

Article

A Hybrid Genetic Algorithm-Based Random Forest Model for Intrusion Detection Approach in Internet of Medical Things

Monire Norouzi ¹, Zeynep Gürkaş-Aydın ², Özgür Can Turna ², Mehmet Yavuz Yağci ²,
Muhammed Ali Aydın ² and Alireza Souri ^{3,*}

¹ Computer Technology Program, Vocational School, Haliç University, Istanbul 34060, Türkiye; monirenorouzi@halic.edu.tr

² Department of Computer Engineering, Istanbul University-Cerrahpaşa, Istanbul 34320, Türkiye; zeynepg@iuc.edu.tr (Z.G.-A.); ozgurcan.turna@iuc.edu.tr (Ö.C.T.); myy@iuc.edu.tr (M.Y.Y.); aydinali@iuc.edu.tr (M.A.A.)

³ Department of Software Engineering, Faculty of Engineering, Haliç University, Istanbul 34060, Türkiye

* Correspondence: alirezasouri@halic.edu.tr

Abstract: The Internet of Medical Things (IoMT) is a bio-network of associated medical devices, which is slowly improving the healthcare industry by focusing its abilities on enhancing personal healthcare benefits with medical data. Moreover, the IoMT tries to deliver sufficient and more suitable medical services at a low cost. With the rapid growth of technology, medical instruments that are widely used anywhere are likely to increase security issues and create safe data transmission issues through resource limitations and available connectivity. Moreover, the patients probably face the risk of different forms of physical harm because of IoMT device attacks. In this paper, we present a secure environment for IoMT devices against cyber-attacks for patient medical data using a new IoMT framework with a hybrid genetic algorithm-based random forest (GA-RF) model. The proposed algorithm achieved better results in terms of accuracy (99.999%), precision, and recall (100%, respectively) to detect cyber-attacks based on two NSL-KDD and UNSW_2018_IoT_Botnet data sets than the other machine learning algorithms.

Keywords: Internet of Medical Things (IoMT); intrusion detection system; machine learning; random forest; genetic algorithm



Citation: Norouzi, M.; Gürkaş-Aydın, Z.; Turna, Ö.C.; Yağci, M.Y.; Aydın, M.A.; Souri, A. A Hybrid Genetic Algorithm-Based Random Forest Model for Intrusion Detection Approach in Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 11145. <https://doi.org/10.3390/app132011145>

Academic Editors:
Chinmay Chakraborty and
Keping Yu

Received: 28 August 2023
Revised: 3 October 2023
Accepted: 6 October 2023
Published: 10 October 2023



Copyright: © 2023 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

Currently, cyber-physical systems (CPS) are famous systems whose architectural paradigm, combined with communication technologies and pervasive sensing, deliver numerous economic and societal advantages. These systems have become essential for complicated infrastructures, such as transportation, healthcare, energy, and the smart grid [1]. They perform with Internet of Things (IoT) instruments that develop massive volumes of data for communication [2]. A CPS is commonly preferred among the recent inventions of computing technology, such as cloud computing, wireless sensor networks (WSNs), medical sensors, and the Internet of Medical Things (IoMT), to achieve advantages in clinical applications such as home patient care and healthcare processes. These applications deliver many advantages and suitable results for better medicines due to the continued monitoring of patients from remote sites [3,4].

Occurring or facing security problems in IoMT networks and their systems can generate disorder in the disease diagnosis process, cause a delay in communication between patients and clinical staff, and result in the patients' private information and clinical history data going missing [5]. Because of all of these important issues, it is critical to determine any types of unauthorized attacks and suspected activities in the IoMT systems as early as possible. By using a powerful intrusion detection system (IDS) [6], due to its advantages and benefits, it becomes a little easier and more practical to recognize an attack by

analyzing and examining system parameters, values, and various other variables or by catching variations from normal and usual behavior [7]. All of these security problems have a deep and maybe long-lasting effect on the IoMT systems and their clients. Therefore, this issue highlights the need for designing and developing an accurate and strong IDS for the IoMT network and systems [8]. New models and frameworks based on machine learning (ML) algorithms can be used at both the network and host levels of IDS systems. Models and frameworks prepared with ML algorithms can recognize and discover unpredictable activities and classify them as already-detected suspected and abnormal activities [9,10].

In this paper, a novel ML-based prediction model with a feature selection approach is presented and explained for effectively identifying intrusions that are malicious in the IoMT environment. Sensitive medical and healthcare information will be protected by the proposed ML-based prediction model against attacks, malware, and suspicious threats. The main contributions of this study are mentioned below:

- A newly designed and optimized genetic algorithm-based random forest (GA-RF) model was developed to recognize and analyze malicious movements and cyber-attacks in IoMT devices and their environment.
- The hybrid GA-RF algorithm was applied to two real data sets, NSL-KDD [1] and UNSW_2018_IoT_Botnet, to discover and recognize the effect and result of security standards and measure them in a cyber-security scenario.
- A performance evaluation of the proposed GA-RF model was completed and the results were analyzed and compared with other ML algorithms.

This paper is organized as follows. Section 2 explains the related works. The ML-based proposed model, with a GA-RF algorithm, is explained in Section 3. The experimental results are presented in Section 4. Finally, the conclusion is presented in Section 5.

2. Related Works

In this section, we examine some studies that deal with the security issues of IoMT network-based devices. In the first study, the authors [8] proposed a new deep learning-based framework incorporating an effective IDS into IoMT systems. First, the feature selection process was carried out by applying a genetic algorithm. Next, the data set was normalized, and finally, a deep learning algorithm was applied to the proposed normalized data set to obtain an effective classification process. The whole-test results proved that the proposed framework performed better than the other ML algorithms in terms of accuracy and F-score. Moreover, this framework can prepare a secure way for data transfer methods in IoMT systems. The authors of [9] proposed a novel IDS system using ML algorithms for detecting IoT network attacks by applying ML-supervised algorithms. First, a Min–Max normalization process and feature selection processes were carried out on the proposed data set, and dimensionality reduction was performed. At the simulation level, the authors used six ML algorithms for the analysis procedure. The simulation results showed that the proposed frameworks and applied ML algorithms achieved sufficient values in terms of accuracy, precision, and F-score evaluation parameters. This study proved that ML techniques can successfully detect anomalies and unexpected attacks using the proposed data set in the IoT environment.

In another study, RM, Maddikunta [11] proposed a new deep neural network (DNN)-based framework to develop IDS in the IoMT network, aiming to predict unexpected attacks at the first step and dynamically classify them at the next step in both the network and host side. The feature selection method was used for all of the network parameters. The pre-processed optimization process was carried out on the proposed data set using a genetic algorithm and so in the results it was expected that the execution time would decrease. The authors analyzed the experimental results compared with other ML algorithms. It was confirmed that the proposed framework achieved better results compared to other ML algorithms in terms of accuracy, and time complexity. Nandy, Adhikari [12] presented a new hybrid IDS model for the IoMT network focusing on patients' health data analysis gathered from different wearable sensors and predicting unexpected attacks at the edge

of the network using a genetic algorithm to satisfy and respond to security and privacy concerns. The experimental results determined the attacks that were occurring through data transmission in the network with higher accuracy and precision over the ToN-IoT data set.

In another paper, Thamilarasu, Odesile [13] designed a scalable IDS system to prepare the secure area for the IoMT network using five ML algorithms. In this study, the authors used sensor data gathered from wireless body sensors and other connected medical devices to detect anomalies, attacks, and malicious activities at the device level. The simulation results were extracted from OMNeT that show the proposed IDS system obtained less overhead and a higher accuracy of up to 99.9% using the decision trees algorithm more effectively than the other four ML algorithms. Manimurugan, Al-Mutairi [14] proposed a new model for the IDS system to determine any type of anomalies and attacks such as botnet attacks, DoS/DDoS attacks, and web attacks in the IoMT network by analyzing the CICIDS 2017 data set and applying a deep belief network. The experimental results extracted from MATLAB by applying a deep learning algorithm showed that the proposed method was able to achieve suitable results in terms of accuracy of up to 99.96% in the four above-mentioned different type of attacks.

In another piece of research, Saheed and Arowolo [15] presented a new IDS model in the IoMT network for three important steps including detecting, classifying, and predicting unpredictable attacks using a deep learning algorithm and four supervised ML algorithms. In this paper, the applied data set was normalized (all values are between 0 and 1); then, by applying a genetic algorithm, the feature selection process was completed. Simulation results proved that the random forest algorithm combined with particle swarm optimization (PSO) achieved better results in terms of accuracy, precision, and recall than the other ML algorithms. Liaqat, Akhunzada [16] proposed a hybrid DL-based model for the SDN environment to detect botnet attacks in the IoMT network. The authors used the Bot-IoT data set for the evaluation of unpredictable attacks in the proposed model. In the first step, data transformation and data normalization were performed in the proposed data set. Evaluation metrics such as accuracy and precision were observed and measured in the proposed model. The experimental results proved the efficiency and scalability of the proposed model. This model using a hybrid DL algorithm provides higher accuracy and precision than the other algorithms.

Finally, Khan, Moustafa [17] proposed a new attack detection method in the IoMT network using a deep learning algorithm. The authors suggested a solution for the vanishing gradient problem to rapidly perform the training process. The simulation results demonstrate that the proposed model provides optimal results in terms of evaluation parameters such as accuracy, precision, recall, and f-score and higher detection rates with less computational cost using the recurrent neural networks (RNN) algorithm.

The main ideas, data sets, simulation environments, and the proposed prediction approaches in related studies are shown in Table 1.

Table 1. Main ideas and the prediction approaches of the related works in the fields of ML-based IDS systems for the IoMT network.

Ref	Main Idea	Data Set	Simulation Environment	Prediction Approach
Gupta, Shar-ma [8]	A tree classifier-based IDS model using DL algorithms in the IoMT network.	Benchmarked data set	Simulated in a restricted network environment	Random forest (RF), GridSearchCV, best estimator, Logistic regression, decision tree, extremely randomized tree.

Table 1. Cont.

Ref	Main Idea	Data Set	Simulation Environment	Prediction Approach
Saheed, Abio-dun [9]	An ML-based IDS system in the IoMT network.	UNSW-NB15	Simulated network traffic	XGBoost, CatBoost, k-nearest neighbors (KNN), support vector machine (SVM), quadratic discriminant analysis (QDA), and naive Bayes (NB).
RM, Maddikunta [11]	A DNN-based model to develop IDS in the IoMT network.	Benchmarked data set	Rigorous testing	Feedforward deep neural networks (FFDNN), filter-based feature selection algorithm (FBFSA).
Nandy, Adhikari [12]	A hybrid IDS system for the IoMT network using a genetic algorithm.	ToN-IoT	Python programming	Swarm neural network, KNN, decision tree, SVM, logistic regression.
Thamilarasu, Odesile [13]	An IDS system based on ML algorithm for the IoMT network.	Benchmarked data set	OMNeT-based Castalia-3.2 simulator	SVM, Decision Trees, NB, KNN, and RF.
Manimuru-gan, Al-Mutairi [14]	A new deep learning-based model for IDS system in the IoMT network.	CICIDS 2017	MATLAB	Deep belief network (DBN) algorithm.
Saheed and Arowolo [15]	An IDS system based on the DL algorithm for the IoMT network.	NSL-KDD	-	PSO, SVM, RF, NB, KNN, ridge classifier, and recurrent neural network.
Liaqat, Akhuzada [16]	A new botnet detection hybrid model based on DL algorithm in SDN environment for IoMT network.	Bot-IoT	Keras with Python	Convolutional neural network algorithm.
Khan, Moustafa [17]	A new attack detection method using a DL algorithm in the IoMT network.	ToN_IoT	Keras and TensorFlow	Recurrent neural networks algorithm.
Proposed method	Hybrid genetic-based random forest prediction model	UNSW_2018_IoT_Botnet and NSL-KDD	WEKA	Genetic algorithm-random forest, SVM, decision trees, NB, Bayesian network and RF.

3. Proposed System

With the rapid development of communication and computing technologies along with more extraordinary computing abilities and power communications, the potential of the IoT in the medical fields should be taken into consideration, which is why it is now named the Internet of Medical Things (IoMT). IoMT includes the related infrastructure of many medical instruments and various related pieces of software to communicate and share healthcare data with different healthcare information systems. By using several smart sensors, especially wearable sensors, medical staff and medical professionals can acquire, gather, and save real-time health data related to their patients. As a result, medical professionals can analyze clinical decision making based on healthcare data and information.

IoMT is developed to respond to important health problems and concerns and presents many useful services and benefits in the IoMT medical areas, as described in Figure 1.

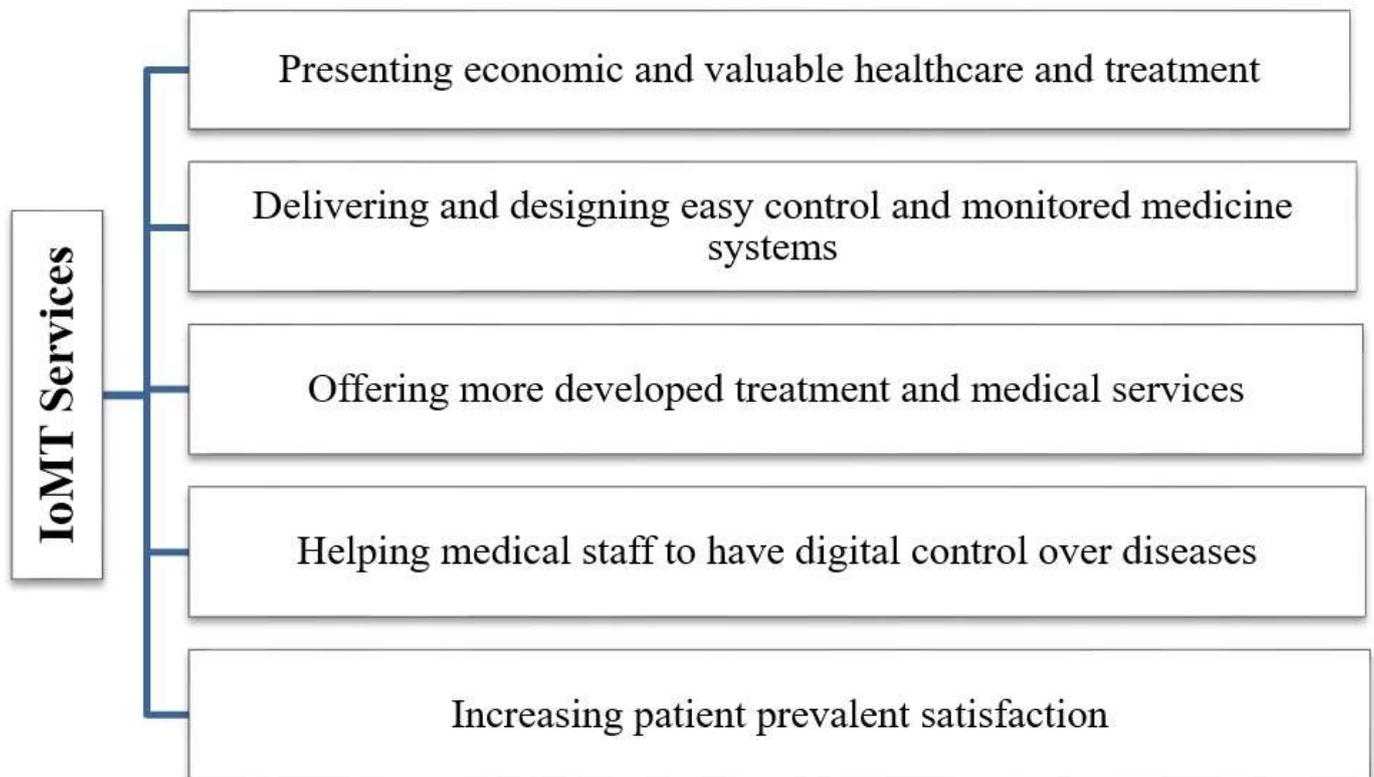


Figure 1. IoMT services and benefits.

Today, IoMT development and data/device management methods have caused security concerns and cyber-security problems. Valid/invalid authentication methods, safe logging, safe data transmission processes, and designing secure interfaces are important challenges in any IoMT system. It is critical to design a proper framework for IoMT systems to respond to all the security concerns and be able to manage complexities, face unexpected attacks, and fend off malicious activities. In the IoMT systems, real-time data are gathered from the wearable sensors of the users in the first step. In the next step, all of the sensed data from different sensors are transmitted to the cloud via Wi-Fi or Bluetooth using smart applications.

As shown in Figure 2, all of the healthcare records of the smart surgery, gathered from wearable sensors and medical devices, are stored in a cloud storage center. There are always some attackers/hackers or malware that try to find gaps to acquire or change data. Unfortunately, the data can be maliciously updated in the cloud. In the first step, pre-processing is applied to the health data set; then, we apply the train and test processes to the data set using ML algorithms. We achieve the intrusion categorization from the result of the test process. Here, there are two statuses as “normal” or “anomaly” detection activities based on the existing protocols with guest login status and the server error rate. If the status is normal, the data are safe, there is no change in the data and so the health data are sent to medical staff for further control. But, if the status is an anomaly, some required security protection policies should be performed to detect the intrusion.

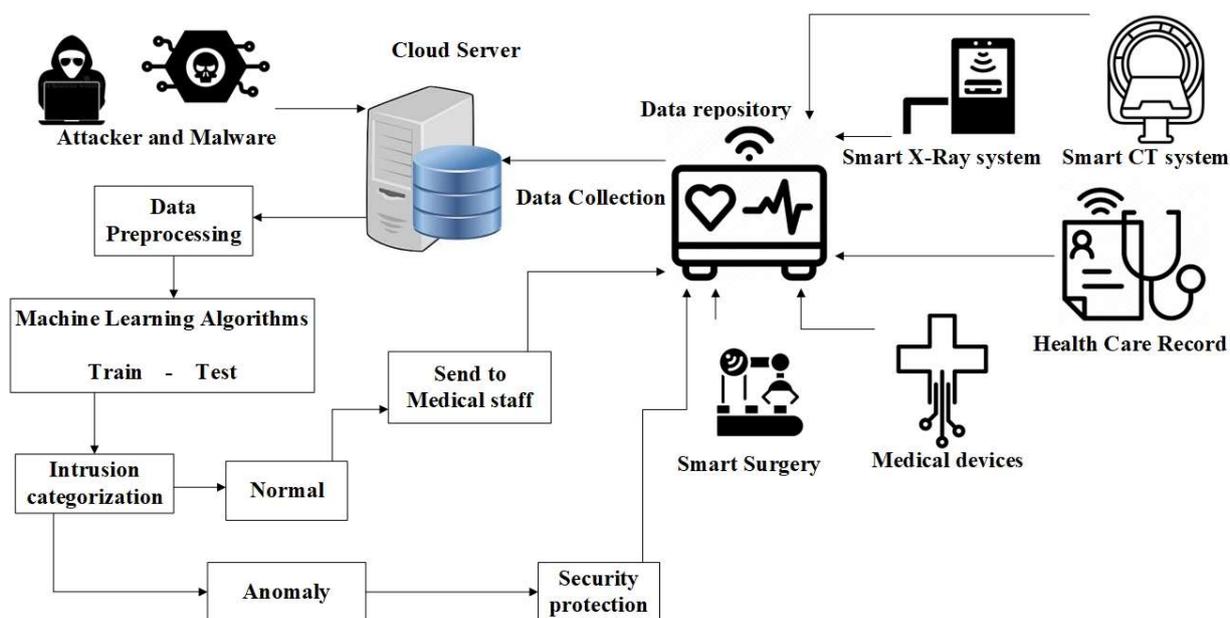


Figure 2. General view of the cyber-attack detection in the IoMT healthcare system [18].

In this work, a novel model is developed for efficient anomaly detection in an IoMT framework using genetic algorithm–random forest (GA-RF) algorithm in comparison to other machine learning algorithms such as support vector machine (SVM), naive Bayes, Bayes net, J48, and random forest algorithms. The random forest algorithm is one of the most famous and commonly used supervised ML algorithms for classification purposes and regression issues. When the number of trees increases in a forest, the forest will be more powerful. Likewise, many numbers of trees in a random forest algorithm causes the algorithm to achieve higher accuracy. This algorithm creates decision trees on different models and considers their high value for classification and average value in regression. By using the random forest algorithm, we can build our model to achieve intrusion categorization purposes with the highest accuracy and precision, rather than the other applied ML algorithms. Implementation of the optimized random forest algorithm using a genetic algorithm as a hybrid GA-RF algorithm was presented [19] to determine an optimal sub forest from a random forest algorithm [20]. For the proposed model, decision random forest sets as initial points are applied for the training method. The number of iterations and population size are initiated. Then, crossover for elitist operator is generated. After the crossover method, the mutation procedure is applied. Then, chromosome selection for a new population is applied, with the setting “elitist operations”. Finally, refinement of the chromosome to select an optimal solution is applied.

4. Experimental Set Up and Result Analysis

In this section, we illustrate the training and testing environments and set up the data sets, simulation tools, and evaluation processes of the suggested framework based on the ML algorithms to recognize malicious activities and movements in the IoMT device and environment.

4.1. Data Set and Simulation Tool

In this paper, we applied two real data sets for our experiments. In the first case study, the NSL-KDD, <https://www.unb.ca/cic/datasets/nsl.html> (accessed on 8 May 2023), data set [10,21] is used, consisting of 42 features with a total of 148,517 instances. NSL-KDD is a data set to solve some of the inherent difficulties of the KDD’99 data set. This data set classifies existing instances into two main categories as “Anomaly” and “Normal” labels [22]. For the second case study, UNSW_2018_IoT_Botnet, <https://www.unb.ca/cic/>

[datasets/nsl.html](#) (accessed on 8 May 2023), Refs. [23–26] data set is applied to evaluate prediction factors for the proposed GA-RF algorithm in IoMT environment [27,28]. This data set has 19 features for a total of 3,668,522 instances. This data set categorizes all instances into five main classes including DoS, DDoS, Reconnaissance, Theft, and Normal labels. We completed the simulation process using a laptop with the Windows 10 Pro 64-bit, Processor type AMD Ryzen 9 PRO 5945 12-Core 3.00 GHz and 32 GB RAM for experimentation. Further, the WEKA tool was used for the implementation of prediction algorithms. Table 2 shows a brief illustration of NSL-KDD and UNSW_2018_IoT_Botnet data sets with the number of instances, type of attacks, and number of existing attributes for the prediction phase. For implementing the proposed GA-RF algorithm in WEKA tool, Table 3 shows a brief illustration of specific parameters for this algorithm that was used during the experiments and the prediction process.

Table 2. Information of existing data sets based on number of instances for training and testing procedures.

Data Set	Type	Train	Test
NSL-KDD	Anomaly	58,630	12,833
	Normal	67,343	9711
UNSW_2018_IoT_Botnet	DDoS	1,541,315	330,112
	DoS	1,320,148	385,309
	Reconnaissance	72,919	18,163
	Theft	65	14
	Normal	370	107

Table 3. The specific parameters of the GA-RF algorithm in WEKA for prediction process.

Parameters	Value
Batch Size	100
Number of Iterations	100
Random Seed	1
Size of Population	20

4.2. Evaluation Parameters

The proposed model performance was tested using the ML algorithms and evaluated and analyzed by the WEKA tool. For analyzing the WEKA outcomes, we used the evaluation parameters accuracy, precision, recall, F1-Score, MAE (mean absolute error), and RMSE (root mean square error) as defined below:

(1) Accuracy illustrates the number of correctly classified anomalous behaviors in all predicted instances:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

(2) The precision factor shows anomalous behaviors with respect to the number of correctly classified positive instances:

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

(3) The recall factor shows the percentage of all correctly classified anomalous behaviors:

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

(4) The F1-score is calculated by a set of weighted factors from precision and recall:

$$F1 - Score = \frac{2 \times precision \times recall}{precision + recall} \tag{4}$$

(5) MAE and RMSE measures the average volume of the errors and the implementation and performance of a forecast model in a set of predictions, without assuming their direction.

4.3. Experimental Results

To confirm the efficacy of the proposed framework, ML algorithms have been considered as part of the experimentation. In this paper, a complete comparative examination of the evaluation parameters operated to consider all the ML methods and techniques together with the proposed framework is shown in Figure 3. The WEKA simulation results demonstrate that the performance of the proposed GA-RF algorithm according to the precision, recall, F1 score, and accuracy parameters are higher than the other ML algorithms in the NSL-KDD data set. The GA-RF algorithm achieved 99.999% for accuracy, 100% for recall and 99.99% for precision. In contrast, the naive Bayes algorithm could not achieve suitable results. The main advantage of our proposed GA-RF algorithm is that this model can select an optimal population for training procedure as an initial categorization of the forest to predict cyber-attacks. The random forest algorithm achieved 99.917% for accuracy and 99.8% for precision and recall.

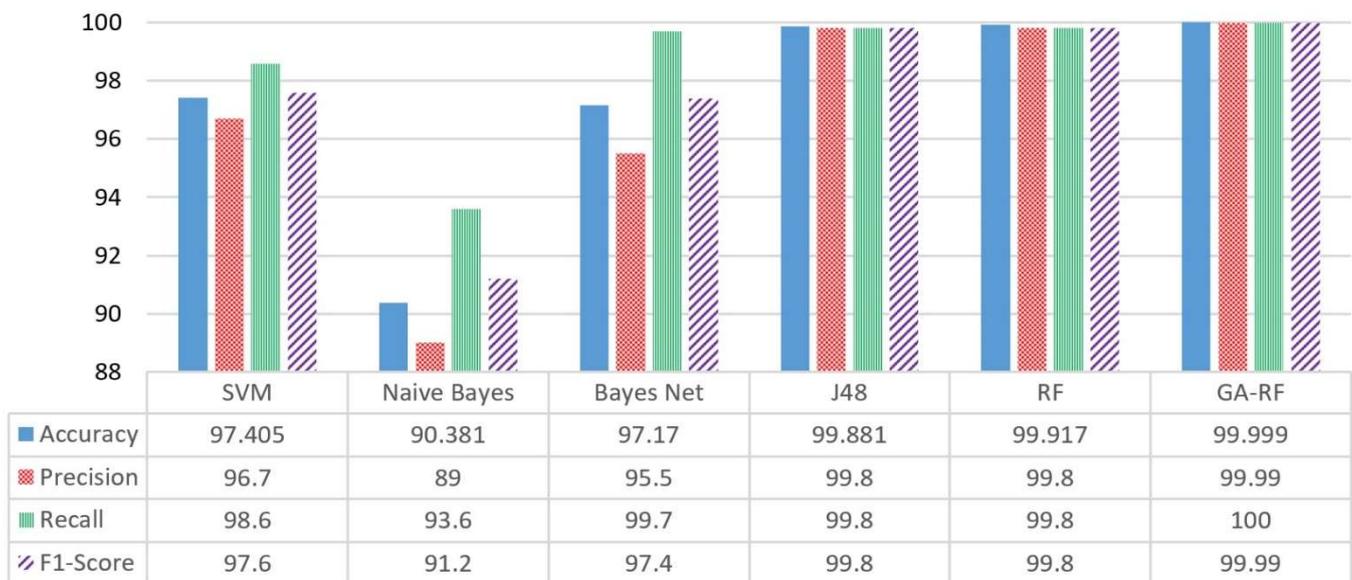


Figure 3. Comparative analysis of prediction metrics among all models in NSL-KDD data set.

Moreover, Figure 3 displays that the performance of the J48 algorithm according to the precision, recall, F1 score, and accuracy parameters are 99.881%, 99.8%, 99.8%, and 99.8%, respectively. Moreover, the performance of the Bayes Net algorithm according to the precision, recall, F1 score, and accuracy parameters are 97.17%, 95.5%, 99.7%, and 97.4%, respectively. The performance of the naive Bayes algorithm in terms of the precision, recall, F1 score, and accuracy parameters are 90.381, 89, 93.6, and 91.2, respectively. Finally, the performance of the SMV algorithm according to the precision, recall, F1 score, and accuracy parameters are 97.405%, 96.7%, 98.6%, and 97.6%, respectively.

Also, Figure 4 shows a comparative analysis of mean absolute error (MAE) and root mean square error (RMSE) among all models. The proposed GA-RF algorithm received minimum MAE with 0.0027 and RMSE with 0.0284. The random forest algorithm has the second lowest error rates for 0.0029 MAE and 0.0285 RMSE. It means that the average

volume of the errors in a set of detected malicious activities is the lowest in the GA-RF algorithm for the proposed data set.

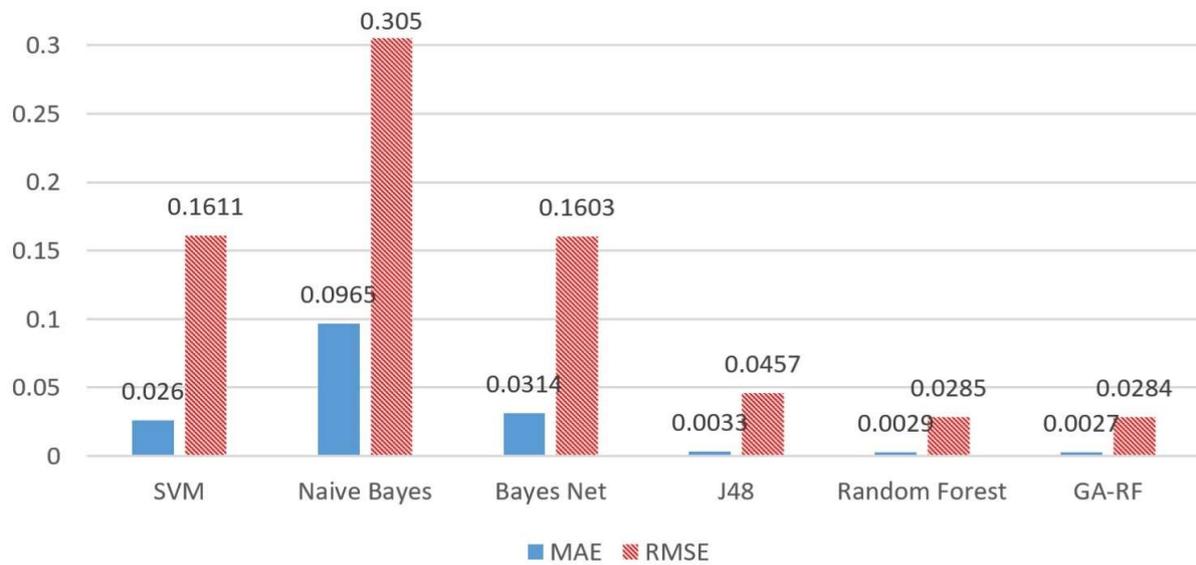


Figure 4. Comparative analysis of error rates among all models in NSL-KDD data set.

For the UNSW_2018_IoT_Botnet data set, Figure 5 illustrates a comparison of results of intrusion detection for applied GA-RF and other machine learning algorithms. The GA-RF algorithm achieved 99.999% accuracy, 100% precision, and 100% recall. Also, Figure 5 displays that the performance of the random forest algorithm according to the precision, recall, F1 score, and accuracy parameters are 99.85%, 99.88%, 99.88%, and 99.88%, respectively. Moreover, the performance of the Bayes Net algorithm according to the precision, recall, F1 score, and accuracy parameters are 99.89%, 97.7%, 97.7%, and 97.7%, respectively. The performance of the naive Bayes algorithm in terms of the precision, recall, F1 score, and accuracy parameters are 99.79%, 96%, 96% and 96%, respectively. Finally, the performance of the SVM algorithm according to the precision, recall, F1 score, and accuracy parameters are 99.74%, 89.4%, 89.4%, and 89.4%, respectively.

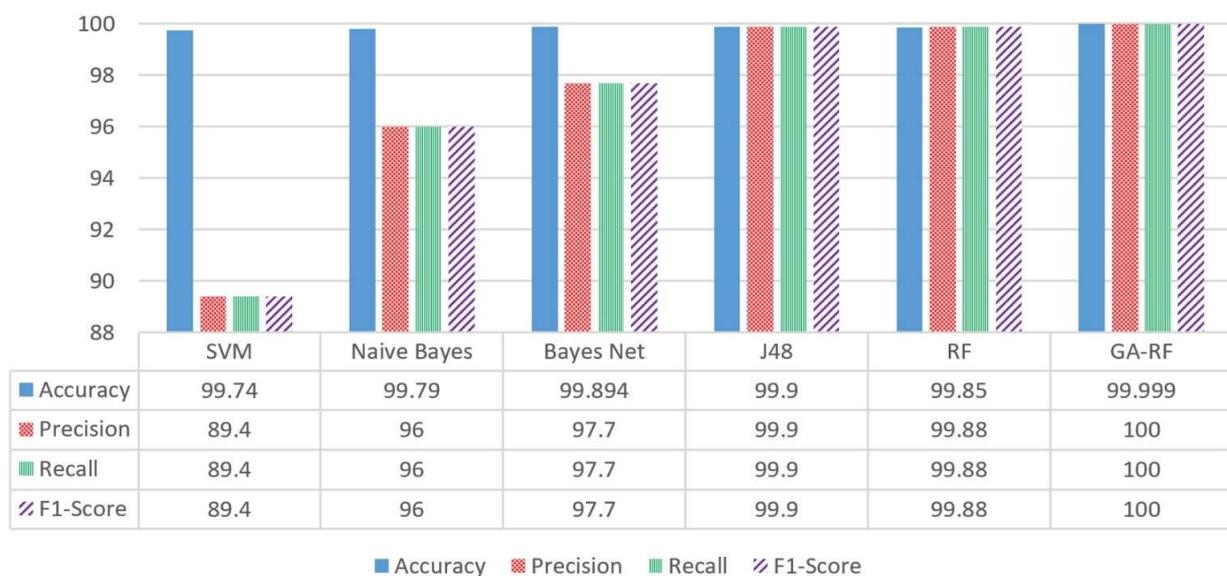


Figure 5. Comparative analysis of prediction metrics among all models in UNSW_2018_IoT_Botnet data set.

Also, Figure 6 shows experimental results of MAE and RMSE factors for UNSW_2018_IoT_Botnet data set in all algorithms. The proposed GA-RF algorithm received the minimum MAE with 0.0001 as near to zero and RMSE with 0.0021 rate. The random forest algorithm has the second lowest error rates of 0.005 MAE and 0.0027 RMSE. It means that the average volume of the errors in a set of detected cyber-attacks is the lowest using the GA-RF algorithm in UNSW_2018_IoT_Botnet data set.

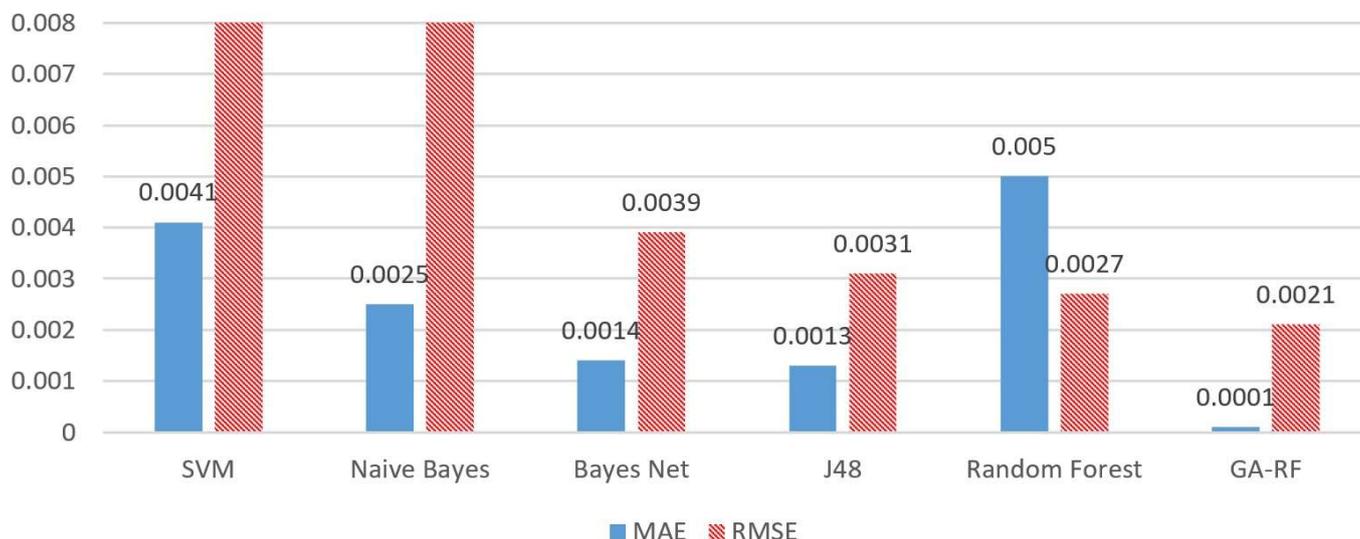


Figure 6. Comparative analysis of error rates among all models in UNSW_2018_IoT_Botnet data set.

Figure 7 illustrates existing classifications of normal activities with blue color or anomalous activities with red color for guest login status in the medical or healthcare networks. Typically, all existing attacks based on guest login accounts have applied malicious activities on the transmission control protocol (TCP). On the other hand, the number of detected anomalous activities by existing attacks based on the personal login account in the internet control message protocol (ICMP) is higher than other protocols. Also, the number of detected anomalous activities by existing attacks based on the personal login account for the TCP is higher than the number of predicted anomalous activities for the user datagram protocol (UDP).

Figure 8 shows a prediction analysis of anomalous activities identified with a red color based on server error rates in the existing protocols. When the server error rate is increased in TCP, the number of anomalous activities is increased. In other words, the TCP provides a safe status to protect against attacks and malicious activities in the intrusion detection system. On the other hand, when the server error rate of TCP is decreased to zero, the proposed intrusion detection model based on the GA-RF algorithm correctly finds normal and anomalous activities. When the server error rate of UDP is increased up to one, the proposed intrusion detection model based on the GA-RF algorithm correctly finds some anomalous activities in the IoMT. Finally, in ICMP, most of the detected anomalous activities using the GA-RF algorithm occurred in server error rate of zero.

Figure 9 shows a technical analysis of anomaly detection activities based on five main protocols in the UNSW_2018_IoT_Botnet data set. It is observed that DoS and DDoS attacks were applied on two main UDP and TCP protocols. Also, we can observe that the IPv6 protocol is a safe protocol with existing cyber-attacks in the UNSW_2018_IoT_Botnet data set.

Finally, to show efficiency of the proposed GA-RF algorithm to detect anomalous behaviors in the IoMT, we compared our simulation results with other case studies that have investigated their prediction approaches using NSL-KDD and BoTNet_IoT data sets. Table 4 illustrates the performance of the GA-RF algorithm in comparison with particle swarm optimization–recurrent neural network (PSO-RNN) algorithm, PSO–random forest (PSO-

RF) algorithm, PSO-k-nearest neighbors (PSO-KNN) algorithm, RF-synthetic minority oversampling technique (RF-SMOTE), enhanced genetic algorithm-PSO (EGA-PSO) and a hybrid convolutional neural network-Cuda deep neural network long short-term memory (CNN-cuDNNLSTM) algorithm.

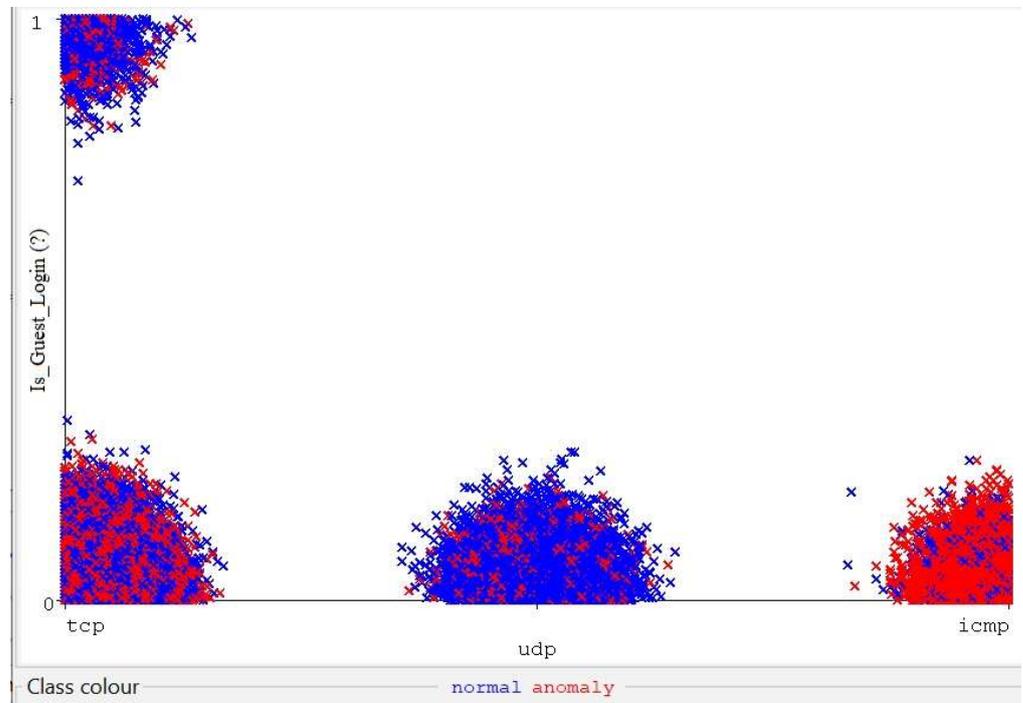


Figure 7. Anomaly detection activities based on the existing protocols as guest login status in NSL-KDD data set.

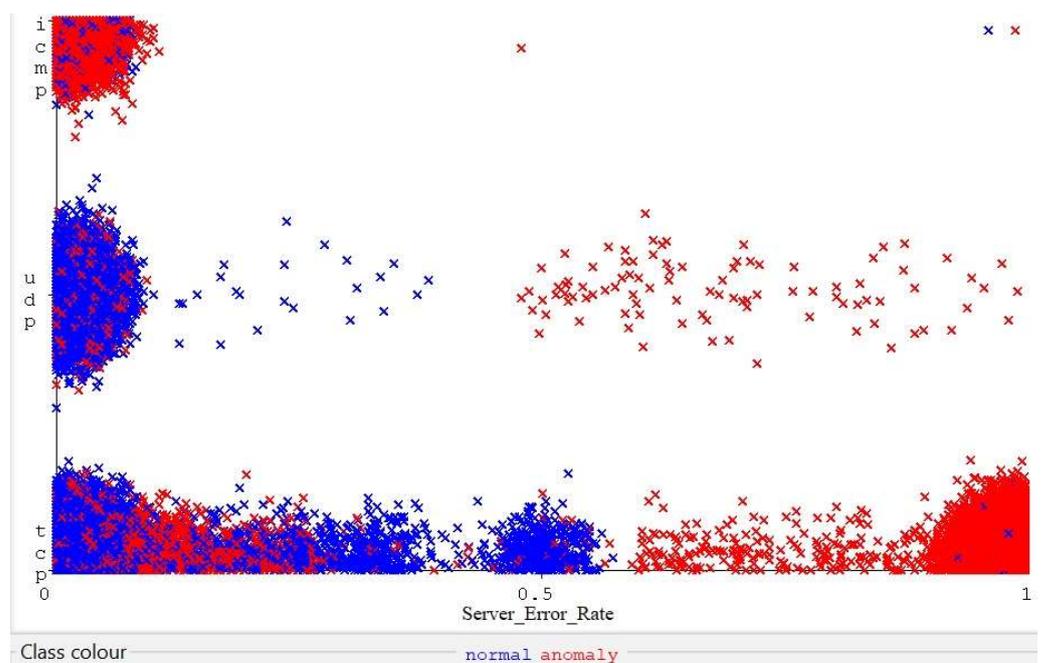


Figure 8. Anomaly detection activities based on the server error rate in NSL-KDD data set.

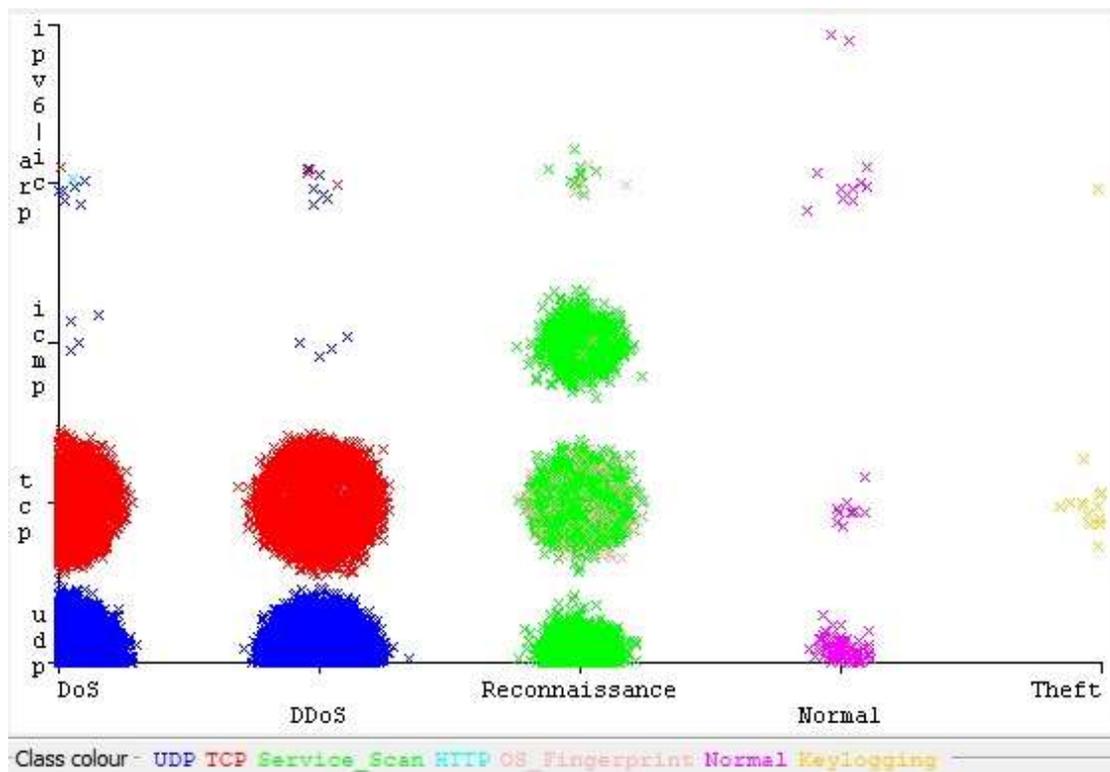


Figure 9. Anomaly detection activities based on the applied protocols in UNSW_2018_IoT_Botnet.

Table 4. Comparison results for intrusion detection with the proposed method and other case studies.

Algorithm	Accuracy	Precision	Recall
PSO-RNN [15]	96.08%	85.63%	85.63%
RF-SMOTE [29]	98.31%	98.61%	98.41%
PSO-KNN [15]	98.9%	98.89%	92.33%
EGA-PSO [30]	98.97%	99.84%	96.12%
PSO-RF [15]	99.76%	99.75	96.45
CNN-cuDNNLSTM [16]	99.99%	99.83%	99.33%
The proposed GA-RF	99.999%	100%	100%

5. Conclusions

With the rapid growth of technology, medical instruments that are widely used anywhere should increase security policies through resource limitations. Moreover, the patients probably face risks of different forms of physical harm because of the IoMT device attacks. In this study, we presented a novel IoMT framework with machine learning for intrusion detection based on GA-RF algorithm. We provided our model using the GA-RF algorithm to achieve intrusion categorization based on the existing protocols as guest login status and the server error rate with the highest accuracy in comparison with the other applied ML algorithms. The simulation results using the WEKA tool showed that the performance of the GA-RF algorithm according to the precision, recall, F1-score, and accuracy parameters is higher than the other ML algorithms. The GA-RF algorithm achieved 99.999% accuracy and 99.9% precision. Moreover, the random forest algorithm obtained 100% recall and a 99.9% F1-score. Also, the GA-RF algorithm obtained minimum error rates of 0.0027 MAE rate and 0.0284 RMSE rate for the NSL-KDD data set. It means that the average volume of the errors in a set of detected malicious activities is the lowest in the GA-RF algorithm

for the proposed data set. Finally, the GA-RF algorithm achieved 99.999% accuracy, 100% precision, and 100% recall for the UNSW_2018_IoT_Botnet data set.

Author Contributions: M.N.: Writing—original draft, visualization, resources, methodology; Z.G.-A.: Validation, writing—review and editing; Ö.C.T.: Validation; M.Y.Y.: validation; M.A.A.: Validation, writing—review and editing; A.S.: Writing—review and editing, visualization, formal analysis. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: The data sets are available as open source materials in Kaggle.

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

References

1. Verma, R. Smart city healthcare cyber physical system: Characteristics, technologies and challenges. *Wirel. Pers. Commun.* **2022**, *122*, 1413–1433. [[CrossRef](#)]
2. Gupta, B.B.; Li, K.-C.; Leung, V.C.M.; Psannis, K.E.; Yamaguchi, S. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1877–1890.
3. Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain enabled cyber-physical systems. *Sensors* **2020**, *20*, 282. [[CrossRef](#)] [[PubMed](#)]
4. Khalil, A.A.; Franco, J.; Parvez, I.; Uluagac, S.; Shahriar, H.; Rahman, M.A. A literature review on blockchain-enabled security and operation of cyber-physical systems. In Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 27 June–1 July 2022; IEEE: New York, NY, USA, 2022.
5. Sharma, M.; Pant, S.; Sharma, D.K.; Gupta, K.D.; Vashishth, V.; Chhabra, A. Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4137. [[CrossRef](#)]
6. Butun, I.; Morgera, S.D.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 266–282. [[CrossRef](#)]
7. Goel, A.; Sharma, D.K.; Gupta, K.D. LEOBAT: Lightweight encryption and OTP based authentication technique for securing IoT networks. *Expert Syst.* **2022**, *39*, e12788. [[CrossRef](#)]
8. Gupta, K.; Sharma, D.K.; Gupta, K.D.; Kumar, A. A tree classifier based network intrusion detection model for Internet of Medical Things. *Comput. Electr. Eng.* **2022**, *102*, 108158. [[CrossRef](#)]
9. 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](#)]
10. Tavallae, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; IEEE: New York, NY, USA, 2009.
11. Swarna Priya, R.M.; 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.
12. Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1969–1976. [[CrossRef](#)]
13. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. *IEEE Access* **2020**, *8*, 181560–181576. [[CrossRef](#)]
14. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access* **2020**, *8*, 77396–77404. [[CrossRef](#)]
15. 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](#)]
16. Liaqat, S.; Akhunzada, A.; Shaikh, F.S.; Giannetsos, A.; Jan, M.A. SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). *Comput. Commun.* **2020**, *160*, 697–705. [[CrossRef](#)]
17. Khan, I.A.; Moustafa, N.; Razzak, I.; Tanveer, M.; Pi, D.; Pan, Y.; Ali, B.S. XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. *Future Gener. Comput. Syst.* **2022**, *127*, 181–193. [[CrossRef](#)]
18. 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](#)]
19. Adnan, M.N.; Islam, M.Z. Optimizing the number of trees in a decision forest to discover a subforest with high ensemble accuracy using a genetic algorithm. *Knowl. Based Syst.* **2016**, *110*, 86–97. [[CrossRef](#)]

20. Elyan, E.; Gaber, M.M. A genetic algorithm approach to optimising random forests applied to class engineered data. *Inf. Sci.* **2017**, *384*, 220–234. [[CrossRef](#)]
21. Choudhary, S.; Kesswani, N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. *Procedia Comput. Sci.* **2020**, *167*, 1561–1573. [[CrossRef](#)]
22. 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](#)]
23. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [[CrossRef](#)]
24. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Slay, J. Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In Proceedings of the Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, 13–15 December 2017; Springer: Berlin/Heidelberg, Germany, 2018.
25. Koroniotis, N.; Moustafa, N.; Sitnikova, E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Gener. Comput. Syst.* **2020**, *110*, 91–106. [[CrossRef](#)]
26. Koroniotis, N.; Moustafa, N. Enhancing network forensics with particle swarm and deep learning: The particle deep framework. *arXiv* **2020**, arXiv:2005.00722.
27. Koroniotis, N.; Moustafa, N.; Schiliro, F.; Gauravaram, P.; Janicke, H. A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access* **2020**, *8*, 209802–209834. [[CrossRef](#)]
28. Koroniotis, N. Designing an Effective Network Forensic Framework for the Investigation of Botnets in the Internet of Things. Ph.D. Thesis, UNSW Sydney, Sydney, Australia, 2020.
29. Karthik, M.G.; Krishnan, M.B.M. Hybrid random forest and synthetic minority over sampling technique for detecting internet of things attacks. In *Journal of Ambient Intelligence and Humanized Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–11. [[CrossRef](#)]
30. Balyan, A.K.; Ahuja, S.; Lilhore, U.K.; Sharma, S.K.; Manoharan, P.; Algarni, A.D.; Elmannai, H.; Raahemifar, K. A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. *Sensors* **2022**, *22*, 5986. [[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.