sustainability

MDPI

Article

A Sustainable W-RLG Model for Attack Detection in Healthcare IoT Systems

Brij B. Gupta [1,2,3,4,*], Akshat Gaurav [5], Razaz Waheeb Attar [6], Varsha Arya [7,8], Ahmed Alhomoud [9] and Kwok Tai Chui [10]

[1] Department of Computer Science and Information Engineering, Asia University, Taichung 413, Taiwan
[2] Department of Computer Science and Engineering, Kyung Hee University, 26 Kyungheedae-ro, Dongdaemun-gu, Seoul 02447, Republic of Korea
[3] Symbiosis Centre for Information Technology (SCIT), Symbiosis International University, Pune 412115, India
[4] Department of Electrical and Computer Engineering, Lebanese American University, Beirut 1102, Lebanon
[5] Computer Science and Engineering, Ronin Institute, Montclair, NJ 07043, USA; akshat.gaurav@ieee.org
[6] Management Department, College of Business Administration, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; raattar@pnu.edu.sa
[7] Department of Business Administration, Asia University, Taichung City 41354, Taiwan; varshaarya2108@gmail.com
[8] Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun 248007, India
[9] Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia; aalhomoud@nbu.edu.sa
[10] Department of Electronic Engineering and Computer Science, Hong Kong Metropolitan University (HKMU), Hong Kong; jktchui@hkmu.edu.hk
* Correspondence: bbgupta@asia.edu.tw

Abstract: The increasingly widespread use of IoT devices in healthcare systems has heightened the need for sustainable and efficient cybersecurity measures. In this paper, we introduce the W-RLG Model, a novel deep learning approach that combines Whale Optimization with Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU) for attack detection in healthcare IoT systems. Leveraging the strengths of these algorithms, the W-RLG Model identifies potential cyber threats with remarkable accuracy, protecting the integrity and privacy of sensitive health data. This model's precision, recall, and F1-score are unparalleled, being significantly better than those achieved using traditional machine learning methods, and its sustainable design addresses the growing concerns regarding computational resource efficiency, making it a pioneering solution for shielding digital health ecosystems from evolving cyber threats.

Keywords: sustainable cybersecurity; healthcare IoT systems; whale optimization algorithm; deep learning models; attack detection

check for updates

Citation: Gupta, B.B.; Gaurav, A.; Attar, R.W.; Arya, V.; Alhomoud, A.; Chui, K.T. A Sustainable W-RLG Model for Attack Detection in Healthcare IoT Systems. *Sustainability* **2024**, *16*, 3103. https://doi.org/10.3390/su16083103

Academic Editors: Ruben Pereira and Isaias Bianchi

Received: 19 February 2024
Revised: 28 March 2024
Accepted: 3 April 2024
Published: 9 April 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, healthcare systems have become increasingly reliant on IoT devices. The integration of wearable IoT devices and mobile applications has substantially enhanced the value of healthcare services, enabling more effective health data exchange, accurate diagnosis, and rapid treatment [1]. This trend is driven by IoT devices' potential to provide personalized and efficient healthcare solutions, including wearable devices for smart healthcare, wireless health monitoring, and ubiquitous electronic healthcare systems [2]. As the number of IoT devices continues to increase, ensuring the availability of necessary resources and services for emerging IoT-based healthcare applications remains an ongoing challenge [3].

The adoption of IoT in healthcare is also influenced by privacy concerns, user data sensitivity, and the need for secure and scalable data transmission [4,5]. The scarcity of

healthcare resources and the increasing population have made IoT a cost-effective and efficient solution for addressing patients' needs [6,7]. However, the low adoption of IoT applications among end users in healthcare indicates that there are still barriers to overcome before IoT can be fully integrated into healthcare systems [8]. Security is a critical consideration in the adoption of IoT in healthcare, and it is necessary to address security issues such as authentication, data protection, and privacy in IoT-enabled healthcare systems [9,10]. The potential for malicious attacks and the need for fault-tolerant data management schemes emphasize the importance of implementing robust security measures in IoT healthcare environments [11,12].

IoT has vast potential in healthcare, with applications ranging from smart healthcare surveillance frameworks to healthcare assessment, patient monitoring, and automatic detection of specific conditions [13,14]. It will revolutionize the industry by enabling efficient resource utilization, enhancing the accuracy and reliability of electronic devices, and improving the quality of healthcare services while reducing costs [15,16]. In conclusion, the increasing reliance on IoT devices in healthcare systems is driven by the potential for personalized and efficient healthcare solutions, the need to address privacy and security concerns, and the potential for cost-effective and scalable healthcare services. However, challenges such as low adoption rates and security issues must be addressed to fully realize the prospects of IoT in healthcare.

Security attacks pose significant risks for IoT devices in healthcare systems, enabling unauthorized access, data breaches, system downtime, and other vulnerabilities that compromise patient privacy and safety Obaid and Salman [17], Kaushik and Gandhi [18]. The limited processing capacity and limited battery life of IoT devices in healthcare systems often affect security architecture, resulting in security breaches [19]. Furthermore, replay, sniffing, eavesdropping, and version number and rank attacks can degrade network communication and compromise the integrity of healthcare data [15,20].

The unique specifications of IoT technology in healthcare, including massive amounts of data, large numbers of cloud-computing servers, and significant number of users, can all lead to security issues [21]. Additionally, ensuring the confidentiality of Electronic Health Records (EHR) and privacy are crucial requirements for healthcare systems, emphasizing the need for robust security measures [22].

The expansion of IoT in healthcare has introduced new vulnerabilities, risks, and security challenges for healthcare practitioners and patients, necessitating the development of efficient security risk management models [23]. Moreover, the large amounts of data collected/generated by wireless medical sensors must be protected from security attacks to ensure patient privacy and data integrity [24].

In order to address these security risks, researchers have focused on developing secure frameworks, intrusion detection systems, and lightweight security models for IoT-based healthcare systems [25,26]. Additionally, the integration of blockchain and deep reinforcement learning has been proposed to enable real-time security and energy-efficient healthcare services, particularly during pandemics such as COVID-19 [27].

Security attacks on IoT devices in healthcare systems present significant risks to patient privacy, data integrity, and overall system reliability. Addressing these challenges necessitates the development of robust security architectures, risk management models, and innovative security technologies to ensure the confidentiality and integrity of healthcare data. In this context, we present a sustainable deep learning-based cyber attack detection approach.

The rest of the paper is organized as follows: Section 2 presents the related work and Section 3 contains the details of our proposed approach, while Sections 4 and 5 contain the results and conclusion, respectively.

2. Related Work

The use of deep learning frameworks for attack detection in healthcare IoT systems has attracted significant attention due to the increasing complexity and frequency of cyber-attacks.

Several studies have proposed innovative approaches to leverage deep learning techniques to detect and mitigate security threats in IoT-based healthcare environments (Table 1).

The authors of Punith and Priya [28] introduced "DeepMIA", an integrated and accelerated approach for detecting malicious insider attacks in IoT using deep learning. This model utilizes deep learning to identify dangerous insider threats within the IoT context, showcasing the potential of deep learning in addressing such security risks.

Meanwhile, in Hussain et al. [11], the authors presented a framework for malicious traffic detection in IoT healthcare environments, demonstrating the application of different machine learning techniques, including deep learning, to develop an AI-based cybersecurity solution. This framework aims to defend IoT healthcare systems against cyber-attacks, highlighting the potential of deep learning in enhancing security measures.

Furthermore, Mishra and Pandya [29] discussed various machine learning and deep learning techniques for data pre-processing and malware detection, emphasizing the relevance of deep learning in anomaly detection and intrusion detection systems for IoT applications.The proposed frameworks offer promising solutions for enhancing the security of healthcare IoT systems, leveraging deep learning methods to detect and mitigate various security threats, including insider attacks, malicious traffic, and malware, thereby contributing to the development of robust security measures in IoT-based healthcare environments.

In their work, the authors of Rodríguez et al. [30] introduced a transfer-learning-based intrusion detection framework in IoT networks, utilizing deep learning to detect zero-day attacks. This approach showcases the potential of using transfer learning, knowledge transfer, and model refinement to address insider security risks. The authors of Khan and Akhunzada [31] introduced a highly scalable hybrid deep learning-driven intelligent SDN-enabled framework for efficient and timely detection of sophisticated IoMT malware, demonstrating the application of deep learning in enhancing security measures for Internet of Medical Things (IoMT) environments. Meanwhile, the authors of Alotaibi and Alotaibi [32] presented a stacked deep learning approach for IoT cyberattack detection, which allowed them to detect malicious traffic data targeting IoT devices. This method highlights the potential of deep learning in effectively identifying and mitigating security threats in IoT environments. In another work, the authors of Alsoufi et al. [33] conducted a systematic literature review of existing works using deep learning techniques for anomaly-based intrusion detection in IoT environments. In their study, W et al. [34] emphasized the prospective use of machine learning and deep learning techniques for detecting and preventing cyber intrusions on IoT devices using anomaly detection, highlighting the relevance of these techniques with regard to IoT security.

Table 1. Literature Review.

Paper	Methods Used	Practical Implications	Results	Contributions
[35]	Deep learning-based approach for network-based intrusion detection; cost-sensitive learning approach	Network intrusion detection for IoMT	95% accuracy on network features	Network-based intrusion detection in IoMT systems; integration of cost-sensitive learning
[36]	Centralized and federated transfer learning; CMTL algorithm	Improved cyber attack detection in healthcare	High-level accuracy; improved performance	Cyber attack detection for healthcare; developed CMTL algorithm
[37]	Hybrid ConvLSTM; retraining against adversarial attacks	Anomaly and adversarial content detection in healthcare monitoring	97% F1 score; 98% accuracy	Anomaly detection in healthcare monitoring; hybrid ConvLSTM technique
[38]	Logistic regression; ML and DL techniques	Intrusion detection for smart healthcare networks	Logistic regression model analysis	Lightweight CNN–bidirectional LSTM model; traffic flow classification

Table 1. *Cont.*

Paper	Methods Used	Practical Implications	Results	Contributions
[39]	Two-phase data preparation and DNN-based attack detection	Resilient cyber-attack detection for IoMT	High-performance accuracy; AUC; low false-positive rate	DNN-based cyber-attack detection for IoMT; high detection accuracy
[40]	CNNs, Bi-LSTMs	Improved cyberattack detection and avoidance	Highest positive metrics, lowest negative metrics	Hybrid DL model, Achieves strong positive metrics
[41]	IoT technology, RNNBiLSTM algorithm	Improved patient privacy and security in healthcare	99.16% accuracy	IoT-based IDS for healthcare, RNNBiLSTM strategy
[42]	Feasibility of deep learning in healthcare	Current applications of DL in healthcare	Feasibility and applications shown	Current implementations and applications of DL in healthcare
[43]	Logistic Regression, ML and DL techniques	IDPS for healthcare communications	Logistic Regression model analysis	DL techniques to improve patient monitoring, diagnosis, and drug development
[44]	Logistic regression, ML and DL techniques	High accuracy in detecting malicious programs	Machine learning using Android's Permission and API features	A machine learning method to detect malicious programs in healthcare
[45]	Network-based attacks and DL solutions	Importance of DL solutions for securing healthcare IoT	Critical review of network-based attacks	Importance of DL solutions for healthcare IoT security
[46]	ML techniques (RF, NB, KNN)	Architecture for detecting IoT attacks in smart healthcare	90% accuracy with KNN model	Architecture for detecting IoT attacks; comparison of ML classifiers
[47]	DL algorithms; conventional ML techniques	Disease prognosis and diagnosis in healthcare	Significance of DL in healthcare discussed	DL for disease prognosis and diagnosis and prevention of infectious diseases

3. Proposed Approach

3.1. Feature Selection

To address the challenges associated with feature selection within an extensive dataset comprising 52 attributes, a Random Forest algorithm was employed to ascertain the relative importance of each feature. This process enhances the model's performance by focusing on the most informative features while reducing the computational complexity and improving the model's sustainability. Figure 1 illustrates the ranked importance of the features, highlighting the top 20, including 'tcp.time_delta', 'tcp.checksum', and 'frame.time_relative', amongst others, as the most significant predictors for distinguishing between 'normal' and 'attack' classes.

The 'tcp.time_delta' feature was the most important, showcasing the critical role of time intervals between packets in detecting anomalous behavior. Similarly, 'tcp.checksum' and 'frame.time_relative' made substantial contributions to the model's predictive capabilities, reflecting the relevance of packet integrity and event timing in the context of attack detection. Other influential features such as 'tcp.window_size_value', 'tcp.hdr_len', and 'tcp.srcport' underscore the multifaceted nature of network traffic analysis in cybersecurity.

These top features, indicated by the bars extending furthest on the y-axis in Figure 1, represent a blend of TCP protocol characteristics, MQTT protocol-specific data, and frame attributes. Combining these features enables a nuanced approach to identifying potential security threats within IoT environments. This refined feature set not only enhances the model's accuracy but also aligns with our goal of developing a sustainable and efficient deep learning-based attack detection system.

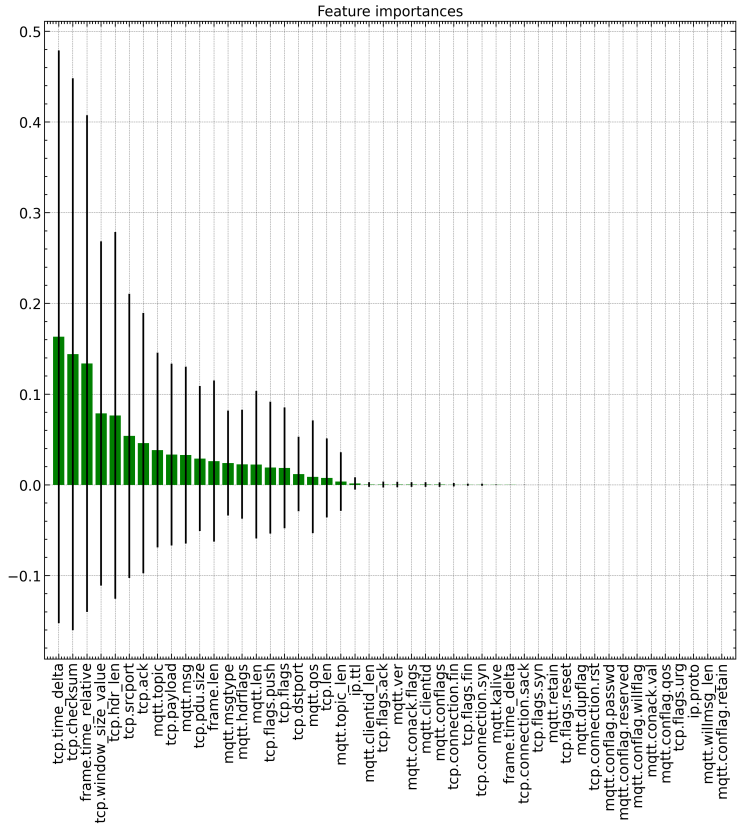


Figure 1. Feature ranking.

3.2. Proposed Model

In the Cascaded model (Figure 2), an input sequence passes through three recurrent neural network (RNN) layers: a simple RNN, an LSTM (Long Short-Term Memory), and a GRU (Gated Recurrent Unit). Here, we provide a brief explanation of how each layer operates, including the equations that govern their behavior:

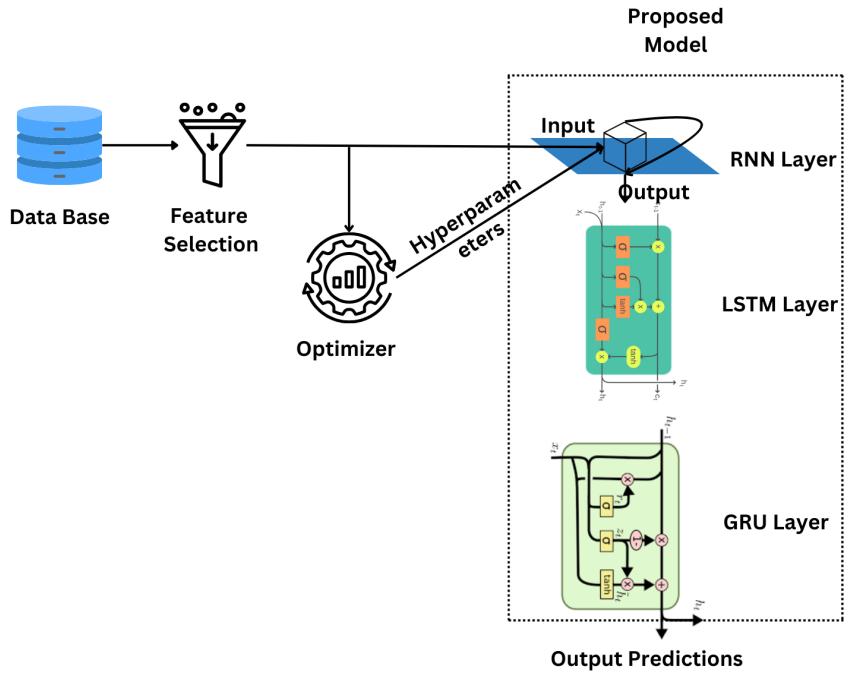


Figure 2. Proposed Model.

3.2.1. RNN Layer

The RNN layer processes the input sequence one element at a time by maintaining a 'hidden state' that captures information about the sequence seen so far. The simplest form of the RNN update for each time step t can be expressed as:

$$u_t = \tanh\left(V_{yu} y_t + d_{yu} + V_{uu} u_{t-1} + d_{uu}\right) \quad (1)$$

Here, u_t signifies the updated hidden state at timestep t, and y_t represents the input at the same timestep. The matrix V_{yu} is the weight matrix connecting the input to the hidden state, and d_{yu} is the bias associated with the input. Similarly, V_{uu} is the weight matrix for connections between the hidden state at the previous and current timestep, with d_{uu} being the corresponding bias. The activation function used here is the hyperbolic tangent function (tanh), which helps normalize the output between -1 and 1.

3.2.2. LSTM Layer

The LSTM layer is designed to overcome the vanishing gradient problem in traditional RNNs. It introduces 'gates' that regulate the flow of information. Each LSTM cell has an input gate, an output gate, and a forget gate. The equations for the LSTM updates are:

$$g_t = \phi(U_g \cdot [u_{t-1}, y_t] + c_g) \quad (2)$$
$$j_t = \phi(U_j \cdot [u_{t-1}, y_t] + c_j) \quad (3)$$
$$k_t = \phi(U_k \cdot [u_{t-1}, y_t] + c_k) \quad (4)$$
$$\widetilde{S}t = \tanh(U_S \cdot [ut - 1, y_t] + c_S) \quad (5)$$
$$S_t = g_t \odot S_{t-1} + j_t \odot \widetilde{S}_t \quad (6)$$
$$u_t = k_t \odot \tanh(S_t) \quad (7)$$

In these equations, ϕ denotes the sigmoid function. The variables g_t, j_t, and k_t are the activations for the forget gate, input gate, and output gate at time step t, respectively. S_t represents the cell state at time t, and u_t is the hidden state. The symbol $\odot$ represents element-wise multiplication, $[u_{t-1}, y_t]$ denotes the concatenation of the previous hidden state with the current input, and U_g, U_j, U_k, U_S, c_g, c_j, c_k, and c_S are the updated parameters of the model, including weight matrices and bias vectors.

3.2.3. GRU Layer

The GRU layer is similar to an LSTM but combines the input and forget gates into an update gate and merges the cell state and hidden state. The GRU's update equations are:

$$m_t = \sigma(Q_m \cdot [u_{t-1}, y_t] + c_m) \quad (8)$$
$$n_t = \sigma(Q_n \cdot [u_{t-1}, y_t] + c_n) \quad (9)$$
$$\widetilde{u}t = \tanh(Q \cdot [n_t \odot ut - 1, y_t] + c) \quad (10)$$
$$u_t = (1 - m_t) \odot u_{t-1} + m_t \odot \widetilde{u}_t \quad (11)$$

In this context, m_t represents the update gate, which determines the degree to which the network updates its state. The reset gate, denoted as n_t, controls how much of the past state is remembered. The candidate activation, $\widetilde{u}_t$, proposes a new state value that might be adopted depending on the influence of m_t. The final state for the current timestep, u_t, is a weighted sum of the previous state and the candidate state, as moderated by the update gate.

In the CascadedRNN class, the output of the RNN layer is used as the input for the LSTM layer, which in turn passes its output to the GRU layer. This creates a deep architecture that leverages the strengths of each RNN variant, allowing the capture of complex patterns in the sequence data.

Finally, the output from the GRU layer passes through a fully connected layer with a linear activation (implemented in self.fc) to obtain the final scores for classification. The final hidden state of the GRU layer (after the entire sequence has been processed) is used for this purpose, as it is assumed to contain information about the entire sequence.

4. Results and Discussion

4.1. Dataset Representation

To validate the effectiveness of the proposed sustainable deep learning attack detection model, a comprehensive dataset created by Kaggle [48] was utilized. This dataset was crafted to simulate a scenario reflective of an IoT-enabled Intensive Care Unit (ICU) comprising two beds. Each bed was observed by nine patient-monitoring devices and controlled by a dedicated Bedx-Control-Unit, all of which were generated through the IoT-Flock tool. The dataset encompasses two distinct classes, "attack" and "normal," with the "attack" class consisting of 80,126 instances and the "normal" class comprising 76,810 instances, as depicted in the dataset distribution chart (Figure 1). This balanced distribution is critical for training the deep learning model to accurately distinguish between normal operations and potential security threats.

The dataset encompasses a diverse range of data types, including floating-point numbers, integers, and categorical data, each contributing to a robust feature set for training the deep learning model. The features extracted from network traffic, such as'tcp.srcport', 'tcp.dstport', 'tcp.flags', and 'mqtt.msgtype', are integral to identifying patterns indicative of either normal behavior or cybersecurity threats. Moreover, the MQTT protocol-specific attributes in the dataset highlight the unique challenges associated with securing IoT environments, which often employ lightweight communication protocols that are vulnerable to various attack vectors.

The dataset contains 156,936 entries, each with 52 features that capture various aspects of network traffic and IoT device behavior. These features include time delta, packet length, source and destination IP addresses, TCP/UDP ports, MQTT protocol-specific data such as client ID and message types, and other protocol-specific flags and identifiers. The 'class' column categorizes each entry into the aforementioned classes, encoded as '1' for "attack" and '0' for "normal". Figure 3 illustrates the somewhat balanced nature of the dataset, which is crucial for mitigating any potential bias during the model training process.

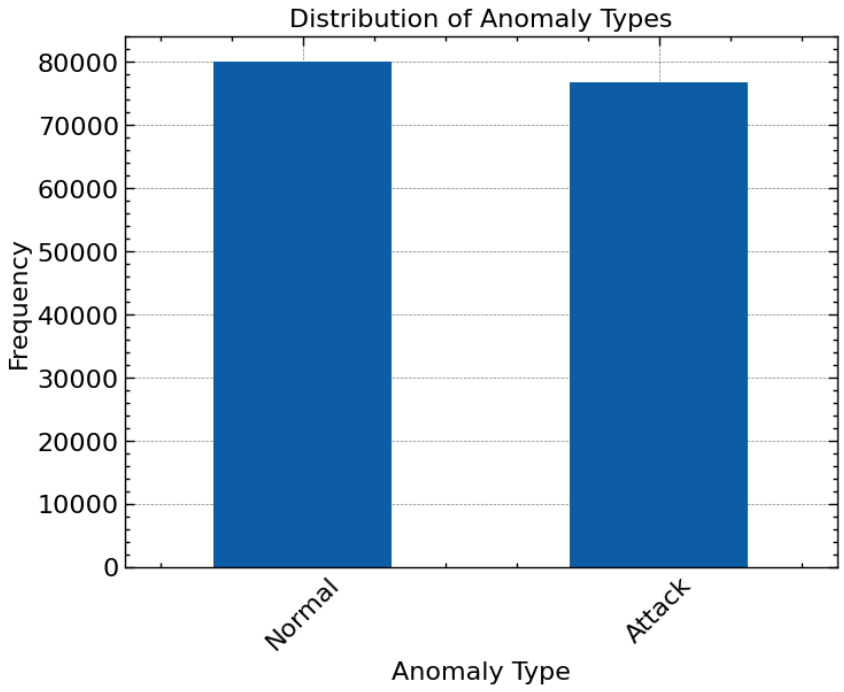
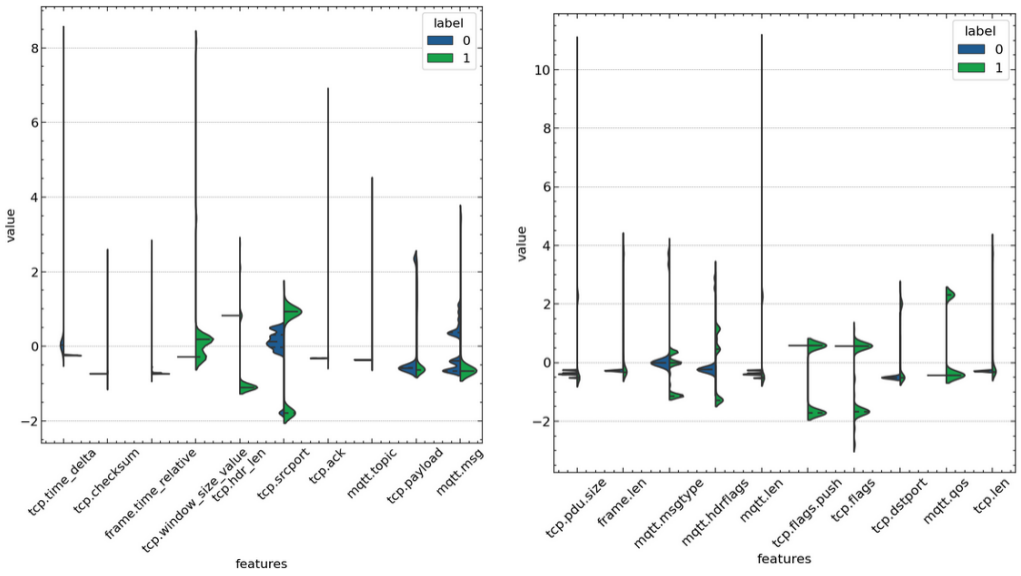


Figure 3. Distribution of labels.

After the feature selection, a detailed analysis of the feature distribution was conducted to ensure a more in-depth understanding of the data characteristics and the distinct patterns associated with each class label. Violin plots, which combine box plots with kernel density estimation, were employed for this purpose, providing a deeper insight into the distribution of values for each feature. Figure 4 presents the violin plots for the top 20 features, as determined by the Random Forest algorithm. These plots reveal the density of the data at different values, highlighting potential outliers and the skewness of the distribution.



(**a**) (**b**)

Figure 4. Violin Plot. (**a**) Violin plot of the first 10 features. (**b**) Violin plot of the last 10 features.

The violin plots underscore notable differences between the 'normal' (label 0) and 'attack' (label 1) classes across various features. For instance, 'tcp.time_delta' and 'tcp.len' demonstrate distinct peaks and variations in their distributions, suggesting a strong discriminatory power between normal and anomalous traffic patterns. Such visualizations are instrumental in validating the feature selection process and emphasize the relevance of each feature in the context of attack detection.

A comprehensive correlation analysis was conducted to evaluate the interdependencies among the top 20 features selected via the Random Forest algorithm. The resulting correlation matrix, as visualized in Figure 5, serves as an informative heatmap that elucidates the pairwise relationships between features. A correlation coefficient close to 1 or -1 indicates a strong positive or negative correlation, respectively, while a coefficient around 0 suggests that there is no linear correlation. As shown in the heatmap, certain features such as 'tcp.time_delta' and 'tcp.ack' exhibit a significant positive correlation, suggesting a possible interplay in their contribution to the model's decision-making process. Conversely, 'frame.time_relative' and 'tcp.checksum' demonstrate a noteworthy negative correlation, which could imply that these features independently contribute contrasting information for the classification task. The matrix also highlights the relationships between feature pairs and the target 'label', demonstrating how each feature may influence the detection of normal versus attack classes. For instance, 'tcp.time_delta' shows a substantial correlation with the 'label', reinforcing its relevance in detecting anomalies. This intricate web of relationships captured by the correlation matrix is pivotal to our understanding the multidimensional nature of the dataset, ensuring that the model leverages complementary features for robust attack detection.

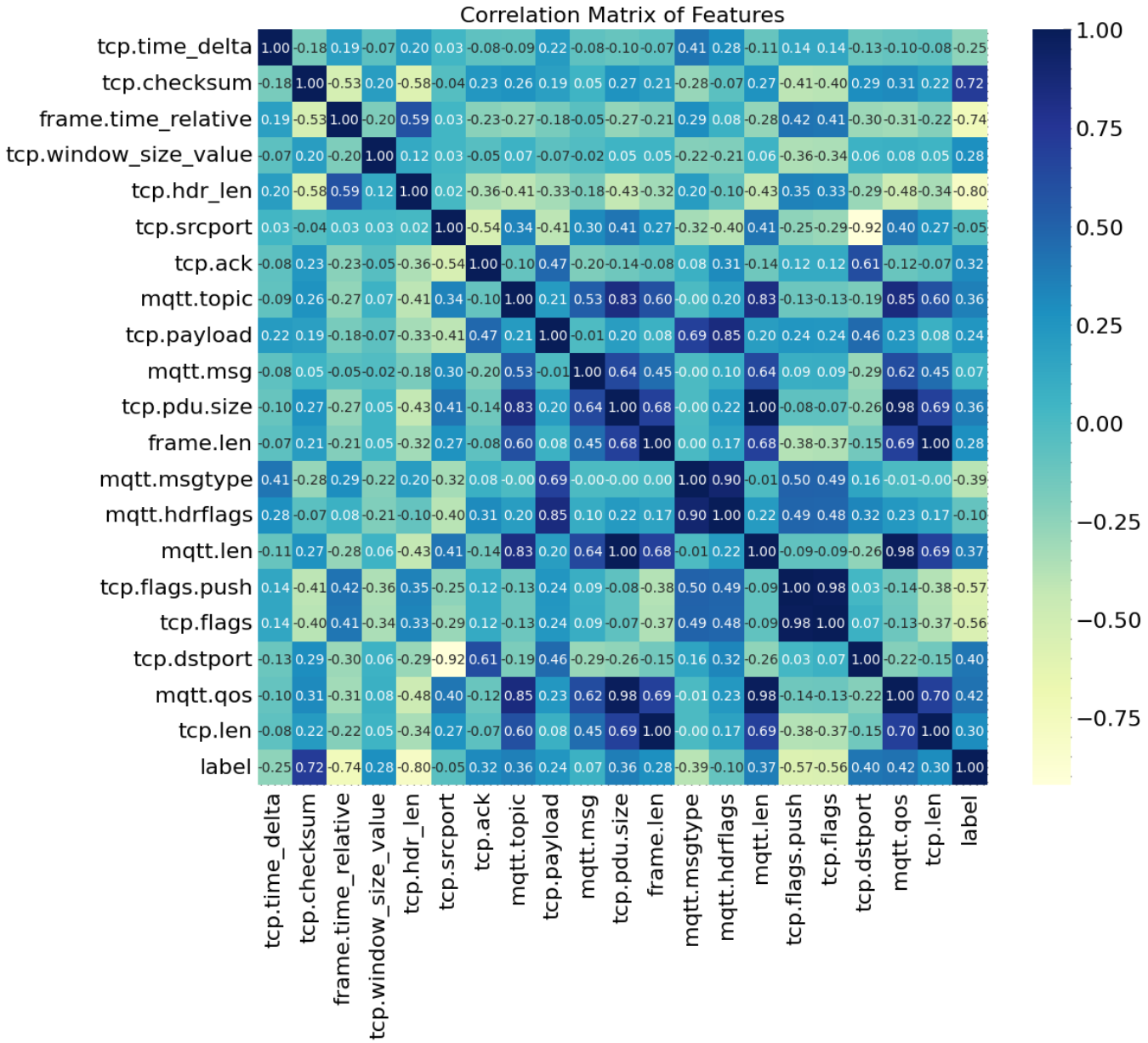


Figure 5. Correlation matrix of features.

4.2. Parameter Evaluation

Optimizing hyperparameters is a crucial step in deep learning, enabling enhancement of the model performance. In this study, the Whale Optimization Algorithm (WOA) was employed to fine-tune the hyperparameters of the combined RNN + GRU + LSTM model, targeting the optimal balance between complexity and performance. The WOA yielded an optimal learning rate of 0.0059398799743742604, with a configuration of 52 hidden units across two layers, achieving an outstanding 99.99 accuracy.

The training process across epochs is depicted in Figure 6, which showcases the loss and accuracy metrics for both the training and test datasets. Initially, a significant divergence between training and test loss was observed; however, as the training progressed, the model rapidly improved, showcasing the effectiveness of the learning. The training loss swiftly decreased from 0.071073 to 0.004515 within ten epochs, while the training accuracy improved from 97.19% to 99.93%. Test loss mirrored this trend, with an initial value of 0.479851 plummeting to an almost negligible 0.000025, followed by 100% accuracy in the final epoch.

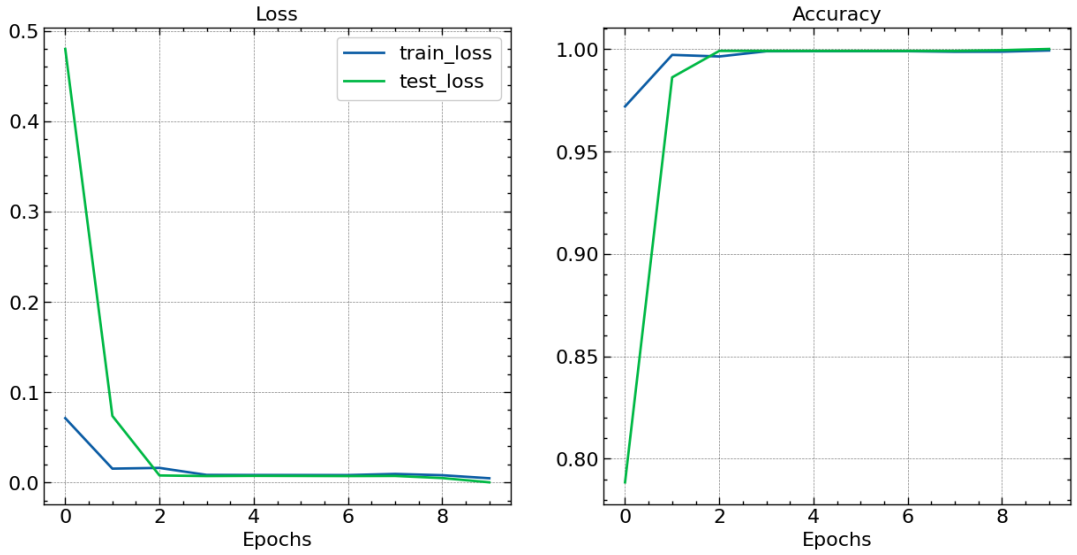


Figure 6. Accuracy and Loss Function.

The performance of the proposed deep learning model, after hyperparameter optimization, was rigorously evaluated using a classification report, which encompasses various metrics such as precision, recall, f1-score, and support for each class. As illustrated in Figure 7, the model achieved perfect precision, recall, and F1-scores of 1.00 for both 'Normal' and 'Attack' classes, correctly identifying each class with exceptional accuracy and without false positives or false negatives.

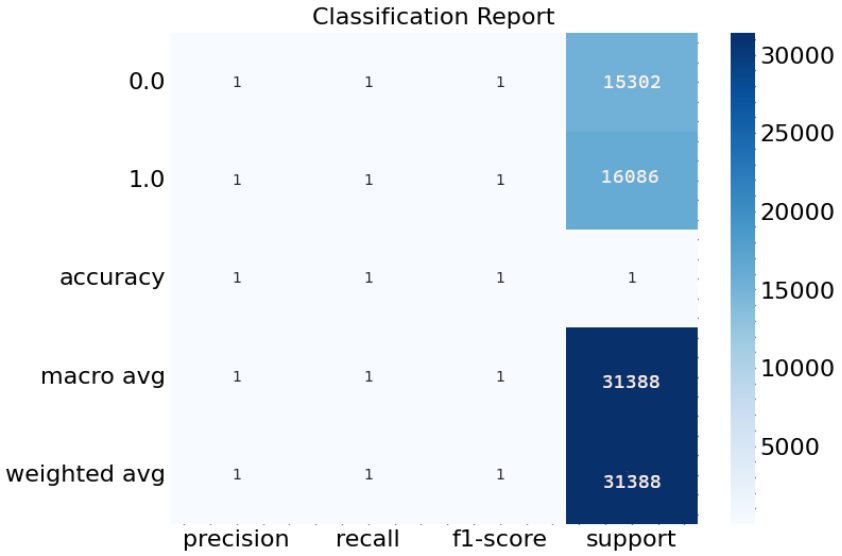


Figure 7. Classification report.

The support values, which represent the number of true instances for each label, were 15,302 for 'Normal' and 16,086 for 'Attack', with a total of 31,388 instances in the test dataset. The accuracy of the model stood at an impressive 100%, which is corroborated by the equally high macro and weighted averages across the precision, recall, and F1-score metrics.

This flawless performance, shown in deep blue in the heatmap of the classification report (Figure 7), underscores the model's ability to differentiate between the two classes with impeccable distinction. Such an outcome not only validates the efficacy of the Whale Optimization Algorithm in hyperparameter tuning but also demonstrates the potential of the RNN+GRU+LSTM ensemble in cybersecurity applications, particularly in the accurate detection of anomalous behavior in IoT environments.

The reliability of the predictive model was further substantiated by the confusion matrix, a pivotal tool in classification tasks which allows the performance of an algorithm to be visualized. The confusion matrix, depicted in Figure 8, provides a clear and concise representation of the perfect classification accuracy across the 'Normal' and 'Attack' categories, with no false positives or false negatives depicted. The model precisely identified all 15,302 instances of the 'Normal' class and 16,086 instances of the 'Attack' class without any misclassification.

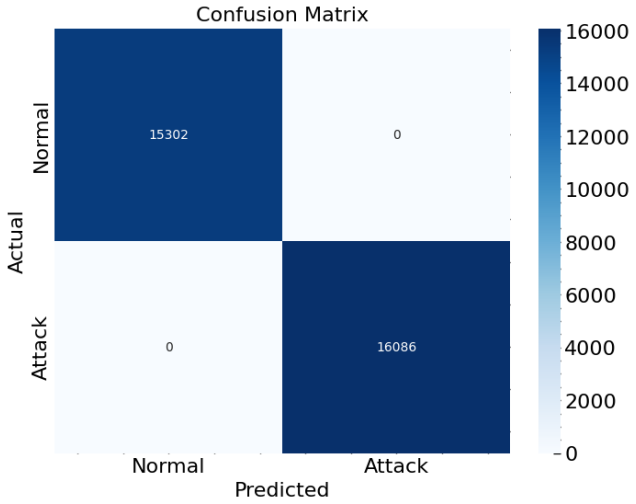


Figure 8. Confusion Matrix.

This impeccable result is signified by the deep blue squares along the diagonal of the matrix, with each square corresponding to the counts of true positive and true negative predictions. The lack of lighter squares or any color differentiation in the off-diagonal elements underscores the absence of false classifications, demonstrating the model's strong discriminatory power and its ability to generalize well when distinguishing between normal behavior and cyber-attacks within the IoT infrastructure.

4.3. Comparative Analysis

Our proposed model, a sophisticated assembly of Recurrent Neural Networks (RNN), Gated Recurrent Units (GRU), and Long Short-Term Memory (LSTM) networks, is markedly superior to traditional machine learning methodologies. As Table 2 illustrates, this cascaded approach excels in handling temporal dependencies and capturing long-term relationships inherent in sequential data, a feat that traditional RNNs, LSTMs, and GRUs can achieve individually, but to a lesser extent. In contrast, models such as Support Vector Machines (SVMs) and Decision Trees, despite their interpretability and lower computational demand, lack dynamic temporal processing capabilities, rendering them less suitable for intricate time-series tasks.

In our evaluation (Table 3), we conducted a comparative analysis against existing models, as detailed in the table. The BLSTM-RNN model proposed by McDermott et al. [49] achieved 97.5% accuracy, highlighting its effectiveness in the given context. Similarly, the DG-CNN technique introduced by Nguyen et al. [50] demonstrated 92% accuracy. The authors of Kumar and Lim [51] employed a KNN algorithm, achieving 94.5% accuracy, which showcased the versatility of traditional algorithms in modern applications. Meanwhile, in their research, the authors of Gao et al. [52] explored a Hybrid-ML approach, achieving 89.2% accuracy, indicating the potential of combining multiple machine learning techniques. The LSTM+RNN model created by Shi and Sun [53] achieved an impressive 99.3% accuracy, underscoring the strength of recurrent neural networks in processing sequential data. Recently, Liao and Guan [54] introduced the MCF-CBAM model, which achieved 99.66% accuracy, reflecting the advancements in model complexity and performance. Our proposed approach, utilizing the W-RLG technique, surpasses these models

with an unprecedented 99.99% accuracy, indicating its superiority in the applied context. This comparison underscores the significance of our proposed approach in pushing the boundaries of accuracy in the domain of interest.

Table 2. Comparative analysis.

Criteria	Proposed Model	RNN	LSTM	GRU	SVM	Decision Tree
Temporal dependency Handling	Excellent (cascaded layers enhance complexity handling)	Good	Excellent	Excellent	Poor (No temporal dynamics)	Poor (No temporal dynamics)
Ability to capture Long-term dependencies	Excellent (LSTM and GRU layers)	Poor	Excellent	Good	Not applicable	Not applicable
Training time	high (Due to model complexity)	Moderate	High	High	Low to moderate	Low
Model complexity	High (multiple stacked layers)	Low	Moderate	Moderate	Low to moderate (depends on the kernel)	Low
Parameter count	Very high (due to cascading layers)	Low	High	Moderate	Low to moderate	Low
Interpretability	Low (complex internal dynamics)	Moderate	Low	Low	Moderate to high (with linear kernels)	High
Risk of overfitting	Moderate (requires careful regularization)	High	Moderate	Moderate	Low to High (depends on kernel and regularization)	Moderate to High (without pruning)
Generalization on unseen data	Excellent (with proper tuning)	Moderate	Good	Good	Moderate to good	Moderate
Performance on small datasets	Moderate (might overfit)	Good	Moderate	Moderate	Good (with an appropriate kernel)	Good
Performance on large datasets	Excellent	Moderate	Good	Good	Varies	Good
Robustness to noise in data	High	Low	High	High	Moderate to high	Low to moderate
Computational resources required	High (needs significant GPU/CPU resources)	Moderate	High	High	Moderate to low	Low

Table 3. Comparison with the most recent work.

MODELS	Technique	Accuracy
[49]	BLSTM-RNN	97.5
[50]	DG-CNN	92
[51]	KNN	94.5
[52]	Hybrid-ML	89.2
[53]	LSTM+RNN	99.3
[54]	MCF-CBAM	99.66
Proposed Approach	W-RLG	99.99

While the parameter count and model complexity are significantly elevated in our stacked model, necessitating considerable computational resources, this investment is offset by the model's robustness to noise and exceptional generalization capabilities when tackling large datasets. Notably, the SVM and Decision Tree models, despite being quicker to train and easier to interpret, display inherent limitations in processing temporal data

and can suffer from overfitting if not meticulously regularized. Our model necessitates careful regularization to mitigate overfitting risks, a common challenge for such deep and complex networks.

5. Conclusions

The W-RLG Model, which integrates Whale Optimization with RNN, LSTM, and GRU, offers a sustainable solution for attack detection within healthcare IoT systems, addressing the need for sustainable cybersecurity. This study validates the model's exceptional efficacy, showcasing its near-perfect accuracy and superior precision, recall, and F1-scores. Its sustainable design minimizes computational demands, aligning with eco-friendly IT development goals. The results affirm the model's ability to efficiently defend healthcare data against cyber threats, marking a significant advancement in digital health security. Future work will explore scalability and real-world application, ensuring the W-RLG Model remains at the forefront of sustainable and effective cybersecurity solutions in the evolving landscape of healthcare technology.

Author Contributions: Methodology, A.G.; Formal analysis, B.B.G. and A.A.; Resources, K.T.C.; Visualization, V.A.; Supervision, R.W.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R 343), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024-1092-03".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data generated or analysed during this study are included in this published article.

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

References

1. Javed, L.; Yakubu, B.; Waleed, M.; Khaliq, Z.; Suleiman, A.; Mato, N. Bhc-iot: A survey on healthcare iot security issues and blockchain-based solution. *Int. J. Electr. Comput. Eng.* **2022**, *2*, 1–9. [CrossRef]
2. Alraja, M.; Farooque, M.; Khashab, B. The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the iot-based healthcare: The mediation role of risk perception. *IEEE Access* **2019**, *7*, 111341–111354. [CrossRef]
3. Kumhar, M.; Bhatia, J. Edge computing in sdn-enabled iot-based healthcare frameworks. *Int. J. Reliab. Qual. E-Healthc.* **2022**, *11*, 1–15. [CrossRef]
4. Princi, E.; Krämer, N. Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of iot healthcare devices. *Front. Psychol.* **2020**, *11*, 582054. [CrossRef] [PubMed]
5. Xu, Z.; He, D.; Vijayakumar, P.; Gupta, B.B.; Shen, J. Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical WSNs. *IEEE J. Biomed. Health Inform.* **2021**, *27*, 2334–2344. [CrossRef] [PubMed]
6. Dahri, A.; Massan, S.; Thebo, L. An overview of ai enabled m-iot wearable technology and its effects on the conduct of medical professionals in public healthcare in pakistan. *3c Tecnol. Glosas InnovaciónN Apl. Pyme* **2020**, *9*, 87–111. [CrossRef]
7. Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel Distrib. Comput.* **2021**, *153*, 150–160.
8. Alrawashdeh, M.; Keikhosrokiani, P.; Belaton, B.; Alawida, M.; Zwiri, A. Iot adoption and application for smart healthcare: A systematic review. *Sensors* **2022**, *22*, 5377. [CrossRef] [PubMed]
9. Khan, M.; Din, I.; Majali, T.; Kim, B. A survey of authentication in internet of things-enabled healthcare systems. *Sensors* **2022**, *22*, 9089. [CrossRef]
10. Yu, H.Q.; Reiff-Marganiec, S. Learning disease causality knowledge from the web of health data. *Int. J. Semant. Web Inf. Syst. (IJSWIS)* **2022**, *18*, 1–19. [CrossRef]
11. Hussain, F.; Abbas, S.; Shah, G.; Pires, I.; Fayyaz, U.; Shahzad, F.; García, N.; Zdravevski, E. A framework for malicious traffic detection in iot healthcare environment. *Sensors* **2021**, *21*, 3025. [CrossRef]
12. Xiao, J.; Liu, X.; Zeng, J.; Cao, Y.; Feng, Z. Recommendation of healthcare services based on an embedded user profile model. *Int. J. Semant. Web Inf. Syst. (IJSWIS)* **2022**, *18*, 1–21. [CrossRef]

13. Said, O.; Tolba, A. Design and evaluation of large-scale iot-enabled healthcare architecture. *Appl. Sci.* **2021**, *11*, 3623. [CrossRef]
14. Qi, J.; Yang, P.; Hanneghan, M.; Fan, D.; Deng, Z.; Dong, F. Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an internet of things environment. *IET Netw.* **2016**, *5*, 107–113. [CrossRef]
15. Li, J.; Jinjin, C.; Khan, F.; Rehman, A.; Balasubramaniam, V.; Sun, J.; Venu, P. A secured framework for sdn-based edge computing in iot-enabled healthcare system. *IEEE Access* **2020**, *8*, 135479–135490. [CrossRef]
16. Onyebuchi, A.; Matthew, U.O.; Kazaure, J.S.; Okafor, N.U.; Okey, O.D.; Okochi, P.I.; Taiwo, J.F.; Matthew, A.O. Business demand for a cloud enterprise data warehouse in electronic healthcare computing: Issues and developments in e-healthcare cloud computing. *Int. J. Cloud Appl. Comput. (IJCAC)* **2022**, *12*, 1–22. [CrossRef]
17. Obaid, O.; Salman, S. Security and privacy in iot-based healthcare systems: A review. *Mesopotamian J. Comput. Sci.* **2022**, *2022*, 29–40. [CrossRef]
18. Kaushik, S.; Gandhi, C. Capability-based access control with trust for effective healthcare systems. *Int. J. Cloud Appl. Comput. (IJCAC)* **2022**, *12*, 1–28. [CrossRef]
19. Shahrani, A.; Rizwan, A.; Chero, M.; Prado, C.; Salazar, E.; Awad, N. An internet of things (iot)-based optimization to enhance security in healthcare applications. *Math. Probl. Eng.* **2022**, *2022*, 6802967. [CrossRef]
20. Sarivougioukas, J.; Vagelatos, A. Fused contextual data with threading technology to accelerate processing in home UbiHealth. *Int. J. Softw. Sci. Comput. (IJSSCI)* **2022**, *14*, 1–14. [CrossRef]
21. Said, O. Lbss: A lightweight blockchain-based security scheme for iot-enabled healthcare environment. *Sensors* **2022**, *22*, 7948. [CrossRef] [PubMed]
22. Nazari, M.; Maneshi, A. Chaotic reversible watermarking method based on iwt with tamper detection for transferring electronic health record. *Secur. Commun. Netw.* **2021**, *2021*, 5514944. [CrossRef]
23. Salih, F.; Bakar, N.; Hassan, N.; Yahya, F.; Kama, N.; Shah, J. Iot security risk management model for healthcare industry. *Malays. J. Comput. Sci.* **2019,** *3*, 131–144. [CrossRef]
24. Yehia, L.; Khedr, A.; Darwish, A. Hybrid security techniques for internet of things healthcare applications. *Adv. Internet Things* **2015**, *5*, 21–25. [CrossRef]
25. Almalki, F.; Soufiene, B. Eppda: An efficient and privacy-preserving data aggregation scheme with authentication and authorization for iot-based healthcare. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5594159. [CrossRef]
26. Gurunathan, M.; Mahmoud, M. A review and development methodology of a lightweight security model for iot-based smart devices. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11* . [CrossRef]
27. Liu, L.; Li, Z. Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things. *IEEE Access* **2022**, *10*, 53640–53651. [CrossRef]
28. Punith, R.; Priya, D. Deepmia: An integrated and accelerated approach for malicious insider attack detection in iot using deep learning. *Int. J. Res. Appl. Sci. Eng. Technol.* **2022**, *10*, 1585–1593. [CrossRef]
29. Mishra, N.; Pandya, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access* **2021**, *9*, 59353–59377. [CrossRef]
30. Rodríguez, E.; Valls, P.; Otero, B.; Costa, J.; Verdú, J.; Pajuelo, M.; Canal, R. Transfer-learning-based intrusion detection framework in iot networks. *Sensors* **2022**, *22*, 5621. [CrossRef]
31. Khan, S.; Akhunzada, A. A hybrid dl-driven intelligent sdn-enabled malware detection framework for internet of medical things (iomt). *Comput. Commun.* **2021**, *170*, 209–216. [CrossRef]
32. Alotaibi, B.; Alotaibi, M. A stacked deep learning approach for iot cyberattack detection. *J. Sens.* **2020**, *2020*, 8828591. [CrossRef]
33. Alsoufi, M.; Razak, S.; Siraj, M.; Nafea, I.; Ghaleb, F.; Saeed, F.; Nasser, M. Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Appl. Sci.* **2021**, *11*, 8383. [CrossRef]
34. Regis Anne, W.; Kirubavathi, G.; Sridevi, U.K. Detection of iot botnet using machine learning and deep learning techniques. *Res. Sq.* 2023, *in press*. [CrossRef]
35. Ravi, V.; Pham, T.D.; Alazab, M. Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. *IEEE Internet Things Mag.* **2023**, *6*, 50–54. [CrossRef]
36. Chakraborty, C.; Nagarajan, S.M.; Devarajan, G.G.; Ramana, T.; Mohanty, R. Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method. *Acm Trans. Sens. Netw.* 2023, *in press*. [CrossRef]
37. Albattah, A.; Rassam, M.A. Detection of Adversarial Attacks against the Hybrid Convolutional Long Short-Term Memory Deep Learning Technique for Healthcare Monitoring Applications. *Appl. Sci.* **2023**, *13*, 6807. [CrossRef]
38. Sharma, A.; Rani, S.; Shah, S.H.; Sharma, R.; Yu, F.; Hassan, M.M. An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2419–2428. [CrossRef]
39. 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]
40. Premkumar, M.; Lakshmi, R.; Velrajkumar, P.; Priya, S.G.; Tanguturi, R.C.; Murali, S.; Sivaramkrishnan, M. Hybrid Deep Learning Model for Cyber-Attack Detection. In Proceedings of the 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 17–19 May 2023; pp. 1435–1441.
41. Jeyanthi, D.; Indrani, B. IoT-based intrusion detection system for healthcare using RNNBiLSTM deep learning strategy with custom features. *Soft Comput.* **2023**, *27*, 11915–11930. [CrossRef]
42. Hu, S. Deep Learning in Healthcare. *Highlights Sci. Eng. Technol.* **2023**, *57*, 279–285. [CrossRef]

43. Gnanasankaran, N.; Subashini, B.; Sundaravadivazhagan, B. Amalgamation of Deep Learning in Healthcare Systems. In *Deep Learning for Healthcare Decision Making*; River Publishers: Aalborg, Denmark, 2023; pp. 1–23.
44. Nong, M.; Chang, H.T.; Huang, L. Research on deep learning technology to detect malicious for healthcare system. *J. Mech. Med. Biol.* **2023**, *23*, 2340054. [CrossRef]
45. Mathew, A.T.; Mani, P. Strength of Deep Learning-based Solutions to Secure Healthcare IoT: A Critical Review. *Open Biomed. Eng. J.* **2023**, *17*, e187412072304060. [CrossRef]
46. Sharma, A.; Babbar, H.; Vats, A.K. Detection of attacks in smart healthcare deploying machine learning algorithms. In Proceedings of the 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 26–28 May 2023; pp. 1–6.
47. Aman; Chhillar, R.S. The Upsurge of Deep Learning for Disease Prediction in Healthcare. In Proceedings of the International Conference on Innovations in Data Analytics, West Bengal, India, 29–30 November 2022; pp. 511–518.
48. Hussain, F. IoT Healthcare Security Dataset. 2023. Available online: https://www.kaggle.com/datasets/faisalmalik/iot-healthcare-security-dataset (accessed on 18 February 2024).
49. McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
50. Nguyen, H.T.; Ngo, Q.D.; Le, V.H. IoT botnet detection approach based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018; pp. 118–122.
51. Kumar, A.; Lim, T.J. EDIMA: Early detection of IoT malware network activity using machine learning techniques. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 289–294.
52. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access* **2019**, *7*, 82512–82521. [CrossRef]
53. Shi, W.C.; Sun, H.M. DeepBot: A time-based botnet detection with deep learning. *Soft Comput.* **2020**, *24*, 16605–16616. [CrossRef]
54. Liao, N.; Guan, J. Multi-scale Convolutional Feature Fusion Network Based on Attention Mechanism for IoT Traffic Classification. *Int. J. Comput. Intell. Syst.* **2024**, *17*, 36. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.