Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 02 ISSUE 07, 2024

Anomaly Detection-Based Intrusion Detection System Using Deep Neural Networks in Healthcare Internet of Things

Maytham Mohammed Tuaama
Imam Al-Kadhum College (IKC), Department of Computer Technical Engineering

Abstract:

In recent years, technology has penetrated every domain with every passing second, making things smart. These smart things offer numerous services of convenience to humans and bring in data using various resources [1]. In the State of the Connected Patient report, it is stated that the medical and healthcare Internet of Things (IoT) product review presented that senior care Internet of Things are going to peg up at 119%, as a share of IoT devices. Besides, it is stated that approximately 42% of seniors could start using home monitoring products or wearables within the next three years [2]. Wearables and implants with Internet of Things actuators and sensors help people with their healthcare diagnose a variety of diseases using data from the patient's electrocardiogram (ECG), core temperature, pulse rate, respiratory rate, and oxygen saturation levels as well as information from the patient's workplace computer (such as an iOS or Android smartphone) or implant. [3] . Healthcare relies on the Internet of Things (IoT) for its innovation. With sensors, communication channels, and artificial intelligence (AI), the IoT collects and processes patient data in real-time, generating immediate responses [4], [5]. These systems, up to now, have generally generated much higher levels of trust than they really should [5]. Following old models of security—layering encryption and access controls on top of an interconnected web of smart devices—hasn't particularly worked out, with the effect of preventing any kind of real, widespread adoption. Traditional, signature-based machine learning (ML) algorithms don't adapt well to new attack types, either [6]. New attack types are precisely what the IoT in healthcare is inviting, given its somewhat weak security that also reveals the privacy-compromising data that's transmitted to and from a host of healthcare devices. By integrating self-learning procedures and automated capabilities, the suggested deep learning architecture (DLA) centres on smart healthcare anomaly detection. It intelligently controls systems by preprocessing and integrating data from IOT devices in medical settings.

Keywords: *IDS; Anomaly detection; HIOT; machine learning; DNN; deep learning; IOT.*

1. Introduction

When it comes to healthcare innovation, A crucial part is played by the Internet of Things (IoT). [4]. The Internet of Things (IoT) in healthcare relies on several interconnected parts, including sensors, communication channels, and AI, in order to gather environmental data (the human body) and store it in a format suitable for processing by a variety of AI algorithms. Integrating these technologies allows for the collection of rich data on various vital signs and enhances healthcare delivery by allowing for immediate responses to any fluctuations in a patient's vitals [5]. The Internet of Things (IoT) can potentially revolutionize healthcare, but security concerns prevent its widespread implementation [7]. Applying conventional security measures to IoT-based healthcare systems (H-IoT) is unsuccessful because H-IoT is made up of disparate, networked, and interdependent smart items (sensors) [8].

H-IoT devices need to collaborate to accomplish a common goal, despite their inherent differences in areas such as functionality, computing capability, software/hardware features, and network access [9]. There are security risks associated with such a cooperative character. Many features of various items serve to ensure their safety. A threat actor may be able to compromise the entire system by exploiting the system's least secure parts. A chain reaction of assaults against other components could be initiated from the compromised parts. Any disruption caused by a compromised H-IoT device might harm the overall system and prevent it from performing as expected [6].

Data security, reliable data mining with improved user privacy, and context-aware intelligence services all depend on well-managed trust in the Internet of Things (IoT). In order to get support, we must allay the fears and doubts that consumers have about IoT apps and services. When we have faith in something, it means we have faith in its honesty, trustworthiness, security, and dependability [10].In order for physical objects to offer people with high-quality information services, the Internet of Things (IoT) aims to make their integration into networks as smooth as possible. Machine learning (ML)-based Internet of Things (IoT) services and applications have lately emerged in several industries, including security, health care, and transportation object monitoring, control, and surveillance. inadequate plans for taking action and execute difficulties are inherent to preventative security designs; The services and strong security measures needed to protect IoT devices from assaults may be provided by ML architecture. Attack detection systems can be either signature-based or anomaly-based. Attacks against systems that depend on signatures match pattern in network traffic, including bytes or malicious instructions supplied by malware, to a database of known attack types. Utilising anomaly-based methodologies allows for the detection of unknown attacks or traffic that differs from the norm.the eleventh Using ML to develop a model of trustworthy behaviour and then putting it through its paces against novel assaults is a crucial tactic. This ML model training may take place on the application and hardware configurations, unlike a signature-based approach.[12].

Despite criticism for its inability to detect new attacks, conventional machine learning procedures and approaches have seen extensive use due to their high attack accuracy and low false alarm rate. When it comes to identifying composite and innovative assaults, traditional ML algorithms fall short. Little variants of modern times called cyberattacks make up the bulk of mutation attacks. Earlier logics and conceptions are novel attacks. Due to their inability to abstract traits that differentiate new attacks, conventional ML models are unable to detect minute mutations.[10] Exploring the assaults becomes much easier when enormous datasets from many IoT devices are analyzed, especially with the use of DL techniques. Because of its adaptability in maintaining generic classifications with high accuracy and its sympathetic nonlinear estimation performance, the architecture of DNN presents the primary challenge to learning IoT[13]. The suggested deep learning architecture (DLA) in this paper deals with anomaly detection handling in a smart healthcare settingWith the help of sensitive self-learning algorithms that can automate and indicate, the DLA builds the smart controlling process. Acquiring massive amounts of data begins with preprocessing and the integration of Internet of Things (IoT) devices from smart medical. The following step is to coordinate intelligence frameworks with DLA so that control technique and management service decisions are safe, secure, and reliable. To classify system states as normal or abnormal, deep architectures use training methods to construct a mathematical model. By combining patterns of data with system variables, these models construct a composite analytic connection, which helps to detect both normal and abnormal system behaviour. Here is the order of the remaining components: In Section 2, we go over the literature review's detection models. The methodology and proposed DNN strategy are outlined in Section 3, and the results analysis is presented in Section 4. Section 5, Conclusions and Plans for the Future.

2. **Literature Review**

The success of the IoT depends on the security of data transmissions between devices. Data integrity is crucial because there can be no additions or deletions to the data during the transfer [6]. For example, in the healthcare sector, system integrity checks are required for remote patient monitoring to safeguard patient data. Conventional detection techniques have become futile [14]. Therefore, modern intrusion prevention and detection systems are vital tools for securing sensitive data and keeping it from unauthorized persons; these measures can help control data transmission and keep everything secure [15] . In addition, IoT devices and services are expected to have high accessibility standards, particularly for healthcare monitoring systems [16] . Many academics have published in both areas, using various methodologies and algorithms to find the most effective ways to prevent or detect infiltration with great precision and can keep everything secure. One of the fundamental requirements for the Internet of Things is that all information, tools, and services be readily available with security and privacy at the precise moment of need [17] .

Alghawli (2021). proposed model of Based on anomalies IDSs rely on the usual (or benign) application patterns and consider any variations to be suspicious. [18] . Moreover, [19] explains that an anomaly-based IDS is designed around the patterns of behavior of "good" applications and flags any deviations as suspicious (abnormal). consequently, the anomaly-based technique is perfect for spotting brand-new (zero-day) threats [20] .

Zachos et al (2021). Many studies have used the anomaly-based method to identify threats to H-IoT networks. To identify malicious or normal behaviour, these algorithms compare the observed behaviour (at the moment of detection) to a usual profile that represents the system's legitimate activities [21]. Any deviation from the usual pattern of the suspicious behaviour is taken as an assault. When built, however, they presuppose that the conventional profile definition would remain unchanged [22]. The typical ranges for different vital signs change at any given instant based on the patient's circumstances, hence this assumption is erroneous. Whether or not a person is exercising when their heart rate is measured affects the normal range of that measurement. In light of this, it is important to take these changes in context into account when trying to define "typical conduct." In addition, H-IoT vital sign monitors typically have an evolving profile that adapts to the ever-changing ecosystem. Nodes (sensors) can join or depart at any moment due to the sensor's deactivation or the user's mobility, which can cause a communication breakdown among the sensor's both sending and receiving sides [23]. In this scenario, the IDS's ability to detect are diminished since previously constructed profiles become ineffective due to rapid modifications.

El Sayed et al (2021). put forth Employ machine learning in a model that combines CNN with their own novel regularizer method they call SD-Reg. In their proposal, they proposed a groundbreaking new hybrid design. The SD-Reg method, which makes use of the standard deviation, can address the overfitting problem in classifier models. Models based on the SD-Reg performed better than those based on the L1 and L2 methods currently used [24].

Mohamed et al (2022). Protecting IoT systems from attacks begins with knowing what to look for [25] .In a similar manner, [26], [27] show that several intrusion detection system types, including misuse-based and anomaly-based Intrusion Detection Systems (IDSs), have been suggested as viable solutions to this issue.[28] drew attention to the fact that misuse-based IDSs build their detection models using attack signatures that have already been established. Because of this, the IDS can identify threats that are exact replicas of those that have already been classified as malicious usage. This method's limitation, according to [29] is that it cannot detect zero-day attacks or ones that have never been observed before.

Zhao et al (2022). used a method known as Correlation feature selection, which seeks the optimal collection of characteristics according to their correlation. The next step is to suggest a weighted Stacking method to boost classification performance. This technique entails giving more weight to the basic classifier that did well during training and less weight to the ones that did badly [30] .

Nguyen et al. (2022). To improve the precision of intrusion detection in monitoring and data-gathering systems, a stacking-based classification model was created as an example of an ensemble learning model. XG Boost, Light GBM and Random Forest, served as base classifiers, with MLP being used for additional improvement. Stacking added complexity to the final model, which made it harder to define [31] Otherwise, [32] concentrate on Stacking Meta classifiers. The comparison findings between Meta Decision Trees, Multi-Response Model Trees, and Multi Response Linear Regression indicated that MDT provided the greatest performance. However, picking the meta classifier will not fix the issue brought on by the foundational model. The poor performance of the basic model will still impact the model's final classifications. Moreover,[33] . Put forth a novel ensemble architecture that can accurately identify various types of attacks. The proposed approach to cyberattack detection relies on building an ensemble by evaluating the detection capabilities of several base classifications. In contrast,[34], [35] the voting strategy relies on a majority vote from all classifiers in the ensemble, regardless of how well they detect the attack. Moreover, ensemble approaches might not be optimal for issues like anomaly identification or identifying outliers. The goal is to single out data points that dramatically deviate from the norm rather than make a prediction.

Vishwakarma et al (2022). A deep neural network-based intrusion detection system was presented as a model to detect malicious packets in real-time. In addition, they employed methods for capturing and detecting packets to identify attacks in progress in real-time [36] . Similarly, this research [37] introduces a deep autoencoder. This essentially proposes switching from the encoder-decoder approach to employing just the encoding step. The concept is that using the right comprehension form can cut down on computational and time-consuming overheads without sacrificing accuracy or efficiency.

Ravi V et al (2022). Recurrent models based on deep learning were introduced. This research presents a comprehensive framework for discovering and labeling security threats in a network. The proposed model employs a kernel-based principal component analysis (KPCA) feature selection approach to extract features from the recurrent model layers and determine the best characteristics [38]. However, [39] introduced the disadvantage of ensemble learning is that it could be time-consuming and resource-intensive, especially when employing many base models or complicated models like deep learning architectures. Otherwise, Saba et al [40]Introduce a convolutional neural network (CNN) based technique for anomaly-based intrusion detection systems (IDS) that leverages the capabilities of the Internet of Things (IoT), giving characteristics to investigate full traffic across the IoT effectively. The suggested approach can identify suspicious activity and unauthorized entry. On the other hand, [41], [42] these studies say CNN-based techniques for anomaly IDSs are not Overfit Resistance. Where the model does a good job of fitting the training data but struggles to generalize to new data. As a result, performance may suffer, and projections may be off.

Zahra Amiri et al (2023). This study presents comprehensive data on the principles and uses of machine learning (ML) approaches in the field of health. and covers a wide range of disorders that are widespread. and thoroughly examines future prospects, taking into account all the necessary processes that need to be planned for the future [43] . However, Applying ML to individual healthcare poses several distinct obstacles. The diagnostic labels that are utilized to train supervised learning algorithms are crucial. But these classifications might not be precise enough to generate AI systems with great sensitivity and specificity due to the diverse nature of mental diseases. Using ML algorithms to anticipate particular symptoms or outcomes instead of diagnoses is one potential option. Furthermore, novel biomarkers for recognizing specific diseases can be discovered autonomously using the power of DNN. Even though there is a need for openness and repeatability, keeping trade secrets is a big obstacle to using ML algorithms. In addition to being fundamentally unstructured, big data necessitates substantial preparation before utilization. Additionally, it is not commonly practiced to integrate information regarding the quality and potential biases of the data used to train the system in the outcomes of ML algorithms.

Ayesha S. Dina et al (2023).

Applying deep learning models with the focus on loss functions as a tool to address data imbalance is the goal of this work. Because of its reliable performance with imbalanced datasets, a focal loss function is used to detect IoT intrusions. Using the targeted loss function, gradient updates may be dynamically changed to improve the model's performance. By reducing the weight of easy examples, this function forces the model to focus on difficult misclassified situations. Updating with averaged gradients is possible with the standard cross-entropy loss function, on the other hand. Many popular deep learning neural network designs, such as Feedforward neural network models (FNNs) as well as Convolutional Neural Networks (CNNs), can benefit from using the focal loss function. We use datasets from three distinct IoT areas to assess the effectiveness of adding the focus on loss functions to deep learning models. Based on our research, we used Bot-IoT [1.4.9] for IoT sensors, WUSTL-IIoT-2021 [1.4.10] for IIoT, and WUSTL-EHMS-2020 [1.4.11] for healthcare monitoring [44]. Nevertheless, a substantial quantity of training data is necessary, comprehending the network's judgements is challenging, and there are significant processing requirements.

Our literature study showed that despite the high detection accuracies achieved so far, there remains space for improvement. Such problems include varying degrees of accuracy and considerable dataset alteration. The region is in its early stages of growth. Most of the researchers focused on preventing intrusion in many ways, and others touched on intrusion detection in several ways; we have detailed the chosen IDSs and compared their fundamental qualities in a table (1). but few of them used deep learning in intrusion detection. Therefore, we believe that the proposed methodology and work mentioned in this paper can generate credible results as well as reduce cost and time by maximizing detection accuracy while minimizing false alarms.

TABLE 1

NO	Author &year	Method	Dataset	Simulation	Advantage	disadvantage

[6]	Daojing He et al. 2019	Stacked Autoencoder, model of stacked-restricted Boltzmann machine (RBM)	KDD’99 dataset.	virtual environment	precision, the one negative aspect is the production process. The memory needs of these cluster trees are higher.	(Less efficient) The higher efficiency, the greater workload on the intrusion detection system, and thus the cost and time increase. Another disadvantage is that producing. The memory needs of these cluster trees are higher.
[14]	Foley et al 2020	ML	novel dataset	virtual IoT environment	high accuracy	Using power metrics, we were only able to identify two simultaneous attacks.
[17]	Eskandari et al 2020	Passban IDS	only Botnet, only Telnet,	Raspberry Pi 3 Model B	Low false positive rates, inexpensive, and maybe run on inexpensive IoT gateway boards such as a Raspberry Pi 3 version B, particularly when the data throughput on the network's interface is not anticipated to surpass 40-50 Mbits/s.	that it works offline with copies of network traffic and does not block malicious traffic
[28]	Zachos et al 2021	machine learning (ML) techniques A set of six popular ML algorithms.	TON_IoT Telemetry dataset	Raspberry Pi 4 Model B device	Easy to operate. Whether the parameters are linearly or non-linearly separated has no effect on performance.	Subject to the risk of overfitting. Instable (i.e., building DTs from seemingly unrelated data sets might provide wildly diverse results).
[29]	Hasan et al 2019	Machine Learning Neural Networks (ANNs), Decision Trees (DTs), Random Forests (RFs), SVM, and Logistic Regression (LR)	The open-source dataset was collected from Kaggle.	virtual IoT environment	is one of the most reliable machine learning methods, capable of very high rates of	if the model is too complicated or the data set is too small, overfitting is still possible

					detection.	with the random forest
[18]	. Alghawli 2022	Anomalies can be detected in real time using complex approaches that rely on time series analysis.	Testing cyclo-stationarity-based networks detection systems with a new dataset	virtual environment	identify some of malicious packets in real time	Vulnerable to overfitting.
[19]	ElSayed et al 2021	DL, (CNN), SDN	CSE-CIC-IDS2018, UNSW-NB15	virtual environment	an enhanced capacity to detect novel threats, faster detection of network attacks, and a general increase in accuracy.	high processing demands, the complexity of understanding the network's judgments, and the necessity for vast volumes of training data.
[20]	ZHAO et al,2022	(ML)a CFS-DE feature selection algorithm and a weighted Stacking classification algorithm	e NSL-KDD and CSE-CIC-IDS2018 data sets	virtual environment	enhancing IDS performance by identifying and prioritizing the features most important for spotting cyberattacks.	This algorithm is not guaranteed to find the best feature subset, and the outcomes will change from dataset to dataset.
[21]	DD Nguyen et al 2022	ML with SCAD(supervisory control and data acquisition)	international dataset (gas pipeline dataset).	virtual environment	can boost a model's ability to predict by combining their strengths	can be time-consuming on a computer because it requires training multiple models and a meta-model, and overfitting is possible if the underlying models are inaccurate.
[32]	O. O. Olasehinde et al 2020	ML (Meta Learner algorithms)	UNSW-NB15 Dataset	virtual environment	improved model performance by increasing prediction accuracy, optimizing learning algorithms to produce optimal results, and enabling models to learn from and adapt to a wide variety of	They need a lot of information to train well. The complexity of meta-learning algorithms can make them challenging to design and maintain, and the performance advantages they provide may not be

					datasets and settings.	substantial for all applications.
[45]	Lin H et al 2021	ML with ensemble learning	CIC IDS 2018 dataset	virtual environment	Ensemble learning has been shown to improve generalization performance and decrease prediction errors.	Ensemble approaches may be not well suited for issues like anomaly detection and outlier detection, where the goal is to single out data points that significantly deviate from the norm rather than make a prediction.
[31]	Nguyen et al 2022	ML with SCAD(supervisory control and data acquisition)	Gas pipeline dataset	virtual environment	Robustness to overfitting	primary disadvantage is that it increases the final model's complexity, making it more difficult to explain.
[36]	Vishwakarma et al 2022	deep neural network-based intrusion detection system, packet capturing, and detecting algorithm for real-time attack detection.	five NetFlow-based NIDS datasets, this database includes NF-UNSWNB15, NF-BoTIoT, NF-ToNIoT, and NF-CSE CICIDS2018.	using raspberry pi (intelligent room light system and fire alarm system)	identify malicious packets in real time.	don't detect the zero-day attack.
[39]	Ravi et al 2022	DL, (RNN), LSTM, CNN,	KDD-Cup-1999, UNSW-NB15, WSN-DS, and CICIDS-2017.	virtual environment	high accuracy	Vulnerable to overfitting.
[40]	Saba et al 2022	(Dl) CNN-based approach for anomaly-based intrusion detection systems (IDS)	the NID Dataset and BoT-IoT datasets	virtual environment	high accuracy	not Resistant to overfitting. consumption more time
[43]	Zahra Amiri et al 2023	ML(CNN,RNN,DNN,MLP)	Micromed	virtual environment	High accuracy High stability	Poor comparison between discussed methods
[44]	Ayesha S. Dina et al	FNNs, CNNs	Bot-IoT, WUSTL-	virtual environment	Enhanced model	The main drawback is

	2023		IIoT-2021, WUSTL-EHMS-2020		performance by improving prediction accuracy, fine-tuning learning algorithms to yield optimal outcomes, and facilitating models to acquire knowledge from and adjust to diverse datasets and contexts.	that it amplifies the intricacy of the final model, rendering it more challenging to elucidate.

3. METHODOLOGY

Several separate procedures have been brought together to form the suggested model framework. The general structure of the security environment for detecting anomalies in Healthcare IOT networks based on deep neural networks is shown in Figure 1. Gathering data sets is the first step in this framework. These data sets include DS2OS traces that were acquired in the Healthcare IoT environment. The necessary data set undergoes data preparation and data visualization procedures as part of the data preprocessing phase. By implementing these procedures, the data is transformed into valuable vectors of attributes. The next step is to divide these attribute vectors into two parts, one for testing and one for training.

3.1. A proposed model for anomaly detection based on DNNs.

Due to its ability to acquire the best answers through general development and mitigate a variety of complicated interactions, ML models have been gaining popularity in recent years. An extensive tool in machine learning, artificial neural networks (ANNs) are data-handling models inspired by natural nervous systems, such as the organization of the human brain. By analyzing and classifying data during training, ANNs can uncover complex functions and nonlinear relationships between independent and dependent variables. In a DNN, as seen in Figure 2, each node has three layers: the input layer, the hidden layer or layers, and the output layer. After receiving input data, the nodes in the input layer transmit it to the nodes in the hidden layer through weighted connections; the nodes in the hidden layer then use an activation function to calculate the link weights, which are then transmitted to the nodes in the output layer. In order to determine which nodes should be activated, the activation function computes the weighted total and adds a bias. Deep learning is a branch of machine learning that relies on networks that can learn from input that is neither organised nor labelled. Because of their inherent complexity, neural networks have limited processing power. Recent advances in big data analytics have included improved neural networks, which have made it possible for computers to analyze, research, and react to complicated situations at a faster rate than people. If we build better neural networks and feed them massive amounts of data, their efficiency will only grow; in other words, the more data we feed larger neural networks, the better they will get. This differs from previous ML approaches in that traditional algorithms' performance drops as compared to deep learning as the amount of input data increases.

Thus, for game-changing tech, deep learning delivers accurate outcomes. A growing number of companies are relying on deep learning to devise fresh strategies. The majority of deep learning algorithms use topologies similar to multiple-layer neural networks.

FIGURE. 1. The model's general structure

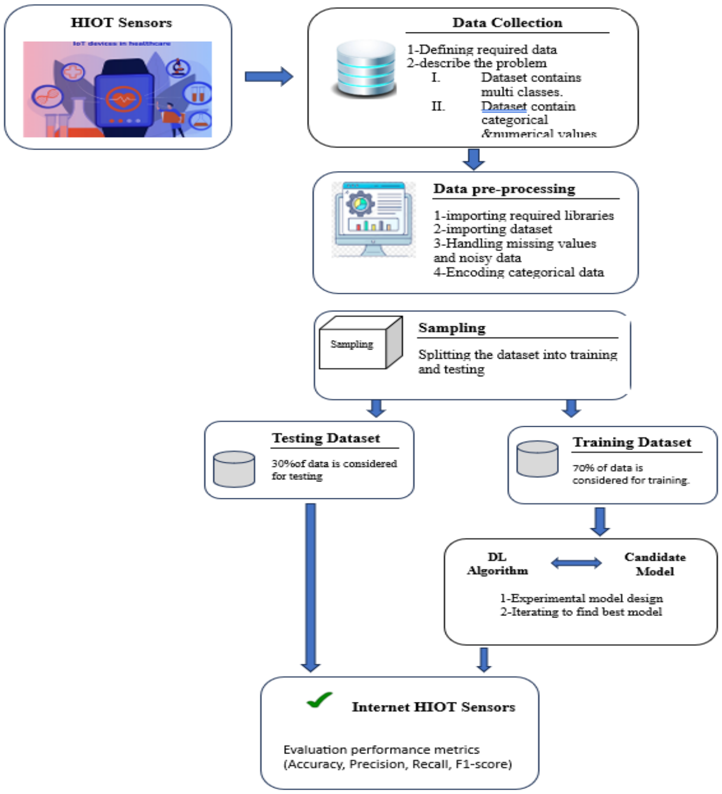
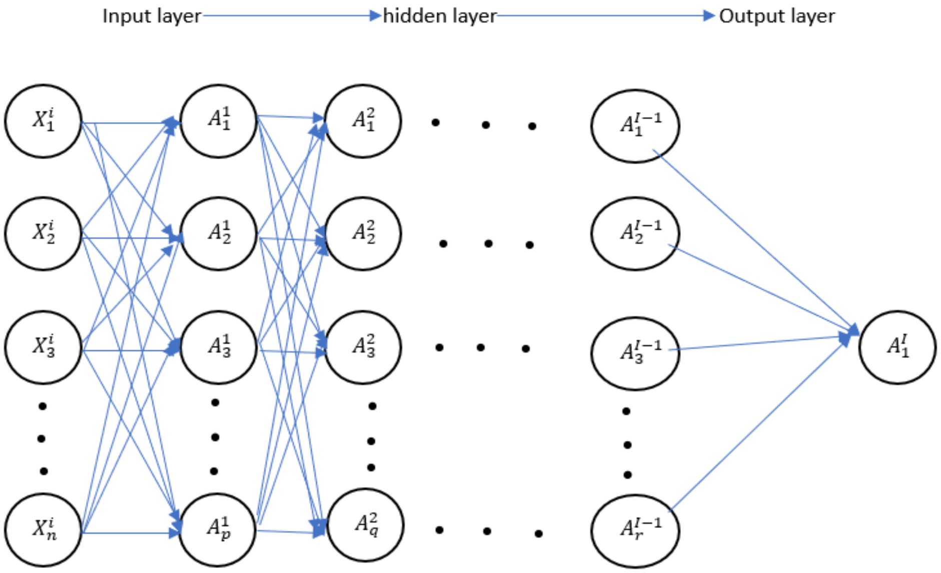

HIOT Sensors
IoT devices in healthcare
Data Collection
1-Defining required data
2-describe the problem
I. Dataset contains multi classes.
II. Dataset contain categorical &numerical values
Data pre-processing
1-importing required libraries
2-importing dataset
3-Handling missing values and noisy data
4-Encoding categorical data
Sampling
Sampling
Splitting the dataset into training and testing
Testing Dataset
30%of data is considered for testing
Training Dataset
70% of data is considered for training.
DL Algorithm
Candidate Model
1-Experimental model design
2-Iterating to find best model
Internet HIOT Sensors
Evaluation performance metrics (Accuracy, Precision, Recall, F1-score)

FIGURE 2. Architecture of DNN



Algorithm for Training of DNN

At layer l = 1, the net input to the neurone Z1 is computed using Equation (1), which takes into account weight W1, input X1, and bias b1.

1- $\boldsymbol{Z^1 = W^1 \times X + b^1}$

By applying the Relu activation function to Z1, a net outcome A1 has been calculated (Equation (2)).

2- $\boldsymbol{A^{1} = Relu(Z^{1})}$

The forward spreading strategy in DNN (Figure 3) follows the procedures outlined in Equations (3) and (4) to move the calculation of the net result A1 from layer 1 to layer l.

3- $\boldsymbol{A^{l-1} = Relu(z^{l-1})}$

4- $\boldsymbol{Z^{l} = W^{l} \times A^{l-1} + b^{l}}$

Predicting Output:

5- $\boldsymbol{O^{l} = A^{l} = \sigma(\ Z^{l})}$

Computing Losses and Gradients: DNN's learning procedure relies on the network's loss ℓ, which is derived from the output ol = Al = σ(Zl) (Equation (6)). Equation (7) is used to generate the gradient of the function of loss ℓ concerning the parameters, which are then used to alter the DNN's parameters . Where T is the transpose matrix, the computation of the gradient of ℓ with respect to the parameters Wl, bl, and Al−1 is given in Equations (8), (9), and (10), respectively.

6- $\boldsymbol{\ell = -\frac{1}{m}\sum_{i=1}^{m}(y^{i}\, log(o^{i}) + (1 - y^{i})log(1 - o^{i}\,))}$

7- $\Delta \boldsymbol{Z^{l}} = \boldsymbol{\frac{\partial \ell}{\partial Z^{1}}}$

8- $\Delta \boldsymbol{W^{1}} = \boldsymbol{\frac{\partial \ell}{\partial W^{1}}} = \boldsymbol{\frac{1}{m}\partial Z^{1}\ A^{l-1T}}$

9- $\Delta \boldsymbol{b^{l}} = \boldsymbol{\frac{\partial \ell}{\partial b^{1}}} = \boldsymbol{\frac{1}{m}\sum_{i=1}^{m} \partial Z^{l,i}}$

10- $\Delta \boldsymbol{A^{1}} = \boldsymbol{\frac{\partial \ell}{\partial A^{l-1}}} = \boldsymbol{W^{lT}\partial Z^{l,i}}$

Updates to Parameters:

Equations (11), (12), and (13), respectively, present the obtained gradients ΔWl, Δbl, and ΔAl−1, which are used to update the parameters Wl, bl, and Al−1.

11- $\boldsymbol{W^{l} = W^{l} - \eta} \times \Delta \boldsymbol{W^{l}}$

12- $\boldsymbol{b^{l} = b^{l} - \eta} \times \Delta \boldsymbol{b^{l}}$

13- $\boldsymbol{A^{i-1}\ = A^{i-1} - \eta} \times \Delta \boldsymbol{A^{l-1}}$

Finally, return $\boldsymbol{II_{i=1}^{N}\, O_{i}\ where\ X = X_{i}\ for\ i = 1\ to\ N}$

This notation uses the product symbol $\boldsymbol{II}$ to indicate the multiplication of O_i for i ranging from 1 to N,given that $X = X_i$.

Using input parameters that are weighted for the next layer of neural networks, a non linear activation function (Relu) calculates the output of each preceding layer and bias. When optimizing loss functions, models using deep learning take the cost function into account. When it comes to multi-label classification, the traditional loss function is the categorical cross-entropy. To determine the neural network's approximate yes/no output, activation functions are employed. Within the range of the activation function, it plots the following characteristics that are function dependent. Also, the sigmoid activation function is used to achieve the model's final forecast. The usage of node dropout helps prevent overfitting. As a training technique, dropout allows for the eventual disregard of randomly selected neurons. A person is "dropped-out" at random. In forward propagation, the activation function of downstream neurons is temporally insensitive, and in backward propagation, the neuron does not get the weights update. The result is a network that can learn more quickly, have less overfitting, and use deep learning to generate better predictions. In general, When simulating several networks with different topologies, it's important to keep in mind that nodes in a network are more robust to inputs and that node dropouts impact the results.

4. Result analysis:

In both the training and testing scenarios, the different techniques in machine learning and deep learning With various number of neurones and hidden layers, we get 98% accuracy or higher, as demonstrated in Table 2.

TABLE 2. Different Techniques in ML&DL Accuracy

	Accuracy	
References	**Training**	**Testing**
(24-10-13)	98.27	98.29
(18-22)	98.26	98.28
(22-27-36)	98.17	98.21
(8-9-33)	98.15	98.18

According to Table 3, DNN models are more effective than the traditional ML method in identifying intrusive activities.

This article examines various approaches for attack detection that have been suggested for the Internet of Things (IoT). Utilising a synthetic dataset. V. Ravi [38] showcased that by utilising the SDN-IoT dataset, the proposed deep learning approach was able to accurately detect network risks with a highest accuracy rating of 99% & an F1-score of 97%. This model obtained similar outcomes when applied to various network intrusion datasets like KDD-Cup-1999, UNSW-NB15, WSN-DS, and CICIDS-2017. The model's findings, as shown in Table 4, indicate an accuracy of 99.28% while an F1-score of 98%. Given the artificial character of the data, the F1-score will prioritise both false-negative or false-positive instances over other factors.

TABLE 3

Traditional Classifiers	**Accuracy (%)**
Decision Tree Classifier	98.89
Naïve Bayes	96.13
logistic Regression	97.85
SVM	97.85
Random Forest Classifier	98.01
Proposed model	99.28

The DNN achieves accuracies of 99.28% by utilising a variety of topologies with varied numbers of hidden layers and neurons. We may see the assessment indicators in Table 5. The accuracy value has remained consistent at 0.97 throughout, as is readily apparent. Training and testing F1-scores and recalls have been in the 0.97 to 0.98 range

TABLE 4

Auther	**Dataset**	**Model accuracy(%)**	**F1-score (%)**
32	SDN-IoT	99	97

proposed model	SDN-IoT	99.28	98

TABLE 5

Evaluation metrics	References	The accuracy	The precision	Recall	F1score
Training	(24-10-13)	0.9815	0. 97	0. 98	0. 98
	(18-22)	0.9821	0. 97	0. 98	0. 97
	(9-8-33)	0.9815	0. 97	0. 98	0. 97
Testing	(24-10-13)	0.98	0. 97	0. 98	0. 98
	(18-22)	0.9812	0. 97	0. 98	0. 97
	(9-8-33)	0.9821	0. 97	0. 98	0. 97

This model incorrectly identifies four hostile control attacks as scan assaults while 253 are considered normal. Only 155 malicious actions have been positively identified; the remaining ones were mistakenly identified as benign. Only 325 of the scan readings were accurate; the rest were false positives, including 20 for hostile operations, 3 for espionage, and 117 for normal. Only 33 cases of suspected eavesdropping were really identified as such, while 126 cases were mistakenly labelled as benign. It is confirmed that all 41 incorrect setups are incorrect setups. Out of a total of 104, 395 normally occurring values, 8 were mistakenly identified as malicious actions, 2 as scan errors, and 1 as incorrect configuration.

Similarly, hostile control assaults, data probing, and denial-of-service attacks are all mistakenly identified as normative. Only 87 harmful actions are identified as such, while the remaining ones are mistakenly labelled as benign. Only 335 of the scan values were really identified as scans, while the other 120 were incorrectly labelled as normal. While the rest were mistakenly identified as normal, eighteen were found to be really espionage. Each of the forty-one incorrect configurations has been pinpointed. The remaining normal values are mistakenly identified as harmful actions, whereas 104, 395 regular values are discovered as normal.

Healthcare IoT applications, public transit, and industrialised applications may all benefit from the increased resilience, decreased resource requirements, and boosted efficiency brought about by deep learning improvements in the Internet of Things (IoT).

Conclusion

With the help of deep learning architectures, we can greatly enhance the expansion of IoT devices and services. The management of data in our a data-driven Internet-connected society is getting more challenging as it traverses different devices, particularly in the healthcare system. Hence, ensuring the protection of the H-IoT infrastructures is vital for providing a secure and safe medical environment. Hacked H-IoT services may cause chaos and perhaps harmful situations. In this post, we demonstrated a way to identify network attacks on the H-IoT network. By using the collected measurements, the system employs a deep learning procedure that incorporates dense random neural networks to forecast the probability of a network assault. Among other proposed models and six wide machine-learning classifiers, the deep learning method produced the highest accuracy (98.26 percent) when evaluated on the DS2OS traffic traces dataset. Many DNN models with various layers and neurones in each layer are the topic of this article due to the fact that their brief accuracy is guaranteed when compared to standard ML approaches. Reliability relies on picking the right model. With the help of the DNN supervisory model, the system is able to better classify assaults and abnormalities. Data probing, denial-of-service attacks, fraudulent control, fraudulent operation, scan, eavesdropping, improper configuration, and typical are all examples of these sorts. The first model achieved the best results compared to the others, with an accuracy in training of 97.27% & an accuracy in testing of 9,19%. A total accuracy of 98.18% was the result of this. The outcomes demonstrate the practicality of the suggested approach in identifying numerous H-IoT abnormalities, especially in cases where the model exhibits subtle variations. To some extent, a model (13-18-22-24-33) may also detect suspicious behaviour, improper configuration, and possible hostile actions, scanning, and eavesdropping. An analysis of the outcomes shows that the proposed approach successfully detects a wide range of Internet of Things (IoT) dangers and anomalies. Conversely, baseline DNN methods are being evaluated using the dataset. There are no new algorithms created using this dataset. To safeguard networks against susceptible IoT networks, more research into anomaly or detection of attacks based on ML is necessary, as shown by this study's results. Building a permanent detection technique and concentrating on the overall architecture of the system both require further research. Researchers are primarily focussing on sophisticated ML algorithms due to their better learning and computation capabilities. This is especially true when it comes to spotting category risks in IoT networks. Devices driven by computers and equipped with artificially intelligent vision are becoming more and more important for a secure and effective healthcare setting. In order to enhance the effectiveness and integrity of the the healthcare internet of things, it is crucial to integrate IoT technological services. The data-gathering capabilities of the deep learning architecture are crucial to the powered systems' autonomously monitoring. Through integrating the IoT with healthcare settings.

Bibliography

1. A. E. Omolara *et al.*, “The internet of things security: A survey encompassing unexplored areas and new insights,” *Comput Secur*, vol. 112, p. 102494, 2022.
2. S. P. Chatrati *et al.*, “Smart home health monitoring system for predicting type 2 diabetes and hypertension,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 3, pp. 862–870, 2022.
3. S. Y. Y. Tun, S. Madanian, and F. Mirza, “Internet of things (IoT) applications for elderly care: a reflective review,” *Aging Clin Exp Res*, vol. 33, pp. 855–867, 2021.
4. Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V Vasilakos, and S. W. Kim, “The future of healthcare internet of things: a survey of emerging technologies,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.
5. R. Indrakumari, T. Poongodi, P. Suresh, and B. Balamurugan, “The growing role of Internet of Things in healthcare wearables,” in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*, Elsevier, 2020, pp. 163–194.
6. R. K. Mahendran and P. Velusamy, “A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things,” *Comput Commun*, vol. 153, pp. 545–552, 2020.
7. M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Future generation computer systems*, vol. 82, pp. 395–411, 2018.
8. J. Granjal, E. Monteiro, and J. S. Silva, “Security for the Internet of Things: A Survey of Existing Pro-tocols and Open Research Issues. IEEE Communica tions Surveys & Tutorials, 17 (3), 1294-1312,” 2015.
9. J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, “An intrusion detection framework for energy constrained IoT devices,” *Mech Syst Signal Process*, vol. 136, p. 106436, 2020.
10. D. K. Reddy, H. S. Behera, J. Nayak, P. Vijayakumar, B. Naik, and P. K. Singh, “Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, p. e4121, 2021.

11. R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, “Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML,” *Journal of Network and Computer Applications*, vol. 201, p. 103332, 2022.
12. A. Hennebelle, H. Materwala, and L. Ismail, “HealthEdge: a machine learning-based smart healthcare framework for prediction of type 2 diabetes in an integrated IoT, edge, and cloud computing system,” *Procedia Comput Sci*, vol. 220, pp. 331–338, 2023.
13. A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions,” *Security and Communication Networks*, vol. 2022, no. 1, p. 4016073, 2022.
14. A. Chacko and T. Hayajneh, “Security and privacy issues with IoT in healthcare,” *EAI Endorsed Trans Pervasive Health Technol*, vol. 4, no. 14, 2018.
15. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.
16. M. Sarrab and F. Alshohoumi, “Assisted Fog Computing Approach for Data Privacy Preservation in IoT-Based Healthcare,” *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*, pp. 191–201, 2022.
17. J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, “A review of performance, energy and privacy of intrusion detection systems for IoT,” *Electronics (Basel)*, vol. 9, no. 4, p. 629, 2020.
18. A. S. Alghawli, “Complex methods detect anomalies in real time based on time series analysis,” *Alexandria Engineering Journal*, vol. 61, no. 1, pp. 549–561, 2022.
19. A. A. Cook, G. Msrl, and Z. Fan, “Anomaly detection for IoT time-series data: A survey,” *IEEE Internet Things J*, vol. 7, no. 7, pp. 6481–6494, 2019.
20. S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, “Intrusion detection systems in the Internet of things: A comprehensive investigation,” *Computer Networks*, vol. 160, pp. 165–191, 2019.
21. G. Zachos, I. Essop, G. Mantas, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, “An anomaly-based intrusion detection system for internet of medical things networks,” *Electronics (Basel)*, vol. 10, no. 21, p. 2562, 2021.
22. M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things*, vol. 7, p. 100059, 2019.
23. Q. Liu, V. Hagenmeyer, and H. B. Keller, “A review of rule learning-based intrusion detection systems and their prospects in smart grids,” *IEEE Access*, vol. 9, pp. 57542–57564, 2021.
24. M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, “A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique,” *Journal of Network and Computer Applications*, vol. 191, p. 103160, 2021.
25. T. S. Mohamed and S. Aydin, “IoT-based intrusion detection systems: a review,” *Smart Science*, vol. 10, no. 4, pp. 265–282, 2022.
26. D. He *et al.*, “Intrusion detection based on stacked autoencoder for connected healthcare systems,” *IEEE Netw*, vol. 33, no. 6, pp. 64–69, 2019.
27. J. Foley, N. Moradpoor, and H. Ochenyi, “Employing a machine learning approach to detect combined internet of things attacks against two objective functions using a novel dataset,” *Security and Communication Networks*, vol. 2020, 2020.

28. A. A. Anitha and L. Arockiam, “A review on intrusion detection systems to secure IoT networks,” *International Journal of Computer Networks and Applications*, vol. 9, no. 1, pp. 38–50, 2022.

29. M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices,” *IEEE Internet Things J*, vol. 7, no. 8, pp. 6882–6897, 2020.

30. R. Zhao, Y. Mu, L. Zou, and X. Wen, “A hybrid intrusion detection system based on feature selection and weighted stacking classifier,” *IEEE Access*, vol. 10, pp. 71414–71426, 2022.

31. D. D. Nguyen, M. T. Le, and T. L. Cung, “Improving intrusion detection in SCADA systems using stacking ensemble of tree-based models,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 119–127, Feb. 2022, doi: 10.11591/eei.v11i1.3334.

32. O. O. Olasehinde, O. V. Johnson, and O. C. Olayemi, “Evaluation of Selected Meta Learning Algorithms for the Prediction Improvement of Network Intrusion Detection System,” in *2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020*, Institute of Electrical and Electronics Engineers Inc., Mar. 2020. doi: 10.1109/ICMCECS47690.2020.240893.

33. S. Seth, K. K. Chahal, and G. Singh, “A Novel Ensemble Framework for an Intelligent Intrusion Detection System,” *IEEE Access*, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

34. V. Kotu and B. Deshpande, “Chapter 2 - Data Mining Process,” in *Predictive Analytics and Data Mining*, V. Kotu and B. Deshpande, Eds., Boston: Morgan Kaufmann, 2015, pp. 17–36. doi: https://doi.org/10.1016/B978-0-12-801460-8.00002-1.

35. V. Kotu and B. Deshpande, “Chapter 2 - Data Science Process,” in *Data Science (Second Edition)*, Second Edition., V. Kotu and B. Deshpande, Eds., Morgan Kaufmann, 2019, pp. 19–37. doi: https://doi.org/10.1016/B978-0-12-814761-0.00002-2.

36. M. Vishwakarma and N. Kesswani, “DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT,” *Decision Analytics Journal*, vol. 5, p. 100142, 2022.

37. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” *IEEE Trans Emerg Top Comput Intell*, vol. 2, no. 1, pp. 41–50, 2018.

38. M. A. Ganaie, M. Hu, A. K. Malik, M. Tanveer, and P. N. Suganthan, “Ensemble deep learning: A review,” *Eng Appl Artif Intell*, vol. 115, p. 105151, 2022, doi: https://doi.org/10.1016/j.engappai.2022.105151.

39. V. Ravi, R. Chaganti, and M. Alazab, “Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system,” *Computers and Electrical Engineering*, vol. 102, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108156.

40. T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, “Anomaly-based intrusion detection system for IoT networks through deep learning model,” *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.

41. L. Alzubaidi *et al.*, “Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions,” *J Big Data*, vol. 8, pp. 1–74, 2021.

42. J. Wu, “Introduction to convolutional neural networks,” *National Key Lab for Novel Software Technology. Nanjing University. China*, vol. 5, no. 23, p. 495, 2017.

43. Z. Amiri *et al.*, “The personal health applications of machine learning techniques in the internet of behaviors,” *Sustainability*, vol. 15, no. 16, p. 12406, 2023.

44. A. S. Dina, A. B. Siddique, and D. Manivannan, “A deep learning approach for intrusion detection in Internet of Things using focal loss function,” *Internet of Things*, vol. 22, p. 100699, 2023, doi: https://doi.org/10.1016/j.iot.2023.100699.

45. H.-C. Lin, P. Wang, K.-M. Chao, W.-H. Lin, and Z.-Y. Yang, “Ensemble Learning for Threat Classification in Network Intrusion Detection on a Security Monitoring System for Renewable Energy,” *Applied Sciences*, vol. 11, no. 23, 2021, doi: 10.3390/app112311283.