processes

MDPI

Article

Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network

Kedalu Poornachary Vijayakumar [1,*], Krishnadoss Pradeep [1], Ananthakrishnan Balasundaram [2] and Manas Ranjan Prusty [2]

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
[2] Center for Cyber Physical Systems, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
* Correspondence: vijayakumar.kp@vit.ac.in

Abstract: Internet of Health Things plays a vital role in day-to-day life by providing electronic healthcare services and has the capacity to increase the quality of patient care. Internet of Health Things (IoHT) devices and applications have been growing rapidly in recent years, becoming extensively vulnerable to cyber-attacks since the devices are small and heterogeneous. In addition, it is doubly significant when IoHT involves devices used in healthcare domain. Consequently, it is essential to develop a resilient cyber-attack detection system in the Internet of Health Things environment for mitigating the security risks and preventing Internet of Health Things devices from becoming exposed to cyber-attacks. Artificial intelligence plays a primary role in anomaly detection. In this paper, a deep neural network-based cyber-attack detection system is built by employing artificial intelligence on latest ECU-IoHT dataset to uncover cyber-attacks in Internet of Health Things environment. The proposed deep neural network system achieves average higher performance accuracy of 99.85%, an average area under receiver operator characteristic curve 0.99 and the false positive rate is 0.01. It is evident from the experimental result that the proposed system attains higher detection rate than the existing methods.

Keywords: cyber-attack; deep learning; IoHT

Citation: Vijayakumar, K.P.; Pradeep, K.; Balasundaram, A.; Prusty, M.R. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. *Processes* **2023**, *11*, 1072. https://doi.org/10.3390/pr11041072

Academic Editors: Guo-Shiang Lin, Ming-Te Chen, Chieh-Ling Huang, Yi-Ying Chang and Jie Zhang

Received: 6 February 2023
Revised: 13 March 2023
Accepted: 21 March 2023
Published: 3 April 2023

1. Introduction

Internet of Things (IoT) is an evolving paradigm that facilitates communication between sensors and electronic devices over the Internet [1]. IoT is applied in various applications such as smart home [2,3], smart industries [4], smart cities [5], transportation [6], smart healthcare [7] and satellites [8]. Internet of Health Things (IoHT) is essentially an IoT-based solution that permits the connection between a patient and health care amenities such as electrocardiography [9], heart rate [10], electroencephalogram [11], diabetes [12] and various sensors which comprises of airflow (breathing), pulse, body temperature, oxygen in blood (SPO2), glucometer, blood pressure, galvanic skin response, electromyography and patient position (accelerometer), and [13,14].

IoT is widely implemented in several health care fields. Most of the devices in IoT use wireless communication for transmission and reception of data that leads to risk of wireless sensor network (WSN) security violations in IoHT [15]. In addition, the Internet is the primary source of security threats and is vulnerable to various kinds of cyber-attacks such as Denial-of-Service attack [16], network sniffing, theft of medical record [17] and treatment manipulation in IoHT environments.

The intention of cyber-attack is to ruin and disturb the operation of a computer network [18]. Cyber-attacks can be categorized into Denial-of-Service (DoS), logical bomb, Sniffer, Trojan horse, Virus, Worm, Send spam, and Botnet. DoS attack precludes the system from using the internet or communicating with other systems. Attacks may be launched

from either single source or multiple distributed sources instantaneously. Logic bomb attacks carry out destructive activity by using a malicious program. Sniffer overhears transmission of data and obtains specific data such as a password.

Cyber security plays a vital role in protecting information and network from various cyber-attacks. Consequently, it is essential to devise an approach for detecting various types of attacks in IoHT. Aside from safety risks, the datasets associated with the cyber-attacks are publicly not available in the medical field due to sensitive data at risk since it can harm and lead to the death of the patients [19]. In order to address the above risks, we use the novel ECU-IoHT dataset [20] that reflects various cyber-attacks.

There exists a variety of intrusions detection approaches that are relying on cluster analytics, statistical analytics and artificial neural network or deep learning [21]. Among these approaches, the intrusion detection approach relying on deep learning achieves greater performance compared to other various approaches since deep learning has an elevated capability for self-learning and adaption, generalization and detection of behavior of unknown attack.

Researchers discovered numerous intrusion detection systems (IDS) for preventing network from various assaults. Albeit an enormous exertion by the researchers, IDS still struggles in identifying new assaults and rising detection accuracy while reducing false detection rate [22]. To address this issue, many researchers are turning to artificial intelligence [23], machine learning and deep learning approaches [24] for detecting cyber assaults in IoT environment. The deep learning method has proved its ability to learn valuable features from the dataset since it has deep architecture devoid of human involvement [1]. Deep neural network (DNN) approach is extensively applied in various domains such as network security, natural language processing, computer vision, cancer detection [25], speech recognition, and robotics [26].

Bearing the above issues in mind, this paper presents the cyber-attack detection system using deep learning approach for detecting various types of cyber-attacks such as ARP Spoofing, DoS attacks, Nmap Port Scan and Smurf attacks in IoHT, unlike the existing approach [19]. To the best of our knowledge, the proposed system using deep learning approach is novel, classifying various types of attacks and elevating the performance in terms of accuracy in multiclass classification in IoHT environment.

The primary innovations and contributions of this paper are as follows:

- Detection of various types of attacks by applying deep learning approach rather than detection of specific type of attacks [19] in IoHT environment.
- The proposed method uses a new dataset ECU-IoHT in the domain of health care [20] to train and evaluate the model. The reason behind selection of the ECU-IoHT dataset is the fact that many datasets are publicly available, such as, for example, DARPA 98, KDD Cup 99, NSL-KDD, Morre, UNSW-NB15, BOT-IoT, ToN-IoT, ISCX, Kyoto and SCADA, which are inappropriate in the domain of health care.
- The proposed system achieves higher detection accuracy by analyzing an enormous amount of data (ECU-IoHT dataset consist of 111,207 numbers of samples).

The rest of the paper is organized as follows: Literature survey is presented in Section 2. Proposed system is described in Section 3. Result and discussions are explained in Section 4. The conclusion of this paper is provided in Section 5.

2. The Literature Survey

The datasets associated with the cyber-attacks are publicly not available in the medical field due to sensitive data at risk since it can harm and lead to the death of the patients. Thus, the authors of [19] developed new dataset ECU-IoHT [20] that reflects various cyber-attacks such as ARP Spoofing, DoS attacks, Nmap PortScan and Smurf attacks in IoHT. Four kinds of approaches such as K-Nearest Neighbor, clustering, statistical and one class support vector machine were implemented using Rapid Miner tool. In clustering category, K-Nearest Neighbor (KNN), Local Outline Factor (LOF), Connectivity-based Outline Factor (COF), approximate Local Correlation Integral (aLOCI), Local Outlier Probability (LoOP)

and Influenced Outlierness (INFLO) were considered. In clustering, Cluster-based Local Outlier Factor (CBLOF), Clustering-based Multivariate Gaussian Outlier Score (CMGOS), Local Density Cluster-based Outlier Factor (LDCOF) were considered. In statistical category, Robust Principal Component Analysis (RPCA) and Histogram-based Outlier Score (HBOS) were considered. The evaluation exhibited that INFLO and LOF algorithms was superior in detecting ARP Spoofing, Nmap PortScan, Smurf attacks and DoS attacks, respectively.

The machine learning methods (decision tree (DT), naïve Bayes (NB), linear regression (LR), random forest (RF), K-Nearest Neighbor (KNN), and support vector machines (SVM) were applied for IoT anomaly intrusion detection using six different datasets [21]. The assessment results exhibited that the DT, RF and KNN methods provided higher detection rate compared to other algorithms used. These algorithms have the ability to ascertain whether there is an attack or not since this study considered only binary classification.

The deep belief neural network models were used to detect various attacks, namely botnet, brute force, DoS, infiltration and ports using CICIDS 2017 dataset [27]. This dataset was obtained for five continuous days between Monday and Friday with normal class and various attacks such as botnet, brute force, DDoS, Infiltration, PortScan, and web attack which may cause IoT system failure. The proposed approach in [27] achieved accuracy of 99.37%, 99.93%, 97.71%, 96.67%, 96.37%, 97.71% and 98.37% for normal class, botnet, brute force, DDoS, infiltration, PortScan and web attack, respectively.

This model achieved better accuracy in detecting various attacks, and was unable to be used in classification and recognition. The studies were conducted on deep and swallow neural network utilizing publicly available dataset and exhibited the performance of 98.27% and 96.75%, respectively, in terms of accuracy [28]. Intrusion detection system using machine learning approach was implemented in Weka tool to recognize DoS attacks [29]. Intrusion detection system devised by employing machine learning methods in [30] used mobile and cluster head agent technologies to safeguard network and find anomalies. The intention of the paper in [31] is to detect substantial solutions to secure, forecast and improve vaccine productions and supply chains. Various collections of algorithmic solutions provided a possibility of predicting risks during a Disease X event. The purpose of the study in [32] is to create an autonomous heath care system for prognostic cyber risk analysis and forecasting medical production and supply chain bottlenecks during future pandemics.

Intensive care unit (ICU) is committed for patient caring. The ICU medical devices are typically utilized for monitoring the present condition of patients for those who are admitted in the ICU [33]. There are several medical devices broadly used as ICU medical devices such as ECG, glucose meter, syringe pump, etc. These devices are easily susceptible to many attacks such as DoS attacks, man-in-the middle attack, ransomware, etc. The study shows that many researchers employed machine learning approaches on medical information mart for intensive care (MIMIC) dataset [34], which consists of discrete structured clinical data, physiological waveforms data, free text documents, and radiology imaging reports.

From the above studies, some of the issues identified are: (i) anomaly detection using statistical methods needs significant amount of repetitions for training the model; in addition, the threshold used to detect anomalies may not suitable for real time scenario, (ii) cluster-based methods lead to time consumption and are inappropriate for anomaly detection, (iii) lack of openly accessible datasets that reflects cyber assaults in the Internet of Medical Things. To fulfill this research gap, this paper presents (i) the cyber-attack detection system using deep learning approach for detecting various types of cyber-attacks such as ARP Spoofing, DoS attacks, Nmap PortScan and Smurf attacks in IoHT and (ii) supports multi-class classification by assimilating the ability of discriminating which type of attack corresponds to a particular malicious incident.

3. Proposed System

This section provides the various cyber-attacks considered in the proposed system. The concept of the deep neural network and the methodology of the proposed system are described in this section.

3.1. Anomaly Detection

Detection of anomaly is an essential cyber safety analysis process for detecting unusual information from a dataset [35]. Anomaly is classified into point, collective and contextual anomaly based on its nature [36]. Novel anomaly or transformation of ancient anomaly is created in IoT environment due to immersion of enormous amount of data [1]. The proposed model considers four types of attacks such as ARP Spoofing, DoS attacks, Nmap PortScan and Smurf attacks.

Address Resolution Protocol (ARP) provides the association between IP address and a MAC address to evade the IP conflict in the network. ARP Spoofing is also referred to as ARP Poisoning; it transmits the fake data over the local area network [37] as well as forwards the data flow the envisioned host to the attackers. Denial-of-Service (DoS) attack proscribes to access the authorized resources [38]. Network mapper (Nmap) is the scanning tool to detect Nmap scanning activities for identifying vulnerabilities [39]. Smurf attack is a kind of distributed DoS attack; it behaves similarly to ping floods and exploits the behaviors of broadcast networks to magnify the attack traffic considerably.

3.2. Deep Nerual Network

Deep Neural Network (DNN) is referred to as deep learning; it is a part of artificial intelligence (AI) [26] and belongs to the family of supervised techniques for training the model through multiple layers. The structure of DNN includes input layer, multiple hidden layers and an output layer. Consider X = {x1, x2, . . . , xn} is the input vector with n = 5 features and Y = {y1, y2, . . . , yn} is the output vector consisting the probability values in the range of [0,1] and values add to 1 to classify normal (no attack) and abnormal (ARP Spoofing, DoS attack, Nmap PortScan and Smurf attack) attacks. The output estimation of each hidden layer (HL) is given in Equation (1):

$$HLi = A\left(w^T i + bi\right), \tag{1}$$

where $A(.)$ denotes nonlinear activation function, (w_i) and bi denote the hidden layer (i)'s weight and bias. "ReLU" and "softmax" activation functions are applied in hidden layer and output layer, respectively. The ReLU activation function is accomplished by using Equation (2):

$$ReLU(x) = \max(0, x). \tag{2}$$

Softmax contains a vector in the range of (0, 1) that is applied to the result scores (rs). Each element denotes a class and has the ability to understand the class probabilities. The softmax function is applied on all elements of rs. For any given class rs_i, the softmax function is computed as given in Equation (3):

$$f(rs_i) = \frac{\exp rs_i}{\sum_j^C \exp rs_j}, \tag{3}$$

where rs_j are the result scores inferred by the net for each class in C. The softmax activation function for a class rs_i is relying on all the scores in rs.

The structure of the DNN employed in the proposed system comprising of input layer with five neurons denoting the feature set; two dense layers are applied with eight neurons followed by softmax classification layer consisting of five outputs to denote the normal and abnormal attacks (ARP Spoofing, DoS attack, Nmap attack and Smurf attack) as shown in Figure 1. In the experimentation, only numerical features are considered, whereas the categorical features are transformed into numerical features using one-hot

encoding. The model is built with input layer, which entails five neurons, followed by two dense layers (each with eight neurons) and output layer with softmax activation function to categorize into normal or abnormal attacks (ARP Spoofing, DoS attack, Nmap attack and Smurf attack).

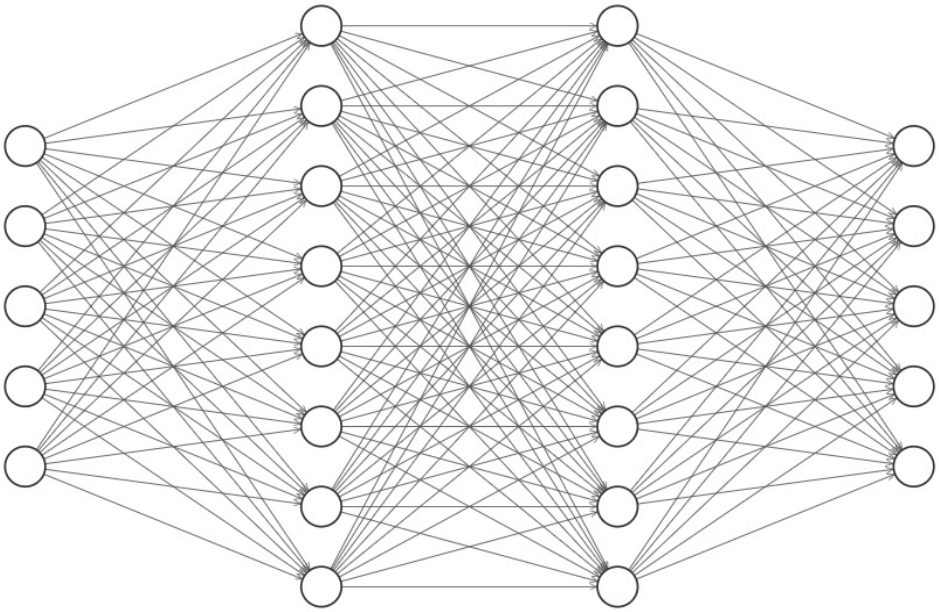

Figure 1. System Model.

3.3. Methodology

The proposed system consists of two phases for detecting the various types of cyber-attacks such as ARP Spoofing, DoS attacks, Nmap attacks and Smurf attacks in IoHT as shown in Figure 2. The two phases are (i) data preparation phase and (ii) DNN-based attack detection phase. The various stages followed to implement and assess DNN model are described as follows: (i) the ECU IoHT dataset [20] is used for analyzing various cyber-attacks; (ii) five features are extracted from this dataset and one-hot encoding is used for encoding categorical features; (iii) the dataset is labeled as Normal, ARP Spoofing, DoS attack, Nmap attack and Smurf attack for preparing for the multi-class classification; (iv) the dataset is split into training and testing dataset of 80% and 20%, respectively; (v) the DNN is trained on the training dataset by choosing these labels as target features using multiclass classification, and it provides a trained model; (vi) the trained DNN model is tested by using testing dataset for predicting normal or other types of attacks.

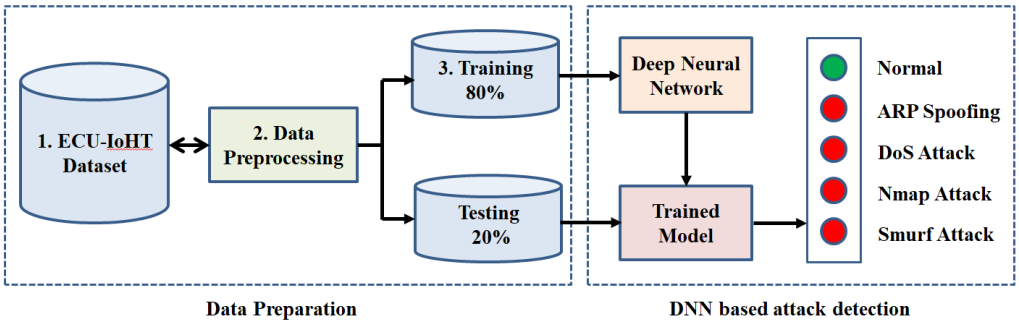

Figure 2. Proposed System.

3.3.1. Description of Dataset

There are many datasets, namely DARPA, KDD Cup 99, NSL–KDD, Moore, UNSW-NB 15, BOT-IoT, ToN-IoT, ISCX, Kyoto and SCADA which were used by many researchers for designing and evaluating the network intrusion detection. However, none of the abovementioned datasets was used for evaluation of device security in the healthcare domain [19]. Therefore, a novel dataset ECU-IoHT [20] in health care domain is used for evaluating the proposed deep learning approach in this paper. The dataset consists of 111,207 samples, including normal and various other types of attacks. The detailed description of the number of counts for normal and other attack labels such as ARP Spoofing, DoS attacks, Nmap Port Scan and Smurf attacks in the original dataset is given in Table 1.

Table 1. Description of ECU-IoHT dataset.

Category	ECU-IoHT	ECU-IoHT in Proposed System		
	Counts	Counts	Training (80%)	Training (20%)
No Attack/Normal	23,453	23,453	18,780	4673
ARP Spoofing	2359	2359	18,780	4673
DoS Attack	639	639	525	114
Nmap PortScan	6836	6836	5510	1326
Smurf Attack	77,920	77,920	62,218	15,642

3.3.2. Data Preprocessing

The original dataset consists of a total of 11 features. Among these features, five features (type, source packets, destination packets, type of protocol, length) are extracted and used to explore the performance of the proposed system. The extracted features are in the form of numerical and categorical. The categorical features are transformed into numerical features using one-hot encoding as shown in Algorithm 1 since merely numerical features are considered in the experimentation. In Algorithm 1, the dataset is denoted by D(f1, f2, . . . , fn), 1 < n < N, where N is the total number of features considered (five features) in the dataset.

Algorithm 1: One-hot encoding for encoding categorical data

```
Input: D(f1,f2, . . . , fn)
IOutput: Dencoded(f1encoded, . . . , fn encoded)
For i from 1 to N do
        If (fi is a categorical input)
        Encode using one hot encode method
End if
End for
```

3.3.3. Proposed DNN Structure

The proposed structure of the DNN employed in the proposed system is comprised of input layer with five neurons denoting the feature set; two dense layers are applied with eight neurons followed by softmax classification layer consisting of five outputs to denote the normal and abnormal attacks (ARP Spoofing, DoS attacks, Nmap attacks and Smurf attacks) as shown in Figure 3. In the experimentation, only numerical features are considered, whereas the categorical features are transformed into numerical features using one-hot encoding. The model which is built with the input layer entails five neurons, followed by two dense layers (each with eight neurons) with ReLU activation function and output layer with softmax activation function to categorize into normal or abnormal attacks (ARP Spoofing, DoS attacks, Nmap attacks and Smurf attacks).

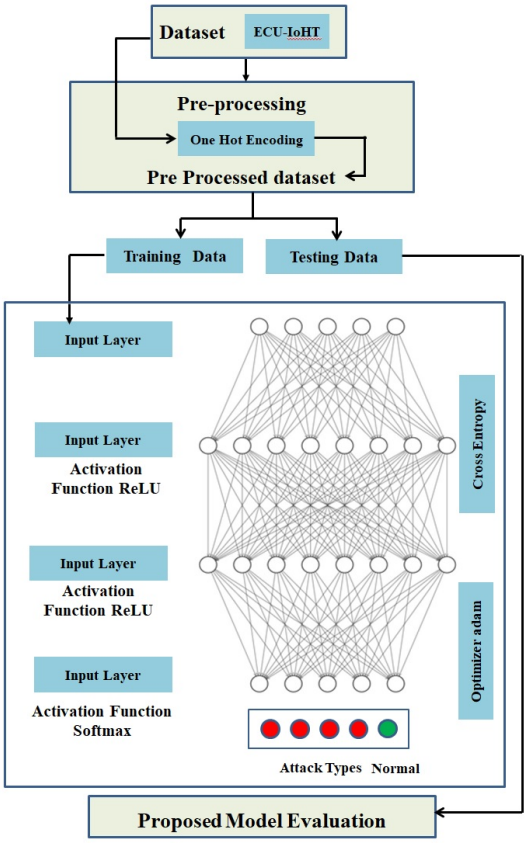

Figure 3. Proposed DNN structure.

4. Results and Discussions

The evaluation metrics, environmental setup and the result of proposed system to detect cyber-attacks in IoHT are presented in this section.

4.1. Evaluation Metrics

The proposed system's performance is evaluated by using Accuracy, Precision, Recall, F1-Score, True Positive Rate and False Positive Rate parameters. Accuracy is estimated as the ratio of accurately classified records to the total number of records or counts as in Equation (4):

$$Accuracy = (TP + TN)/(TP + TN + FP + FN). \quad (4)$$

Precision is the ratio of accurately predicted abnormal instances to all the instances predicted as abnormal as given in Equation (5):

$$Precision = TP/TP + FP. \quad (5)$$

Recall is the ratio of all the accurately predicted abnormal instances to the entire actual abnormal instance as given in Equation (6):

$$Recall = TP/TP + FN. \quad (6)$$

F1 Score offers the harmonic mean of the Precision and Recall for examining the system's accuracy as given in Equation (7):

$$F1Score = 2((Precision * Recall)/(Precision + Recall)). \quad (7)$$

The accuracy is also measured by Receiver Operating Characteristics (ROC) curve and Area Under the ROC curve (AUC). This metric denotes the likelihood of a randomly

selected positive test point having a higher possibility of being predicted more positive than a randomly selected negative test point [40].

4.2. Environmental Setup

To implement and evaluate the proposed approach on the ECU-IoHT dataset, the experiment is conducted on the DELL laptop installed with Windows 10 OS, 16 GB RAM with Intel Core I5-10210U processor. Spyder Python (version 3.8) is used as an implementation tool with some libraries such as matplotlib (version 3.3.2), Numpy (version 1.19.2), Pandas (1.1.3), Scikit-learn (version 0.23.2), Keras (version 2.6.0) and Tensor flow (version 2.6.0).

4.3. Discussion

The proposed approach is applied on a dataset which consists of normal instances as well as abnormal instances for detecting various types of attacks in IoHT. In the proposed DL approach, ReLU and softmax are used as activation functions, and we selected the batch size of 64, with Optimizer as Adam and loss function as categorical cross entropy.

The model is trained with different epoch values between 100 and 500. The training time of the proposed model with 100 and 500 epochs is 2482 and 5459 s, respectively. The model with 500 epochs provided the maximum validation accuracy and minimum loss. The proposed model's performance in terms of accuracy and loss with 100 epochs is given in Figures 4 and 5.

Figure 4. Training and validation accuracy with 100 epochs.

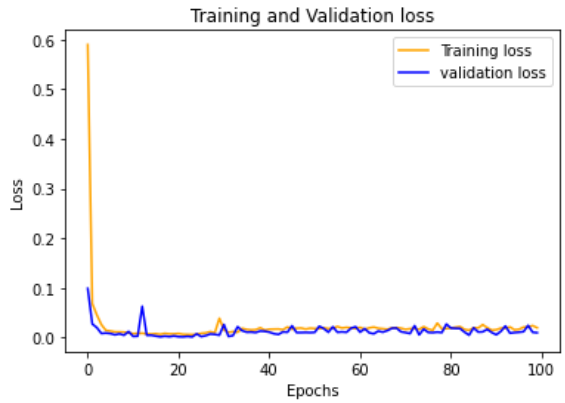

Figure 5. Training and validation loss with 100 epochs.

The proposed model's performance in terms of accuracy and loss with 500 epochs is given in Figures 6 and 7.

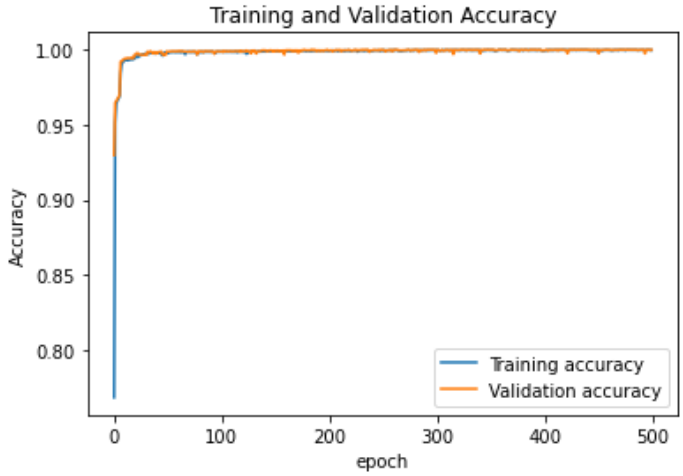

Figure 6. Training and validation accuracy with 500 epochs.

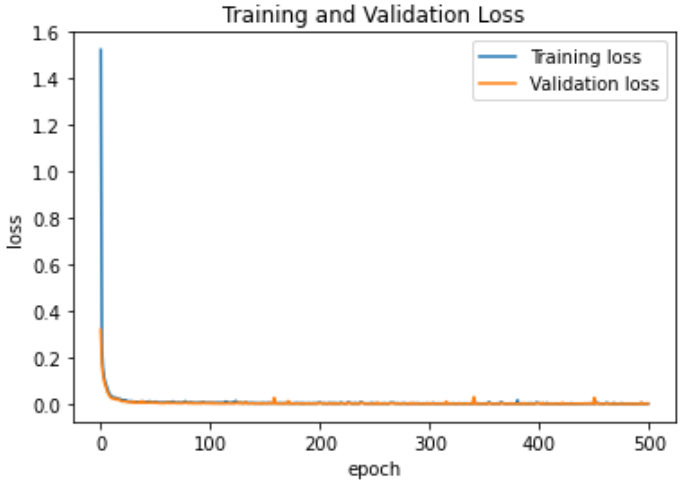

Figure 7. Training and validation loss with 500 epochs.

From Figures 6 and 7, the proposed system with 500 epochs substantially enhances the detection accuracy to 100%. Thus, from the experimental result, it is evident that the proposed system with DNN performs well for detecting various attacks compared to the existing system [19].

Figures 8 and 9 illustrate the ROC curve for detecting various classes. Numbers 0, 1, 2, 3, and 4 denote ARP Spoofing, DoS attacks, Nmap attacks, normal behavior and Smurf attacks, respectively. This model ran for 50 iterations, and it is evident from the ROC curve that the TDR achieves highest accuracy and negligible FDR in identifying the presence of cyber-attacks with 500 epochs. From Figures 8 and 9, it can be observed that the ROC curve is on the top left corner of the image, which is an indicator of good classification of results.

Figure 10 shows the comparison of performance of the proposed model with 100 and 500 epochs using Accuracy, average Precision, Recall and F1 Score. The result shows that the model with 500 epochs is superior to others using Accuracy, average Precision, Recall and F1 Score parameters.

Figure 11 shows the performance of the proposed model with 500 epochs using Precision, Recall and F1 Score for various types of attacks (ARP Spoofing, DoS attacks, Nmap Port Scan, Smurf attacks). Thus, the proposed approach is superior and most suitable for detecting normal class and various attacks such as ARP spoofing, Nmap and Smurf attacks.

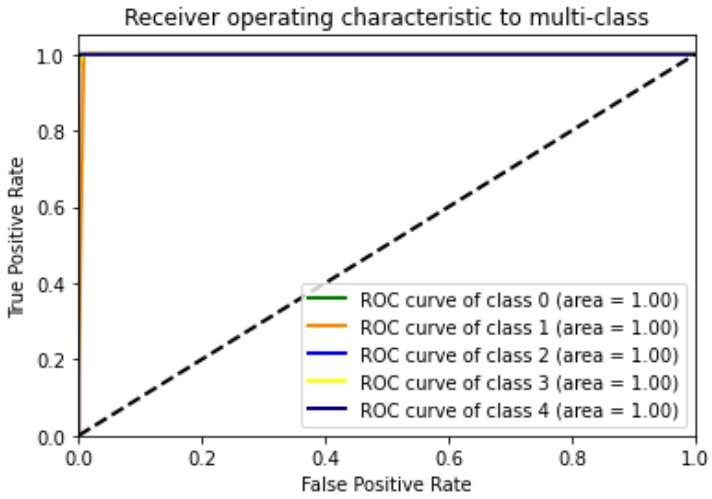

Figure 8. Receiver operating characteristics curve for 100 epochs.

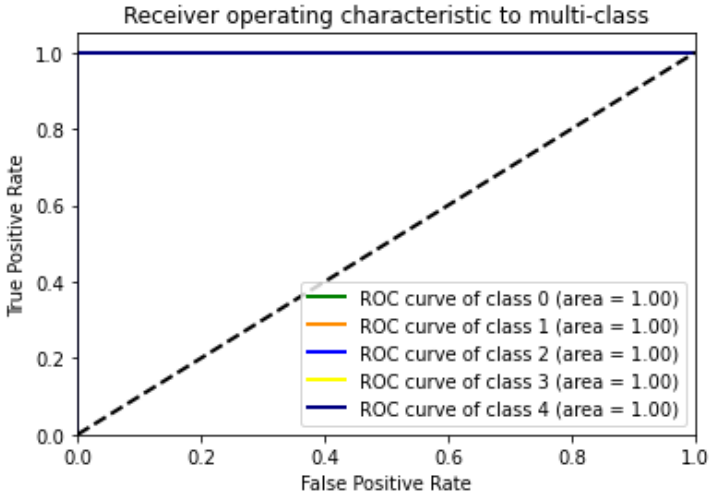

Figure 9. Receiver operating characteristics curve for 500 epochs.

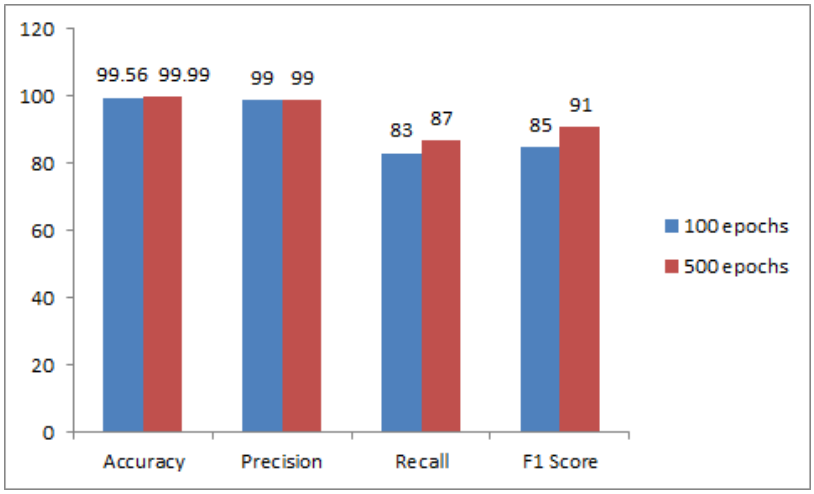

Figure 10. Comparison of performance of the proposed model with 100 and 500 epochs.

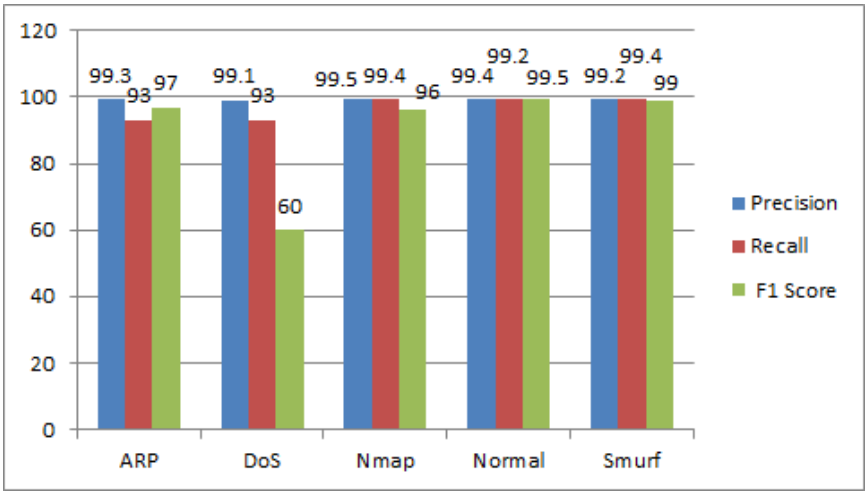

Figure 11. Performance of the proposed model on various attacks.

The deep belief neural network models were used to detect various attacks, namely botnet, brute force, DDoS, infiltration, PortScan and web attack using CICIDS 2017 dataset [27]. The performance evaluation of the deep belief network is modeled for detection of various other types of attacks compared to the attacks considered in our proposed system. However, the overall performance of proposed system is compared with the deep belief network as shown in Table 2. From Table 2, it is apparent that the proposed system performs better for detection of normal class and Nmap PortScan attack compared to the existing system.

Table 2. Comparison of performance of proposed with existing system.

Systems/ Attacks		ARP	DoS	Nmap	Normal	Smurf
Proposed System (%)	Precision	99.3	99.1	99.5	99.4	99.2
	Recall	93	93	99.4	99.2	99.4
	F1 Score	97	60	96	99.5	99
Existing System [27] %	Precision			96.12	96.21	
	Recall			96.24	98.34	
	F1 Score			97	97	
Existing DM System [28] %	Precision		97	98.56	99.52	
	Recall		99.5	99	97.43	
	F1 Score		98.47	98.78	98.47	
Existing SM System [28] %	Precision		96.55	87.44	99.35	
	Recall		99	99.48	95	
	F1 Score			93		
Existing SM System [29] %	Precision			97.7		
	Recall			97.7		
	F1 Score			97.7		

Serena Nicolazzo et.al. [41] proposed privacy preserving methods for preventing feature disclosure in the development of the Internet of Things. The proposed method focused on protecting sensitive information as well as user privacy by hiding features of objects. In [42], the authors proposed a framework for detecting various anomalies in the scenario of multiple Internet of Things (MIoT). In future, in our proposed approach, the aspect of privacy management and handling the anomalies in MIoT will be the main focus.

5. Conclusions

This work presents a DNN-based approach that enhances the process of detecting and mitigating cyber-attacks in IoHT devices, thereby ensuring the safety of healthcare devices using IoT. The proposed system is designed to focus on multi-class classification to detect ARP Spoofing, DoS attacks, Nmap attacks and Smurf attacks as well as the work assessed by considering health care domain (ECU-IoHT) dataset unlike the existing system built on binary class classification to detect various types of attacks. The experimental result highlights that the proposed DNN-based process attains significantly high true detection rate and negligible false detection rate compared to the existing system. An accuracy of over 99% was obtained when the proposed system was trained with 500 epochs. In addition, the Precision, Recall and F1 Scores were significantly high. The average precision, Recall and F1 Score values for the proposed system were 99.3%, 96.8 and 90.3%, respectively. This clearly underlines that the proposed system evidently outperforms the contemporary works. In the future, the proposed system can be applied for testing its efficiency in the real-time IoHT environment, and the focus will also be directed towards increasing the scalability of this work for detecting other types of attacks in IoHT devices.

Author Contributions: Conceptualization, K.P.V.; methodology, K.P.V.; software, K.P.; validation, K.P.V., A.B. and M.R.P.; formal analysis, K.P.V.; investigation, K.P.; data curation, K.P.; writing—original draft preparation, K.P.V.; writing—review and editing, K.P.; visualization, A.B. and M.R.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: ECU-IoHT, 2020, [online] http://dx.doi.org/10.25958/5f1f97b837aca (accessed on 10 January 2023).

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

References

1. Ahmad, Z.; Shahid Khan, A.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J.P.C. Anomaly detection using deep neural network for IoT architecture. *Appl. Sci.* **2021**, *11*, 7050. [CrossRef]
2. Huang, Z. Analysis of IoT-based smart home applications. In Proceedings of the IEEE International Conference on Computer Science, Artificial Intelligence and Electronic Engineering (CSAIEE), SC, USA, 20–22 August 2021.
3. Ma, L.; Li, Z.; Zheng, M. A research on IoT based smart home. In Proceedings of the 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Qiqihar, China, 28–29 April 2019.
4. Tabaa, M.; Monteiro, F.; Bensag, H.; Dandache, A. Green industrial internet of things from a smart industry perspectives. *Energy Rep.* **2020**, *6*, 430–446. [CrossRef]
5. Brincat, A.A.; Pacifici, F.; Martinaglia, S.; Mazzola, F. The internet of things for intelligent transportation systems in real smart cities scenarios. In Proceedings of the IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019.
6. Alluhaidan, A.S.; Alluhaidan, M.S.; Basheer, S. Internet of things based intelligent transportation of food products during COVID. *Wirel. Pers. Commun.* **2021**, *127*, 27. [CrossRef]
7. Harb, H.; Mansour, A.; Nasser, A.; Cruz, E.M.; de la Torre Díez, I. A sensor-based data analytics for patient monitoring in connected healthcare applications. *IEEE Sens. J.* **2021**, *21*, 974–984. [CrossRef]
8. Centenaro, M.; Costa, C.E.; Granelli, F.; Sacchi, C.; Vangelista, L. A survey on technologies, standards and open challenges in satellite IoT. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1693–1720. [CrossRef]
9. Deb, S.; Islam, S.M.R.; RobaiatMou, J.; Islam, M.T. Design and implementation of low cost ECG monitoring system for the patient using smart device. In Proceedings of the International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 16–18 February 2017.
10. Li, C.; Hu, X.; Zhang, L. The IoT-based heart disease monitoring system for pervasive healthcare service. *Proc. Comput. Sci.* **2017**, *112*, 2328–2334. [CrossRef]
11. Vergara, P.M.; de la Cal, E.; Villar, J.R.; González, V.M.; Sedano, J. An IoT platform for epilepsy monitoring and supervising. *J. Sens.* **2017**, *2017*, 6043069. [CrossRef]
12. Deshkar, S.; Thanseeh, R.A.; Menon, V.G. A review on IoT based m-health systems for diabetes. *Int. J. Comput. Sci. Telecommun.* **2017**, *8*, 13–18.

13. Catarinucci, L.; de Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things* **2015**, *2*, 515–526. [CrossRef]
14. Yin, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
15. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017.
16. Nagarajan, S.M.; Deverajan, G.G.; Kumaran, U.; Thirunavukkarasan, M.; Alshehri, M.D.; Alkhalaf, S. Secure data transmission in internet of medical things using RES-256 algorithm. *IEEE Trans. Ind. Inform.* **2021**, *18*, 8876–8884. [CrossRef]
17. Bosri, R.; Uzzal, A.R.; Al Omar, A.; Bhuiyan, M.Z.A.; Rahman, M.S. HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020.
18. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security. Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
19. Ahmed, M.; Byreddy, S.; Nutakki, A.; Sikos, L.F.; Haskell-Dowland, P. ECU-IoHT: A dataset for analyzing cyberattacks in internet of health things. *Ad Hoc Netw.* **2021**, *122*, 102621. [CrossRef]
20. Ahmed, M.; Byreddy, S.; Nutakki, A.; Sikos, L.; Haskell-Dowland, P. ECU-IoHT, 2020. Available online: https://doi.org/10.25958/5f1f97b837aca (accessed on 10 January 2023).
21. Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C.; Rodriguez, J. An anomaly-based intrusion detection system for internet of medical things networks. *Electronics* **2021**, *10*, 2562. [CrossRef]
22. Ahmad, Z.; Shahid Khan, A.; Wai Shiang, C.; Abdullah, J.; Ahmad, J.F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4150. [CrossRef]
23. Kuzlu, M.; Fair, C.; Guler, O. Role of artificial intelligence in the internet of things (IoT) cyber security. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
24. Sarker, I.H.; Abushark, A.I. Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions. *Mob. Netw. Appl.* **2022**, 1–17. [CrossRef]
25. Esteva, A.; Kuprel, B.; Novoa, R.A.; Justin, Ko.; Sweeter, S.M.; Blau, H.M.; Thrun, S. Dermatologist-level classification of skin cancer with deep neural networks. *Nature* **2017**, *542*, 115–118. [CrossRef]
26. Sze, V.; Chen, Y.H.; Yang, T.J.; Emer, J.S. Efficient processing of deep neural networks: A tutorial and survey. *Proc. IEEE* **2017**, *105*, 2295–2329. [CrossRef]
27. 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]
28. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for internet of things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]
29. Anthi, E.; Williams, L.; Burnap, P. Pulse: An adaptive intrusion detection for the internet of things. In Proceedings of the Conference on Living in the Internet of Things: Cyber Security of the IoT, London, UK, 28–29 March 2018.
30. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
31. Radanliev, P.; De Roure, D. Disease X vaccine production and supply chains: Risk assessing healthcare systems operating with artificial intelligence and industry 4.0. *Health Technol.* **2023**, *13*, 11–15. [CrossRef]
32. Radanliev, P.; De Roure, D. Advancing the cyber security of the healthcare system with self-optimising and self-adaptive artificial intelligence (part 2). *Health Technol.* **2022**, *12*, 923–929. [CrossRef]
33. Eliash, C.; Lazar, I.; Nissim, N. SEC-C-U: The Security of Intensive Care Unit Medical Devices and Their Ecosystems. *IEEE Access* **2020**, *8*, 64193–64224. [CrossRef]
34. Syed, M.; Syed, S.; Sexton, K.; Syeda, H.B.; Garza, M.; Zozus, M.; Syed, F.; Begum, S.; Syed, A.U.; Sanford, J.; et al. Application of Machine Learning in Intensive Care Unit (ICU) Settings Using MIMIC Dataset: Systematic Review. *Informatics* **2021**, *8*, 16. [CrossRef] [PubMed]
35. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
36. Fernandes, G.; Rodrigues, J.J.P.C.; Carvalho, L.F.; Al-Muhtadi, J.F.; Proenca, M.L., Jr. A comprehensive survey on network anomaly detection. *Telecommun. Syst.* **2019**, *70*, 447–489. [CrossRef]
37. Hijazi, S.; Obaidat, M.S. A new detection and prevention system for ARP attacks using static entry. *IEEE Syst. J.* **2019**, *13*, 2732–2738. [CrossRef]
38. Vijayakumar, K.P.; Pradeep, M.K.K.; Kottilingam, K.; Karthick, T.; Ganeshkumar, P. An adaptive neuro-fuzzy logic based jamming detection system in WSN. *Soft Comput.* **2019**, *23*, 2655–2667. [CrossRef]
39. Liao, S.; Zu, C.; Zhao, Y.; Zhang, Z.; Zhang, C.; Gao, Y.; Zhong, G. A comprehensive detection approach of Nmap: Principles, rules and experiments. In Proceedings of the 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China, 29–30 October 2020; 30 October 2020.
40. Zhang, Q.; Han, R.; Xin, G.; Liu, C.H.; Wang, G.; Chen, L.Y. Lightweight and accurate DNN-based anomaly detection at edge. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 2927–2942. [CrossRef]

41. Nicolazzo, S.; Nocera, A.; Ursino, D.; Virgili, L. A privacy-preserving approach to prevent feature disclosure in an IoT scenario. *Future Gener. Comput. Syst.* **2020**, *15*, 502–519. [CrossRef]
42. Cauteruccio, F.; Cinelli, L.; Corradini, E.; Terracina, G.; Ursino, D.; Virgili, L.; Savaglio, C.; Liotta, A.; Fortino, G. A framework for anomaly detection and classification in Multiple IoT scenarios. *Future Gener. Comput. Syst.* **2021**, *114*, 322–335. [CrossRef]