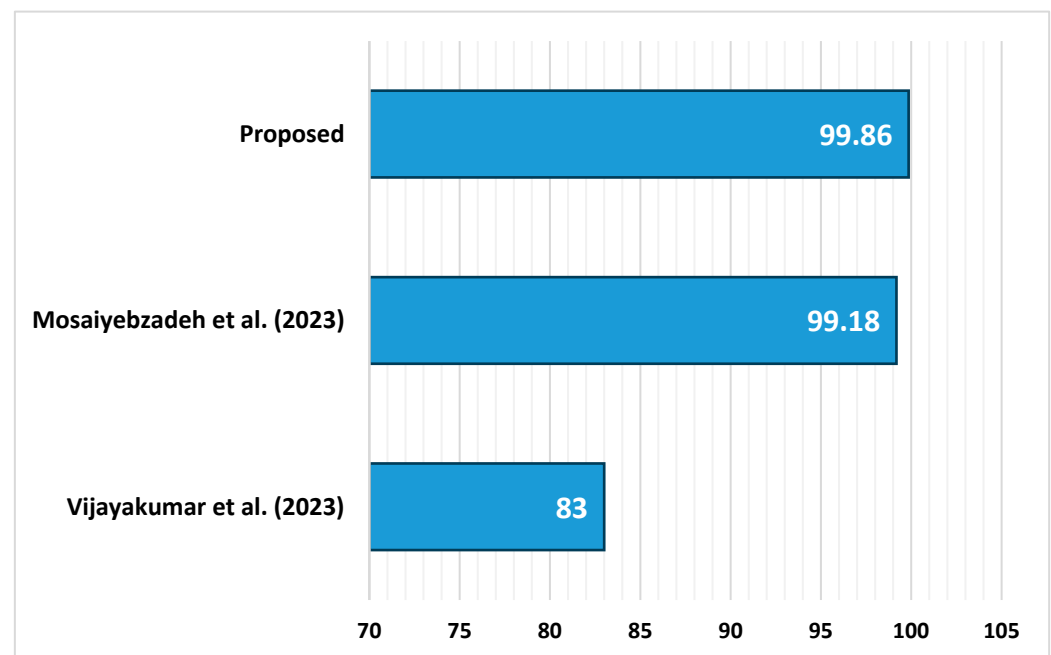
Figure 5. Comparison of recall results for different models. The references are as follows: Vijayakumar et al. (2023) [27], Mosaiyebzadeh et al. (2023) [28], and the proposed method.

Although the proposed model demonstrated high performance, its relatively lower precision in detecting Smurf attacks than other types of attacks highlight an opportunity for improvement. Possible avenues for future work include the integration of additional layers or alternative architectures that can enhance sensitivity to such attacks. In addition, continual learning mechanisms could be implemented to enable adaptation to new and evolving cyber threats without requiring extensive retraining.

The proposed model's success in IoHT environments adds to the ongoing discussion about the practicality of implementing deep learning techniques to safeguard IoT networks. By skillfully combining ANN, BLSTM, and GRU, this hybrid model showcases the potential of such approaches in addressing intricate and ever-changing security obstacles inherent in IoT systems.

This study showcases the effectiveness of advanced deep learning models in combating cybersecurity threats in the IoHT sector. The hybrid IoHT attack detection model's extraordinary performance establishes a new standard for IDSs in the IoT and IoHT realms, emphasizing the crucial role of innovative AI-based solutions in enhancing digital security in healthcare and beyond. Subsequent research should focus on strengthening and broadening the applicability of these models to other fields while continually improving their ability to adapt to the ever-changing cyber threat landscape.

5. Conclusions and Future Direction

The extensive research encapsulated in this paper has laid a foundational framework for a deep learning-based cybersecurity system in IoHT environments. This system leverages a hybrid deep learning-based IoHT attack detection model that integrates an ANN with BLSTM and GRU architectures.

The research's key findings highlight the proposed model's exceptional performance, achieving near-perfect precision, recall, and F1-Score metrics in both multiclass and binary classification scenarios. As presented in Table 1 and visually supported by Figure 3's confusion matrix, the multiclass classification results indicate a superior ability to detect and classify a broad range of cyber-attack types with minimal misclassifications. Similarly, the binary classification scenario detailed in Table 3 and Figure 4 demonstrates unprece-

dented performance, with accuracy, precision, recall, and F1-Score, all reaching the ideal value of 100%.

These findings represent a groundbreaking development in IDS for the IoHT landscape, with potential implications for patient safety and data security. The proposed model is reliable and efficient, setting a benchmark for future developments in the field.

Considering future directions, as IoHT devices and their cyber threats become more complex, there is a growing need for adaptive models that can learn from new attacks and evolve. Incorporating unsupervised learning techniques for anomaly detection within the proposed model could enhance its ability to detect novel threats not part of the original training dataset.

Author Contributions: For this research article, both authors contributed equally in all sections. Conceptualization, S.A.A. and S.S.A.; methodology, S.A.A.; software, S.A.A.; validation, S.A.A. and S.S.A.; formal analysis, S.S.A. and S.A.A.; writing—original draft preparation, review and editing, S.A.A. and S.S.A. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

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

References

1. Sestino, A.; Prete, M.I.; Piper, L.; Guido, G. Internet of Things and Big Data as Enablers for Business Digitalization Strategies. *Technovation* **2020**, *98*, 102173. [CrossRef]
2. Kamruzzaman, M.M. Key Technologies, Applications and Trends of Internet of Things for Energy-Efficient 6G Wireless Communication in Smart Cities. *Energies* **2022**, *15*, 5608. [CrossRef]
3. Sunyaev, A. The Internet of Things. In *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*; Springer International Publishing: New York, NY, USA, 2020; pp. 301–337.
4. Li, J.; Herdem, M.S.; Nathwani, J.; Wen, J.Z. Methods and Applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in Smart Energy Management. *Energy AI* **2023**, *11*, 100208. [CrossRef]
5. Olawale, O.P.; Ebadinezhad, S. The Detection of Abnormal Behavior in Healthcare IoT Using IDS, CNN, and SVM. In *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023*; Springer: Singapore, 2023; pp. 375–394.
6. Zoppi, T.; Ceccarelli, A.; Puccetti, T.; Bondavalli, A. Which Algorithm Can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection. *Comput. Secur.* **2023**, *127*, 103107. [CrossRef]
7. Injadat, M.; Moubayed, A.; Nassif, A.B.; Shami, A. Machine Learning towards Intelligent Systems: Applications, Challenges, and Opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3299–3348. [CrossRef]
8. Imran, M.; Haider, N.; Shoaib, M.; Razzak, I. An Intelligent and Efficient Network Intrusion Detection System Using Deep Learning. *Comput. Electr. Eng.* **2022**, *99*, 107764.
9. Smys, S.; Basar, A.; Wang, H. Hybrid Intrusion Detection System for Internet of Things (IoT). *J. ISMAC* **2020**, *2*, 190–199. [CrossRef]
10. Awajan, A. A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. *Computers* **2023**, *12*, 34. [CrossRef]
11. Chaganti, R.; Suliman, W.; Ravi, V.; Dua, A. Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks. *Information* **2023**, *14*, 41. [CrossRef]
12. Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. *J. Sens. Actuator Netw.* **2023**, *12*, 29. [CrossRef]
13. Saba, T.; Rehman, A.; Sadad, T.; Kolivand, H.; Bahaj, S.A. Anomaly-Based Intrusion Detection System for IoT Networks through Deep Learning Model. *Comput. Electr. Eng.* **2022**, *99*, 107810. [CrossRef]
14. Houda, Z.A.E.; Brik, B.; Khoukhi, L. "Why Should I Trust Your IDS?": An Explainable Deep Learning Framework for Intrusion Detection Systems in Internet of Things Networks. *IEEE Open J. Commun. Soc.* **2022**, *3*, 1164–1176. [CrossRef]
15. Yadav, N.; Pande, S.; Khamparia, A.; Gupta, D. Intrusion Detection System on IoT with 5G Network Using Deep Learning. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, e9304689. [CrossRef]
16. Kumar, A.K.; Vadivukkarasi, K.; Dayana, R. A Novel Hybrid Deep Learning Model for Botnet Attacks Detection in a Secure IoMT Environment. In Proceedings of the 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 9–11 February 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 44–49.

17. Diro, A.A.; Chilamkurti, N. Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]

18. Garg, A.; Singh, A.K.; Garg, M. Role of Internet of Things and Artificial Intelligence for Healthcare Informatics: An Overview. In *Innovations in Healthcare Informatics: From Interoperability to Data Analysis*; IET: London, UK, 2023; Volume 41, p. 107.

19. Mehta, R.; Prasad, V.K.; Mishra, S.; Tanwar, S.; Patel, Y. Evolving Technologies: IoT and Artificial Intelligence for Healthcare Informatics. In *Innovations in Healthcare Informatics: From Interoperability to Data Analysis*; IET: London, UK, 2023; Volume 41, p. 231.

20. Balas, V.E.; Kumar, R.; Srivastava, R. *Recent Trends and Advances in Artificial Intelligence and Internet of Things*; Springer: Cham, Switzerland, 2020; ISBN 3-030-32644-6.

21. Alshamrani, M. IoT and Artificial Intelligence Implementations for Remote Healthcare Monitoring Systems: A Survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 4687–4701. [CrossRef]

22. Verma, H.; Chauhan, N.; Awasthi, L.K. A Comprehensive Review of 'Internet of Healthcare Things': Networking Aspects, Technologies, Services, Applications, Challenges, and Security Concerns. *Comput. Sci. Rev.* **2023**, *50*, 100591. [CrossRef]

23. Ketu, S.; Mishra, P.K. Internet of Healthcare Things: A Contemporary Survey. *J. Netw. Comput. Appl.* **2021**, *192*, 103179. [CrossRef]

24. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]

25. Alkhudhayr, F.; Alfarraj, S.; Aljameeli, B.; Elkhdiri, S. Information Security: A Review of Information Security Issues and Techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.

26. 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]

27. Vijayakumar, K.P.; Pradeep, K.; Balasundaram, A.; Prusty, M.R. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. *Processes* **2023**, *11*, 1072. [CrossRef]

28. Mosaiyebzadeh, F.; Pouriyeh, S.; Parizi, R.M.; Han, M.; Batista, D.M. Intrusion Detection System for IoHT Devices Using Federated Learning. In Proceedings of the IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hoboken, NJ, USA, 17–20 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.

29. 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]