electronics

MDPI

Article

Harris-Hawk-Optimization-Based Deep Recurrent Neural Network for Securing the Internet of Medical Things

Sidra Abbas [1], Gabriel Avelino Sampedro [2,3], Mideth Abisado [4], Ahmad Almadhor [5], Iqra Yousaf [6] and Seng-Phil Hong [7,*]

1 Department of Computer Science, COMSATS University, Islamabad 22060, Pakistan; sidraabbas@ieee.org
2 Faculty of Information and Communication Studies, University of the Philippines Open University, Los Baños 4031, Philippines
3 Center for Computational Imaging and Visual Innovations, De La Salle University, 2401 Taft Ave., Malate, Manila 1004, Philippines
4 College of Computing and Information Technologies, National University, Manila 1008, Philippines
5 Department of Computer Engineering and Networks, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia
6 International Institute of Science Arts and Technology, Gujranwala 52250, Pakistan
7 AI Advanced School, aSSIST University, 46 Ewhayeodae 2-gil, Fintower, Sinchon-ro, Seodaemun-gu, Seoul 03767, Republic of Korea
* Correspondence: sphong@assist.ac.kr

Abstract: The healthcare industry has recently shown much interest in the Internet of Things (IoT). The Internet of Medical Things (IoMT) is a component of the IoTs in which medical appliances transmit information to communicate critical information. The growth of the IoMT has been facilitated by the inclusion of medical equipment in the IoT. These developments enable the healthcare sector to interact with and care for its patients effectively. Every technology that relies on the IoT can have a serious security challenge. Critical IoT connectivity data may be exposed, changed, or even made unavailable to authenticated users in the case of such attacks. Consequently, protecting IoT/IoMT systems from cyber-attacks has become essential. Thus, this paper proposes a machine-learning- and a deep-learning-based approach to creating an effective model in the IoMT system to classify and predict unforeseen cyber-attacks/threats. First, the dataset is preprocessed efficiently, and the Harris Hawk Optimization (HHO) algorithm is employed to select the optimized feature. Finally, machine learning and deep learning algorithms are applied to detect cyber-attack in IoMT. Results reveal that the proposed approach achieved an accuracy of 99.85%, outperforming other techniques and existing studies.

Keywords: harris hawk optimizer; internet of medical things; cyber-attacks; machine learning; deep learning

Citation: Abbas, S.; Sampedro, G.A.; Abisado, M.; Almadhor, A.; Yousaf, I.; Hong, S.-P. Harris-Hawk-Optimization-Based Deep Recurrent Neural Network for Securing the Internet of Medical Things. *Electronics* **2023**, *12*, 2612. https://doi.org/10.3390/electronics12122612

Academic Editors: Cheng-Chi Lee and Elif Bilge Kavun

Received: 30 March 2023
Revised: 18 May 2023
Accepted: 8 June 2023
Published: 9 June 2023

1. Introduction

The healthcare industry is the foremost provider of revenue and employment, which is increasing daily [1]. A patient's diseases and abnormalities can only be diagnosed after going to a hospital for physical analysis. Ultimately, it increases the healthcare cost, and there need to be more healthcare facilities in rural and remote areas. Technology improves over time; the health condition of the patient can now be diagnosed and monitored using a miniaturized device such as a smartwatch, on-body sensors, or smart homes [2–4]. IoT technology enables intelligent identification, tracking, deployment, monitoring, and management in addition to data exchange and transfer by connecting anything to the internet utilizing a specific protocol and data sensor systems [5,6]. The IoT has sparked much interest in the Healthcare Information Technology (IT) community in recent decades. Though the healthcare industry is efficient, IoT provides many options to improve it [7,8]. Various networks can connect modern medical devices and sensors, giving access to

critical information regarding patients' situations. This information can be used for various things, such as improving the automation and mobility of the diagnostic and therapeutic procedure, remote patient monitoring, and predicting disease and recovery through a broader understanding of symptoms [9].

IoT-enabled devices are being employed in several medical disciplines, especially with the widespread use of wireless medical sensors, equipment, and robotic systems as part of the latest phase of digitalized healthcare called Healthcare 4.0. Early diagnosis, disaster situations, remote patient monitoring, and real-time checks have benefited from the Internet of Medical Things. Integrating medical equipment into the IoT has aided in developing the IoMT [10–12]. The IoMT can improve diagnostic accuracy, reduce errors, and minimize healthcare costs by allowing individuals to submit healthcare data to physicians via technology. Due to the effects of the global pandemic, COVID-19 has mandated that medical services be made available online to everyone in any remote area; limiting in-person medical advice will stop the virus from spreading [13–15].

Ensuring security becomes paramount when human lives are at risk, especially when accountability is placed on managing equipment and embedded systems in upcoming enterprises [16,17]. In recent years, the healthcare industry has increasingly become a prime target for cyber-criminals due to the vast amounts of sensitive personal and medical information stored within healthcare systems [18]. The rise of electronic health records (EHRs), telemedicine, and other digital healthcare technologies has made healthcare data more accessible [19]. However, it has also created new avenues for cyber-attacks. As a result, security is a significant issue that must be addressed entirely for IoT to achieve full adoption and exponential growth [20–22]. Furthermore, the security threats to these systems can result in significant issues [22–26]. For example, when a linked insulin pump receives an incapacitated command, it may deliver excessive insulin into the patient's bloodstream [27]. Lately, more intelligent cyber-attacks are being attempted and traditional security methods are no longer in effect. As a result, researchers have turned their attention to another aspect of defending systems from cyber-attacks [18,28,29].

Various machine- and deep-learning approaches have been proposed for the prediction of security threats on multiple datasets: TON-IOT [30–32], UNSW-NB15 [33], intrusion detection dataset [34–36], etc. However, these approaches lack performance and are limited in that they do not consider multi-label attack datasets [37]; malicious activities such as DDoS and ransomware, and removal of redundant and irrelevant features [31]; feature selection techniques for feature optimization [31]; or low accuracy [34,38].

The proposed methodology consists of three steps: first, pre-processing the dataset (one-hot encoding and data normalization); second, removing irrelevant features by using HHO; and third, applying a base classifier (RF and SVM), ensemble classifier (Bagging and Boosting), and deep learning techniques (RNN) for classification. This research makes the following contributions:

- This research proposed a new technique that constructs machine learning and deep learning techniques in combination with the HHO algorithm for detecting cyber-attacks in IoMT.
- HHO is used for feature selection due to its quick coverage ability; it also hardly gets stuck in local minima. It improves the model performance compared with other optimizers.
- Results reveal that the proposed approach attains an accuracy of 99.85%, outperforming other techniques and existing studies, and provides an efficient model for detecting cyber-attacks in IoMT devices, preventing serious issues between end-users.

The remainder of the research paper is organized as follows: Section 2 presents a literature review of machine learning and deep learning techniques for detecting cyber-attacks in IoMT. Section 3 provides the proposed approach for cyber-attack detection in IoMT. Section 4 demonstrates the experimental result and discussion. Section 5 includes the conclusion of the work and future work.

2. Literature Review

This section's literature review comprises the proposed secured models based on machine learning and deep learning algorithms.

2.1. Machine Learning Techniques

Several machine learning techniques deal with security problems in the Internet of Things medical devices. Authors in [30] presented the IoMT framework to detect cyber-attacks on medical devices. The novel IoMT framework was proposed to hybridize the ELM and Bayesian optimization. The proposed technique secures patient data by providing security to IoMT devices. The proposed hybridization technique was implemented on the ToN-IoT dataset, and the experimental results indicate that the best results are recall 0.990, precision 0.990, F1-score 0.990, F2-score 0.989, F-beta scores 0.986, and an AUC–ROC value of 0.870. Authors in [33] proposed the machine-learning-based intrusion detection system to detect IoT network attacks. In the first phase of the proposed technique, the features were scaled to control the information leakage. This dataset combines nine attacks, including network traffic group activities and recent attacks. In the last phase, machine learning models are used for analysis. The proposed technique achieved the best results with an accuracy of 99.9% and MCC of 99.97%. The Principal Component Analysis (PCA) technique limits dimensionality in the next phase.

The novel Smart Healthcare Checker (Checker) framework was proposed for threat analysis in [37]. The proposed framework identifies the potential attacks and the corresponding effect of the IoMT Smart Healthcare Systems (SHS). Machine learning techniques such as DT, LR, ANN, DBSCAN, and K-means were implemented on the synthetic and UQVS dataset and achieved the best results regarding accuracy, precision, recall, and f1-score with values of 0.97, 0.92, 0.93, and 0.92, respectively. Authors in [39–41] proposed frameworks based on cloud cyber-attack detection and other tasks on the cloud. Authors in [31] combined the NB, DT, and RF in the first phase of the proposed framework design. The second phase used the classification result of XGBoost to identify the attacks. The third phase presented the fog-cloud-based deployment architecture [42]. The proposed framework was implemented on the ToN-IoT dataset. The experimental result indicates that the proposed framework achieved an accuracy of 96.35%, a detection rate of 99.98%, and decreased the false alarm rate by up to 5.59%.

Authors in [43] introduced an automated approach for detecting cybersecurity attacks in the healthcare environment. The proposed approach utilized Recursive Feature Elimination (RFE) in conjunction with Multilayer Perceptron (MLP) optimization to enhance the accuracy and efficiency of attack detection. RFE was employed to select the most relevant features from the dataset, reducing dimensionality and eliminating noise, which improves the detection algorithm's effectiveness. MLP optimization refines the neural network architecture, enhancing its ability to learn and classify attack patterns accurately. The experimental results demonstrated that using RFE and MLP significantly improves the attack detection accuracy, outperforming traditional detection methods. The researchers in [44] presented an approach to detect cyber-attacks in IoMT via secure ensemble learning. Furthermore, the fog-cloud framework distributes the computation and storage tasks between fog nodes and cloud servers, optimizing resource utilization and minimizing response time. This distributed architecture enables real-time detection and response to cyber-attacks, ensuring the timely protection of IoMT systems. The proposed system achieved high detection accuracy and low false alarm rates.

2.2. Deep Learning Techniques

Authors in [5] proposed the classification model constructed on RNN and machine learning algorithms to classify unexpected cyber-attacks. The proposed model outperforms similar models with an accuracy of 99.76%. Authors in [38] proposed different deep learning models for the intrusion detection system to expose interrupting tasks in the computing

environment. The proposed model was implemented on the UNSW-NB15 dataset and achieved an accuracy of 99.26%.

Authors in [34] proposed the Instruction Detection System and Prevention System (IDPs) to protect healthcare communication. Conventional healthcare systems usually adopted HTTP, while IoMT adopted TCP, an industrial protocol. The results indicate that the proposed system IDPS achieved an accuracy of 0.831 and a mitigation accuracy of 0.923. Authors in [20] proposed a framework to detect IoMT malware. Hybrid approaches are Convolutional Neural Network (CNN)–Long Short-Term Memory (LSTM), CNN–Gated Recurrent Unit (GRU), and GRU-LSTM; CNN-LSTM performed well with 99.83% accuracy on the IoT dataset with a lower time complexity of 1.2 s. A Hybrid PCA-GWO technique with a DDN classifier model was proposed for analyzing the pounce using the kaggle dataset. The hybrid approach was used to reduce redundant features and extract them for classification. Machine learning and deep learning techniques—KNN, NB, RF, SVM, and deep neural networks—were used with a hybrid approach and their performance in terms of accuracy increased by 15% [45]. Authors in [46] focused on applying deep learning techniques for detecting Distributed Denial-of-Service (DDoS) attacks in the IoT framework. They proposed a deep-learning-based detection method that utilized a CNN architecture to extract optimal features from network traffic data. The experimental results revealed that the proposed approach achieved a higher accuracy in detecting DDoS attacks in IoT networks. The method's ability to automatically learn discriminative features from raw network traffic data enables it to effectively identify anomalous patterns associated with DDoS attacks. Moreover, the deep-learning-based approach exhibits robustness against various attack scenarios, showcasing its potential for real-world deployment.

Authors in [47] designed a deep-learning-based architecture to capture both spatial and temporal dependencies in network traffic data, enabling the detection of complex and evolving intrusion patterns. The DCNN component extracts high-level spatial features from network data using convolutional layers, while the BiLSTM component captures sequential dependencies by processing the data bi-directionally. By utilizing parallel processing capabilities and optimizing memory usage, the IDS efficiently handles large-scale network traffic, making it suitable for real-time intrusion detection in high-speed networks. Authors in [48] proposed an ensemble of deep learning models to hunt cyber threats in the Industrial Internet of Things (IIoT). The proposed model combines multiple deep learning algorithms to enhance the detection and classification of cyber threats in IIoT environments. The ensemble model comprises CNN, LSTM, and Autoencoder (AE) models that are trained and integrated into a single model. The model is designed to capture spatial and temporal dependencies in IIoT data, enabling the detection of complex and evolving cyber threats. The results revealed that the model outperforms individual deep learning models, achieving high detection accuracy.

Some gaps can be used for identifying security threats in IoMT devices, such as ensemble classifiers and deep learning approaches; multiple datasets can be used for checking the extrapolation of these techniques, such as BoT-IoT and UNSWNB-15; and feature selection techniques for feature optimization to remove irrelevant and repeated features can be used so that a multi-classification label attack can be identified.

3. Proposed Methodology

This section explains the proposed approach and algorithms for classifying cyber-attacks in IoMT devices. The proposed approach has the following phases: Select the dataset. In the second pre-processed dataset, the third phase applies the feature selection algorithm HHO to remove the redundant or irrelevant features. Lastly, machine learning (RF, SVM, Bagging, and Boosting) and deep learning algorithms (RNN) are applied to compare the proposed approach. The proposed approach is explained in Figure 1.

Figure 1. Proposed approach for cyber-attack detection in IOMT environment.

3.1. Experimental Dataset

The Network Security Layer–Knowledge Discovery Database (NSL-KDD) dataset served as the input for this investigation [49]. Tavallaee et al. presented the NSL-KDD dataset after criticizing the underlying issues with KDD'99, as machine learning techniques are inclined to understand high-frequency attacks; KDD'99 has a lot of duplicate data, which can impair test-process assessment findings and restrict it from rare instruction records, which are typically more harmful to networks. The NSL-KDD dataset includes 41 features of the network stream and label that show the classes of attack or regular.

3.2. Dataset Preprocessing

The dataset is preprocessed using two techniques: one-hot encoding and data normalization. Any raw data must first be encoded, a starting phase in the pre-processing process. The method of "one-hot-encoding" is frequently used when working with categorical data [50]. Compared with other encoding methods, label encoding is more straightforward, although some numerical values might be misinterpreted due to specific problems with the order by the algorithm [45]. In consequence, the ordering problem is addressed by one-hot encoding. One-hot encoding defines a binary representation of a nominal feature in which a categorical value is replaced with a binary value for every distinct nominal value. The protocol type in a used dataset, such as in our case, is encoded into three binary variables: TCP (1, 0), UDP (0, 1), and ICMP (0, 1). The benefit of data normalization is that it can make some machine learning algorithms run faster. According to the authors in [51], the mean range [0, 1] and statistical normalization are typically the two attribute normalization techniques most effective for NSL-KDD preprocessing. Z-score normalization is employed to get all values in our model into the [0, 1] range. After applying pre-processing techniques such as one-hot encoding (on protocol type, TCP, UDP, and ICMP) and data normalization (applied on all features to get all values in the range of 0 and 1), the full features in the NSL-KDD dataset are 117 instead of 41. Then, HHO is applied with machine learning (ML) algorithms for feature selection.

3.3. Harris-Hawk-Optimization-Based Feature Selection

Feature selection is a significant step of pre-processing for performing classification tasks. To achieve effective learning, feature selection (FS) is a technique for selecting and removing a subset of essential attributes from a large amount of redundant and unnecessary information [52]. Feature selection is an approach for deleting unrelated and unnecessary features to improve the training result in detecting learning performance and model project duration [53]. Feature selection can help remove some computations in contrast to replica complexity [54]. We use HHO for feature selection.

HHO is a latterly developed metaheuristic algorithm that draws inspiration from swarm intelligence. Heidari et al. suggested it in 2019 [55] to emulate the behavior of Harris Hawks in the wild, who use unique pursuit techniques to capture their prey. HHO is categorized as a population-based algorithm in which a group of hawks work together while pursuing prey in various ways. There are two main phases of the Harris Hawk—namely, exploitative and explorative—in which hawks plan to find the target, jump abruptly, and use various attack strategies [56]. The HHO algorithm can be used to

implement any optimization problem. The primary working exploitation and exploration phases are illustrated in Figure 2, which depend on the prey energy level (E) and activity chances (q and r). Further details of these activities' chances are given in [55].

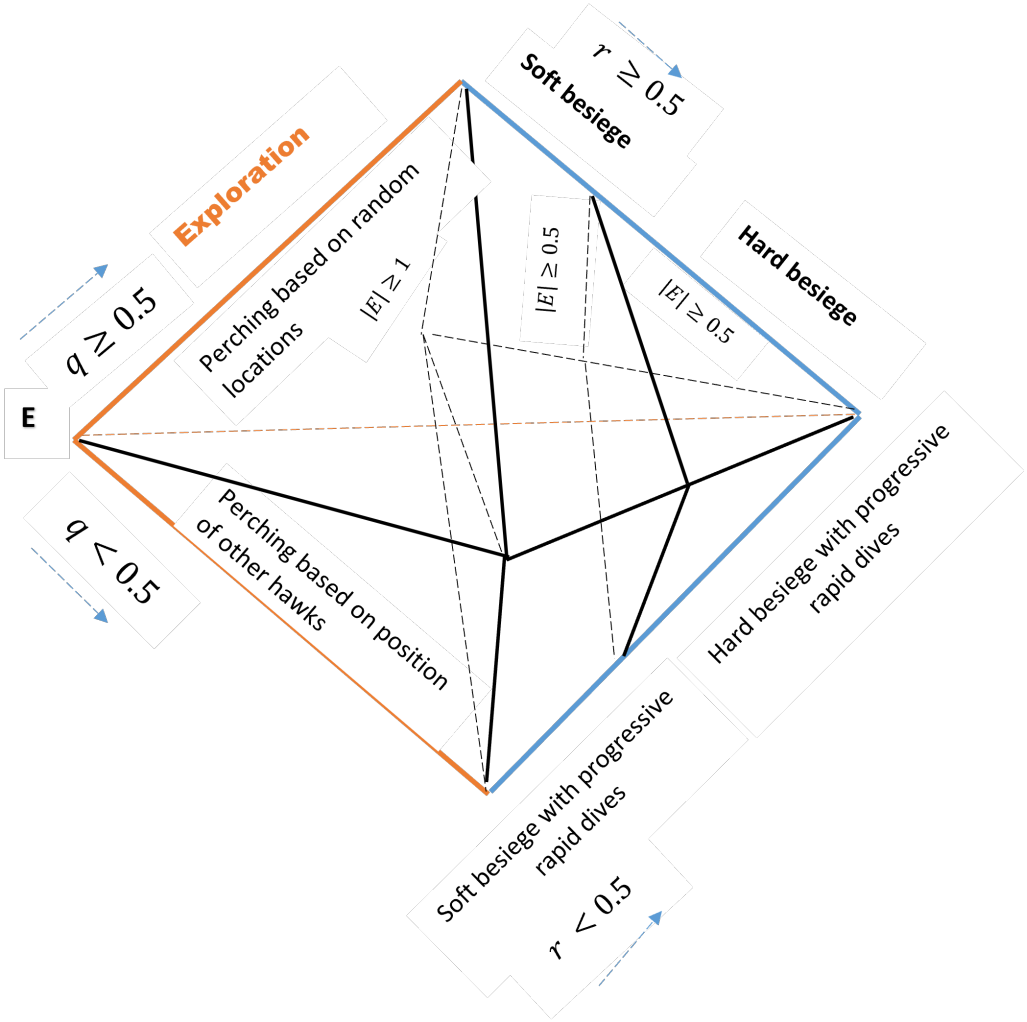

Figure 2. Process of Exploration and Exploitation Phases.

3.3.1. Exploration Phase

The Harris Hawks have exceptional sight for locating and monitoring their prey but frequently struggle to locate it. Therefore, the hawks locate the area to look for prey. Consequently, the hawks pole on a location and watch their prey using two informal observational strategies. When $q < 0.5$, the hawks perch where other hawks and the prey are; otherwise, they randomly perch on any largest tree when $q \geq 0.5$. For all strategies, there are equivalent possibilities. As per the energy the prey is exerting, the HHO technique can transform from an exploration phase to an exploitation phase.

$$E = 2Eo\frac{1-t}{T} \tag{1}$$

Equation (1) above states that the energy of the prey (E) minimizes with iterations, where T is the total iterations, t is the show's iteration, and Eo is the starting energy of the prey. For every iteration, Eo is the random number starting with $(-1, -1)$. So, when the Eo value rises from 0 to 1, the prey grows more powerful [55–57].

3.3.2. Exploitation Phase

Prey typically has an easy time evading dangerous situations. So, the hawks use a variety of chasing techniques. According to the hawks' plan, four main techniques are employed throughout the exploitation phase. Assume that r represents the probability that the prey will either be unable to escape $(r \geq 0.5)$ or able to do so $(r < 0.5)$. To surround the prey, soft and hard besieges are executed. Based on the energy (E) of the prey, the hawks surround it in various places. Collectively, the hawks attack prey to increase the chances of catching the prey. As soon as the prey releases energy, the hawks increase their besiege to capture the prey. When $|E| \geq 0.5$, soft besiege is employed, and when $|E| < 0.5$, hard besiege is employed [55–57].

Soft besiege: When $|E| \geq 0.5$ and $r \geq 0.5$, the prey has sufficient energy to run away through a chance bounce. The Harris Hawks silently surround the prey simultaneously, exhausting it to the point that they can suddenly pounce. From the actual dataset, a small number of features J is created (which show the prey movement in nature) and the different number of features from prey are replicated to the chosen hawks.

Hard besiege: When $|E| < 0.5$ and $r \geq 0.5$, the prey has the lowest energy status and cannot run comfortably. The Harris Hawk's present position is upgraded using Equation (2):

$$X(i,d) = Xrb(0,d) - E \times abs(\Delta X) \tag{2}$$

The prey's single feature is replicated for the present hawk in the proposed model for the hard besiege. This step is represented by Figure 3. ΔX shows the dissimilarity between the prey's location and the hawk's iterations.

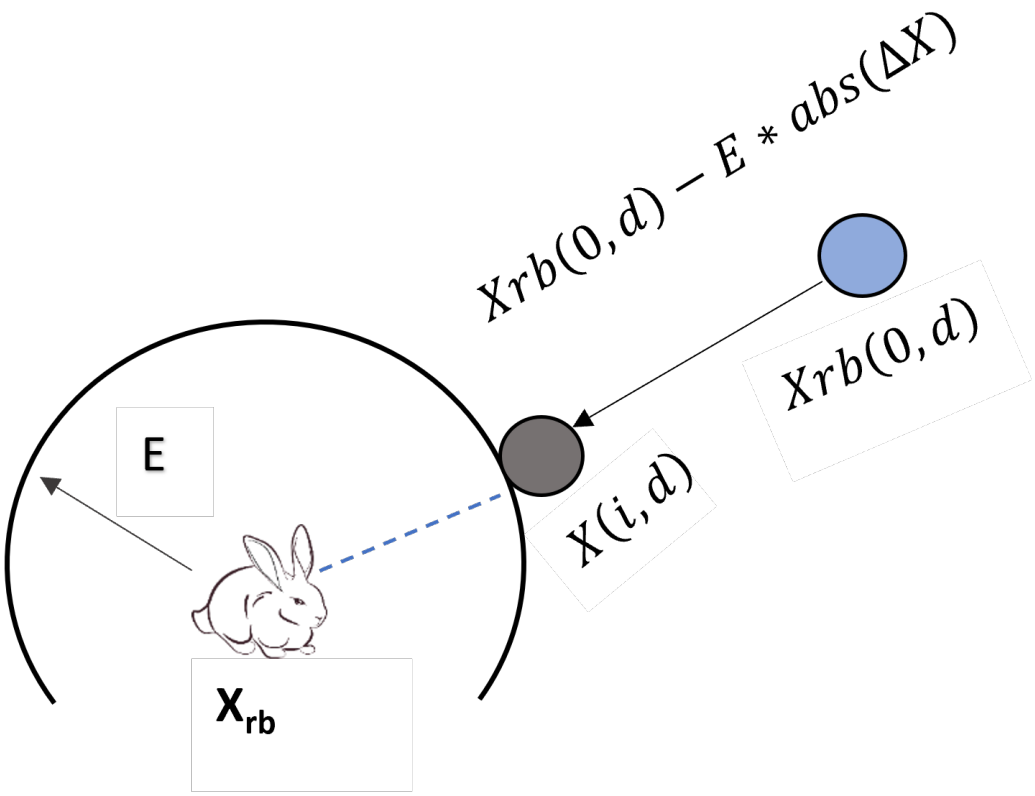

Figure 3. Process of hard besiege.

Soft besiege (SB) with progressive rapid dives: When $r < 0.5$ and $|E| \geq 0.5$, the prey can quickly run and the SB may be executed before the sudden attack. The levy distribution with excellent perturbation is used to design this prey sample in the HHO algorithm. Following the prey energy level, select the features that differ from the present hawk through the given solution. The greedy selection technique chooses the finest features

at the point and resolves the issues that later arise. The classifiers become more efficient due to this technique.

Hard besiege (HB) with progressive rapid dives: The hard besiege is applied when $r < 0.5$, $|E| < 0.5$, and the prey cannot run away. This overall scenario is related to the SB. Hawks gradually reduce the distance from the prey. According to the prey energy status, select the different features from the prey, which are replicated to the hawk randomly selected by the population. To decrease the high disturbance level, a few features are chosen.

Algorithm 1 presents the working HHO. In the first step, the population of hawks is initialized. Next, each hawk's fitness value is evaluated, the location of the hawk is designated, and a new energy level is assigned. When updating the energy level of the prey using Equation (1), exploration (EP) and exploitation phases are executed. If hawks are in the exploitation phase, then four strategies—SB, HB, SB with progressive rapid dives, and HB with progressive rapid dives—are applied according to the energy status of the prey and the probability of prey escaping. In the end, the updated hawk's fitness value is computed and the best result is found.

Algorithm 1 HHO's pseudo code.

Input: N is the Population size, T is the total No. Of iterations, and t is the current iteration.
Output: Best Feature for assessing the performance of the model
Initialize the population of hawks X*i* $(i = 1, 2, 3, \ldots, N)$
While (end)
Evaluate the Hawks' new fitness value, discover the ideal location, and designate it as the prey's location (Xrb))
For (every hawk (X*i*))
Update *Eo*, Update the energy level of prey using Equation (1)
if $(|E| \geq 1)$
Then (Execute the EP)
If $((|E| < 1)$
Then (Execute the EP)
If $(|E| \geq 0.5$ *and* $r \geq 0.5)$ **Then** Execute the SB
Else if $(|E| < 0.5$ *and* $r \geq 0.5)$ **Then** Execute the HB by updating the hawk's position using Equation (2)
Else if $(|E| \geq 0.5$ *and* $r < 0.5)$ **Then** Execute SB with progressive rapid dives **Else if** $(|E| < 0.5$ *and* $r < 0.5)$
Then Execute HB with progressive rapid dives
Compute the updated hawk's fitness value
Result ← Best feature subset
Return Results

3.4. Classification Algorithms

Machine learning is a method that relies on patterns and makes decisions by learning from previous outcomes. Machine learning applications fall under the categories of classification or regression issues [45]. In this detection of cyber-attack in IoMT devices, in this study, some classifiers such as RF, SVM, and ensemble classifiers (Bagging and Boosting), as well as deep learning classifiers such as Recurrent Neural Networks, are applied for the detection of cyber-attack.

3.4.1. Recurrent Neural Network (RNN)

RNN uses sequential data and carries out a similar task for every classification component, with the result depending on the estimation that came previously [58]. RNNs are particularly well suited for modeling sequences because of their cyclic connectivity [5]. Transformers have shown superior performance in certain tasks involving sequential data. However, there are still reasons to use RNNs in certain contexts due to their simplicity, effectiveness in modeling long-term dependencies, and interpretability.

3.4.2. Random Forest

RF is a group learning technique, and RF classification can improve accuracy. Multiple decision trees are used to make up an RF. RF has a reduced classification error in contrast to conventional classification approaches. The RF generates many classification trees. A tree classification approach is used to create the tree and distinct bootstrap samples from the source data are used [59]. When a forest is established, each tree has a new object that must be categorized. A distinctive sample from the source data and a strategy for classifying trees are used by random forest to generate each tree.

3.4.3. Support Vector Machine

SVM employs a kernel to resolve the non-linear separable problem by projecting the elements into a multi-resolution region. SVM aims to discover the best hyper-plane amongst dataset classes by widening the distance between their nearest points. The maximal distance between the two classes is provided by the maximum hyperplane gap [57]. In some learning algorithms, over-fitting problems arise, and the SVM classifier resolves this.

3.4.4. Bagging

Bagging is an ensemble technique used to enhance the performance of a machine learning algorithm. Bagging is also known as bootstrap aggregation, creating samples sequentially and concurrently. Bagging often trains parallel, similar weak learners before combining them using specific averaging techniques. In Bagging, a base learner is trained on every set of replacement training instances after numerous base learners are hypothesized on every set using a random selection of training instances [60].

3.4.5. Boosting

Boosting is a classification error reduction method aiming to outperform many other classification methods. Boosting is also used to enhance machine learning algorithm performance and utilize the sequential ensemble method. The ensemble learner can enhance weak learners and transform them into strong learners by using the Boosting approach [61]. A strong learner is optimal and achieves near-perfect (moderate) performance. A group of learners is sequentially trained and combined for prediction. Every base model depends on the base model before it [60].

4. Result and Discussion

In this section, we thoroughly analyze and demonstrate the performance of the proposed approach. We assess the proposed approach using multiple parameters to determine its superiority over current methodologies and its suitability for detecting cyber-attacks in IoMT devices. This research approach is implemented on the NSL-KDD dataset, providing better outcomes than existing techniques. After preprocessing, the features selected by the machine learning classifiers from the dataset are as follows: RF selects 71 features, SVM chooses 32 features, Bagging selects 46 features, and Boosting chooses 44 features.

4.1. Evaluation Measurements

The result of the proposed approach is assessed on these evaluation measurements, namely, accuracy, precision, recall, and f1-score.

Accuracy: Calculates the ratio of *true positives (TP), false positives (FP), false negatives (FN), and true negatives (TN)* to measure a model's efficiency. Equation (3) presents the accuracy estimate.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

Precision: The ratio of true positives versus all positives (true and false) in the data. This is also known as the positive predicted value. Equation (4) presents the formula to calculate the precision.

$$Precision = \frac{TP}{TP + FP} \tag{4}$$

Recall: The ratio of TPs versus true positives and FNs. These can also be considered as TP rate, sensitivity, and probability of detection. Equation (5) presents the formula to calculate the recall.

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

F1-score: F1-score is the recall and precision weighted average, as shown in Equation (6).

$$F1\text{-}Score = \frac{2 \times Precision + Recall}{Precision + Recall} \tag{6}$$

4.2. Result and Analysis of the Experiment

The proposed employed machine learning (RF, SVM, Bagging, and Boosting) and deep learning algorithms. The proposed approaches' results are explained in Table 1. The HHO-RNN model demonstrated exceptional performance with an accuracy of 0.998%, precision of 0.983%, recall of 0.987%, and f1-score of 0.976%. Similarly, the HHO-RF model achieved a high accuracy of 0.975%, precision of 0.982%, recall of 0.987%, and an f1-score of 0.985%. The HHO-SVM model achieved an accuracy of 0.968%, precision of 0.997%, recall of 0.972%, and an f1-score of 0.987%, indicating its effectiveness. Moreover, the HHO-Bagging model achieved an accuracy of 0.998%, precision of 0.983%, recall of 0.987%, and an f1-score of 0.976%. Lastly, the HHO-Boosting model achieved an accuracy of 0.981%, precision of 0.961%, recall of 0.979%, and an f1-score of 0.970%, showcasing its notable performance.

Table 1. Proposed approach results of different classification algorithms. Key: Accuracy—AC, Precision—PR, Recall—RE, F1-Score—F1.

Algorithms	**AC%**	**PR%**	**RE%**	**F1%**
HHO-RNN	99.8	98.3	98.7	97.6
HHO-RF	97.5	98.2	98.7	98.5
HHO-SVM	96.8	99.7	97.2	98.7
HHO-Bagging	97.5	97.9	98.5	98.2
HHO-Boosting	98.1	96.1	97.9	97.0

Figure 4 illustrates the proposed model's results. The results indicate that the HHO-RNN model achieved an outstanding accuracy of 0.998. In terms of precision, the HHO-SVM model exhibited exceptional performance with a precision score of 0.997. Both the HHO-RNN and HHO-RF models demonstrated the highest recall score of 0.987. Additionally, the HHO-SVM model delivered the best f1-score of 0.987, indicating its overall effectiveness and robust performance.

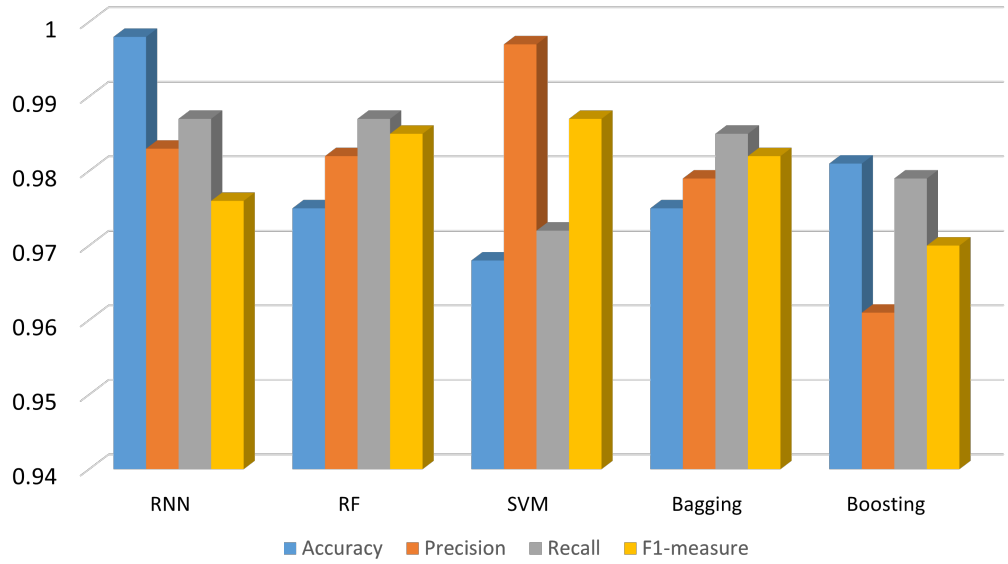

Figure 4. Results of the proposed model.

4.3. Comparison of Proposed Approach with Exiting Studies

Table 2 provides the proposed approach of HHO-RNN with the existing previous techniques. Authors in [32] reported outcomes with accuracy of 89%, precision 91%, recall 88%, and f1-score 90%. Authors in [62] obtained results with accuracy of 92.0% and f1-score of 94%. Authors in [5] reported results with an accuracy of 99.76%, precision 99.75%, and f1-score 96.45%.

Table 2. Comparative table with previous methodologies.

Authors	Methods	A%	P%	R%	F1%
Moukafih et al. [32]	Ensemble	89.0%	91.0%	88.0%	90.0%
Saheed et al. [5]	PSO-RF	99.7%	99.7%	-	96.4%
Nguyen et al. [62]	CNN	92.0%	-	-	94%
Proposed Approach	HHO-RNN	99.8%	98.3%	98.7%	97.6%

Figure 5 shows that the proposed approach in this research outperformed previous approaches; however, in terms of precision, the HH0-RNN model performance decreased by 1.43%. The existing approaches performed well in terms of precision.

Some limitations can be addressed, such as increasing the number of devices and data sources, and the proposed approach may need to be revised. It requires more processing power and storage space to handle the growing volume of data, and the computational resources need to be increased to support real-time processing. The approach may need to be optimized for scalability by incorporating distributed computing and parallel processing techniques to address this limitation. Large-scale IoMT networks generate massive data that require significant computational power to process, analyze, and extract valuable insights. The proposed approach may have greater computational complexity and take too long to analyze the data, leading to delays and decreased real-time applicability. To overcome this challenge, the approach may need to incorporate different deep learning algorithms, which can aid in minimizing computational complexity. Deep learning models such as RNNs can be highly accurate but very complex, making it difficult to understand and explain their decision-making process. To address these challenges, practitioners can use techniques such as feature importance analysis, model visualization, partial dependence plots, layer-wise

relevance propagation, and dimensionality reduction to improve the interpretability of the RNN.

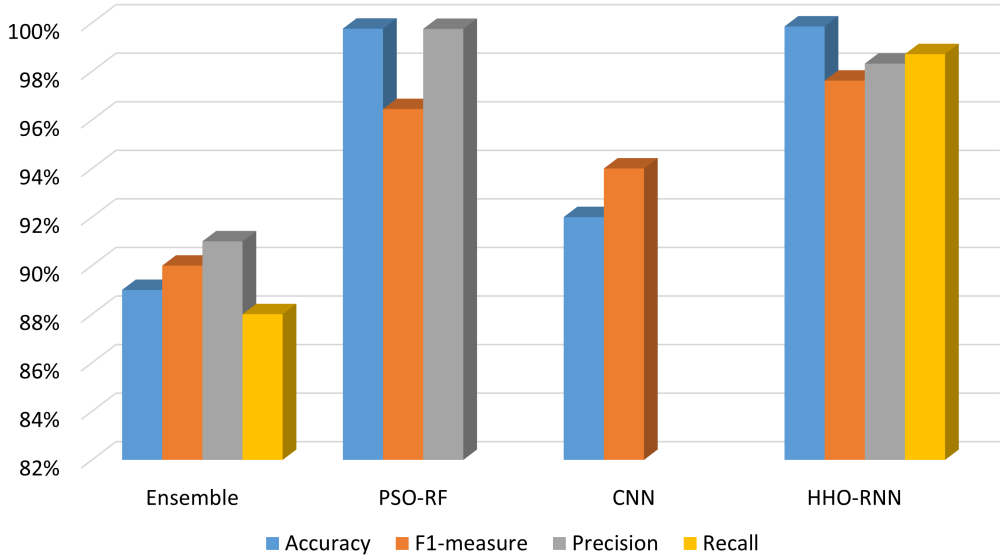

Figure 5. Graphical representation of the results. Ensemble [32], PSO-RF [5], CNN [62], and the proposed approach (HHO-RNN).

5. Conclusions

This study proposed an implicit approach construct on machine learning and deep learning algorithms with the Harris Hawk optimization algorithm for classifying cyber-attacks using the NSL-KDD dataset. Firstly, raw data are preprocessed using one-hot encoding and normalization to normalize the data. Secondly, HHO is applied to optimize the features. The proposed method could be most suitable for IoMT environments where peer-to-peer communication between innovative healthcare equipment is possible using various IP addresses. Lastly, RF, SVM, Bagging, Boosting, and RNN are applied for classification. The results show that the accuracy is enhanced when the classifiers are combined with HHO. Future work will be to scrutinize the proposed approach's results on the multi-class problem and check the generalizability of the proposed approach on multiple datasets; further, comparing the proposed approach with more existing techniques, examining potential trade-offs between evaluation metrics, and validating the methodology in real-world IoMT environments may be fruitful.

Author Contributions: Conceptualization, S.A.; methodology, S.A. and G.A.S.; validation, M.A. and A.A.; formal analysis, S.A., G.A.S., M.A., A.A., S.-P.H. and I.Y.; writing—original draft preparation, S.A., I.Y., S.-P.H. and G.A.S.; writing—review and editing, M.A., A.A., S.-P.H. and M.A.; supervision, G.A.S. and M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia, for funding this research work through project number 223202.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors share no conflict of interest.

References

1. Dhasarathan, C.; Hasan, M.K.; Islam, S.; Abdullah, S.; Mokhtar, U.A.; Javed, A.R.; Goundar, S. COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach. *Comput. Commun.* **2023**, *199*, 87–97. [CrossRef]
2. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-based applications in healthcare devices. *J. Healthc. Eng.* **2021**, *2021*, 6632599. [CrossRef]
3. Akhras, K.S.; Alsheikh-Ali, A.A.; Kabbani, S. Use of real-world evidence for healthcare decision-making in the Middle East: Practical considerations and future directions. *Expert Rev. Pharmacoecon. Outcomes Res.* **2019**, *19*, 245–250. [CrossRef]

4. Javed, A.R.; Khan, H.U.; Alomari, M.K.B.; Sarwar, M.U.; Asim, M.; Almadhor, A.S.; Khan, M.Z. Toward explainable AI-empowered cognitive health assessment. *Front. Public Health* **2023**, *11*, 1024195. [CrossRef]
5. Saheed, Y.K.; Arowolo, M.O. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEE Access* **2021**, *9*, 161546–161554. [CrossRef]
6. Safa, M.; Pandian, A.; Gururaj, H.; Ravi, V.; Krichen, M. Real time health care big data analytics model for improved QoS in cardiac disease prediction with IoT devices. *Health Technol.* **2023**, 1–11
7. Akram, F.; Liu, D.; Zhao, P.; Kryvinska, N.; Abbas, S.; Rizwan, M. Trustworthy Intrusion Detection in E-Healthcare Systems. *Front. Public Health* **2021**, *9*, 1800. [CrossRef] [PubMed]
8. Rahman, H.; Naik Bukht, T.F.; Ahmad, R.; Almadhor, A.; Javed, A.R. Efficient Breast Cancer Diagnosis from Complex Mammographic Images Using Deep Convolutional Neural Network. *Comput. Intell. Neurosci.* **2023**, *2023*, 7717712. [CrossRef] [PubMed]
9. Bharadwaj, H.K.; Agarwal, A.; Chamola, V.; Lakkaniga, N.R.; Hassija, V.; Guizani, M.; Sikdar, B. A review on the role of machine learning in enabling IoT based healthcare applications. *IEEE Access* **2021**, *9*, 38859–38890. [CrossRef]
10. Javed, A.R.; Shahzad, F.; ur Rehman, S.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Xu, G. Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. *Cities* **2022**, *129*, 103794. [CrossRef]
11. Lian, Z.; Zeng, Q.; Wang, W.; Gadekallu, T.R.; Su, C. Blockchain-Based Two-Stage Federated Learning with Non-IID Data in IoMT System. *IEEE Trans. Comput. Soc. Syst.* **2022**. [CrossRef]
12. Yenduri, G.; Kaluri, R.; Gadekallu, T.R.; Mahmud, M.; Brown, D.J. Blockchain for Software Maintainability in Healthcare. In Proceedings of the 24th International Conference on Distributed Computing and Networking, Kharagpur, India, 4–7 January 2023; pp. 420–424.
13. Rbah, Y.; Mahfoudi, M.; Balboul, Y.; Fattah, M.; Mazer, S.; Elbekkali, M.; Bernoussi, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey. In Proceedings of the 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 3–4 March 2022; pp. 1–9.
14. Mohiyuddin, A.; Chakraborty, C.; Rizwan, M.; Shabbir, M. Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. *Int. J. Fuzzy Syst.* **2022**, *24*, 1203–1215. [CrossRef]
15. Mehmood, M.; Rizwan, M.; Gregus ml, M.; Abbas, S. Machine learning assisted cervical cancer detection. *Front. Public Health* **2021**, *9*, 788376. [CrossRef] [PubMed]
16. Haraty, R.A.; Boukhari, B.; Kaddoura, S. An Effective Hash-Based Assessment and Recovery Algorithm for Healthcare Systems. *Arab. J. Sci. Eng.* **2021**, *47*, 1523–1536. [CrossRef]
17. El Zarif, O.; Haraty, R.A. Toward information preservation in healthcare systems. In *Innovation in Health Informatics*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 163–185.
18. Kaddoura, S.; Haraty, R.A.; Al Kontar, K.; Alfandi, O. A parallelized database damage assessment approach after cyberattack for healthcare systems. *Future Internet* **2021**, *13*, 90. [CrossRef]
19. Chehab, M.; Mourad, A. Towards a lightweight policy-based privacy enforcing approach for IoT. In Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 12–14 December 2018; pp. 984–989.
20. 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]
21. Wahab, O.A.; Mourad, A.; Otrok, H.; Taleb, T. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1342–1397. [CrossRef]
22. AbdulRahman, S.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet Things J.* **2020**, *8*, 5476–5497. [CrossRef]
23. AbdulRahman, S.; Tout, H.; Mourad, A.; Talhi, C. FedMCCS: Multicriteria client selection model for optimal IoT federated learning. *IEEE Internet Things J.* **2020**, *8*, 4723–4735. [CrossRef]
24. Dasaradharami Reddy, K.; Gadekallu, T.R. A Comprehensive Survey on Federated Learning Techniques for Healthcare Informatics. *Comput. Intell. Neurosci.* **2023**, *2023*, 8393990. [CrossRef]
25. Xue, B.; Warkentin, M.; Mutchler, L.A.; Balozian, P. Self-efficacy in information security: A replication study. *J. Comput. Inf. Syst.* **2023**, *63*, 1–10. [CrossRef]
26. Yunis, M.M.; El-Khalil, R.; Ghanem, M. Towards a Conceptual Framework on the Importance of Privacy and Security Concerns in Audit Data Analytics. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Sao Paulo, Brazil, 5–8 April 2021.
27. Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access* **2020**, *8*, 106576–106584. [CrossRef]
28. Abbas, N.; Nasser, Y.; Shehab, M.; Sharafeddine, S. Attack-specific feature selection for anomaly detection in software-defined networks. In Proceedings of the 2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Agadir, Morocco, 3–5 December 2021; pp. 142–146.
29. Wahab, O.A.; Bentahar, J.; Otrok, H.; Mourad, A. Resource-aware detection and defense system against multi-type attacks in the cloud: Repeated bayesian stackelberg game. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 605–622. [CrossRef]

30. Nayak, J.; Meher, S.K.; Souri, A.; Naik, B.; Vimal, S. Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *J. Supercomput.* **2022**, *78*, 14866–14891. [CrossRef]
31. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Comput. Commun.* **2021**, *166*, 110–124. [CrossRef]
32. Moukafih, N.; Orhanou, G.; El Hajji, S. Neural network-based voting system with high capacity and low computation for intrusion detection in SIEM/IDS systems. *Secur. Commun. Netw.* **2020**, *2020*, 3512737. [CrossRef]
33. Saheed, Y.K.; Abiodun, A.I.; Misra, S.; Holone, M.K.; Colomo-Palacios, R. A machine learning-based intrusion detection for detecting internet of things network attacks. *Alex. Eng. J.* **2022**, *61*, 9395–9409. [CrossRef]
34. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Lagkas, T.; Fragulis, G.; Sarigiannidis, A. A self-learning approach for detecting intrusions in healthcare systems. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
35. Rahman, S.A.; Tout, H.; Talhi, C.; Mourad, A. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Netw.* **2020**, *34*, 310–317. [CrossRef]
36. Gautam, S.; Henry, A.; Zuhair, M.; Rashid, M.; Javed, A.R.; Maddikunta, P.K.R. A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization. *Electronics* **2022**, *11*, 3529. [CrossRef]
37. Haque, N.I.; Rahman, M.A.; Shahriar, M.H.; Khalil, A.A.; Uluagac, S. A novel framework for threat analysis of machine learning-based smart healthcare systems. *arXiv* **2021**, arXiv:2103.03472.
38. Aleesa, A.; Younis, M.; Mohammed, A.A.; Sahar, N. Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques. *J. Eng. Sci. Technol.* **2021**, *16*, 711–727.
39. Hammoud, A.; Mourad, A.; Otrok, H.; Wahab, O.A.; Harmanani, H. Cloud federation formation using genetic and evolutionary game theoretical models. *Future Gener. Comput. Syst.* **2020**, *104*, 92–104. [CrossRef]
40. Shamseddine, H.; Nizam, J.; Hammoud, A.; Mourad, A.; Otrok, H.; Harmanani, H.; Dziong, Z. A novel federated fog architecture embedding intelligent formation. *IEEE Netw.* **2020**, *35*, 198–204. [CrossRef]
41. Kuppusamy, P.; Kumari, N.M.J.; Alghamdi, W.Y.; Alyami, H.; Ramalingam, R.; Javed, A.R.; Rashid, M. Job scheduling problem in fog-cloud-based environment using reinforced social spider optimization. *J. Cloud Comput.* **2022**, *11*, 99. [CrossRef]
42. Wahab, O.A.; Bentahar, J.; Otrok, H.; Mourad, A. Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. *IEEE Trans. Serv. Comput.* **2017**, *13*, 114–129. [CrossRef]
43. Kilincer, I.F.; Ertam, F.; Sengur, A.; Tan, R.S.; Acharya, U.R. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybern. Biomed. Eng.* **2023**, *43*, 30–41. [CrossRef]
44. Khan, F.; Jan, M.A.; Alturki, R.; Alshehri, M.D.; Shah, S.T.; ur Rehman, A. A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT. *IEEE Trans. Ind. Inform.* **2023**. [CrossRef]
45. RM, S.P.; Maddikunta, P.K.R.; Parimala, M.; Koppu, S.; Gadekallu, T.R.; Chowdhary, C.L.; Alazab, M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput. Commun.* **2020**, *160*, 139–149.
46. Aswad, F.M.; Ahmed, A.M.S.; Alhammadi, N.A.M.; Khalaf, B.A.; Mostafa, S.A. Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. *J. Intell. Syst.* **2023**, *32*. [CrossRef]
47. Hnamte, V.; Hussain, J. DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telemat. Inform. Rep.* **2023**, *10*, 100053. [CrossRef]
48. Yazdinejad, A.; Kazemi, M.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H. An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digit. Commun. Netw.* **2023**, *9*, 101–110. [CrossRef]
49. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 22009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
50. Farahnakian, F.; Heikkonen, J. A deep auto-encoder based approach for intrusion detection system. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; pp. 178–183.
51. Wang, W.; Zhang, X.; Gombault, S.; Knapskog, S.J. Attribute normalization in network intrusion detection. In Proceedings of the 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaoshiung, Taiwan, 14–16 December 2009; pp. 448–453.
52. Shakya, V.; Makwana, R.R.S. Feature selection based intrusion detection system using the combination of DBSCAN, K-Mean++ and SMO algorithms. In Proceedings of the 2017 international conference on trends in electronics and informatics (ICEI), Tirunelveli, India, 11–12 May 2017; pp. 928–932.
53. Saheed, Y.K.; Hamza-Usman, F.E. Feature selection with IG-R for improving performance of intrusion detection system. *Int. J. Commun. Netw. Inf. Secur.* **2020**, *12*, 338–344. [CrossRef]
54. Deka, R.K.; Bhattacharyya, D.K.; Kalita, J.K. Active learning to detect DDoS attack using ranked features. *Comput. Commun.* **2019**, *145*, 203–222. [CrossRef]
55. Heidari, A.A.; Mirjalili, S.; Faris, H.; Aljarah, I.; Mafarja, M.; Chen, H. Harris hawks optimization: Algorithm and applications. *Future Gener. Comput. Syst.* **2019**, *97*, 849–872. [CrossRef]
56. Abdel-Basset, M.; Ding, W.; El-Shahat, D. A hybrid Harris Hawks optimization algorithm with simulated annealing for feature selection. *Artif. Intell. Rev.* **2021**, *54*, 593–637. [CrossRef]

57. Dokeroglu, T.; Deniz, A.; Kiziloz, H.E. A robust multiobjective Harris' Hawks Optimization algorithm for the binary classification problem. *Knowl.-Based Syst.* **2021**, *227*, 107219. [CrossRef]
58. Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep recurrent neural network for intrusion detection in sdn-based networks. In Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Canada, 25–29 June 2018; pp. 202–206.
59. Zhang, H.; Dai, S.; Li, Y.; Zhang, W. Real-time distributed-random-forest-based network intrusion detection system using Apache spark. In Proceedings of the 2018 IEEE 37th international performance computing and communications conference (IPCCC), Orlando, FL, USA, 17–19 November 2018; pp. 1–7.
60. Rani, D.; Gill, N.S.; Gulia, P.; Chatterjee, J.M. An Ensemble-Based Multiclass Classifier for Intrusion Detection Using Internet of Things. *Comput. Intell. Neurosci.* **2022**, *2022*, 1668676. [CrossRef] [PubMed]
61. Odegua, R. An empirical study of ensemble techniques (bagging boosting and stacking). *Deep Learn. IndabaXAt* **2019**. [CrossRef]
62. 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.