International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient DDOS Detection in Internet of Medical Things using CNN-ACL Approach

Jeethu Mathew*[1], Dr. R. Jemima Priyadarsini [2]

Submitted: 07/05/2023 **Revised**: 13/07/2023 **Accepted**: 09/08/2023

Abstract: Internet of Things (IoT) has made great progress in the field of health care system and has the possibility of revolutionizing technical, sociological, and commercial hopes for a healthier future. The term "IoMT" (Internet of Medical Things) refers to the use of networking technology to connect medical devices and software programs related to health-care data to the Internet. These advancements allow the healthcare industry to continue providing patients with a higher level of attention and care. Despite the many advantages they provide, these gadgets also provide new attack surfaces, raising various security and privacy issues. Attacks against medical instruments that is connected to the Internet have the potential to affect people severely and in a life-threatening way. To guarantee accuracy and patient data confidentiality, this thesis focuses on offering a highly secure method of transmitting medical data via IoMT. This paper proposes the average convolution layer (CNN-ACL), a unique CNN architecture type for learning the content features of anomalous activity and then identifying the individual anomaly. A powerful system for detecting network DDOS that incorporates a cutting-edge convolutional layer capable of teaching low-level anomalous qualities is designed with the aid of the CNN-ACL, which is highly recommended. Experimental results demonstrate that this method's network DDOS detection effectiveness is superior to machine learning methods based on the KDDCUP99 and CICIDS2017 datasets. Python is used to stimulate the study, and the average accuracy may be increased to 91%, with 0.87 precision and 0.86 recall.

Keywords: *Healthcare, IoMT, DDOS detection, network security, machine learning, CNN-ACL.*

1. Introduction

Rosen et al., (2006) proposed a network of real-world devices that have sensors built in make up the Internet of Things (IoT), a new paradigm that aims to perfectly combine the digital and physical worlds. It uses a unique protocol to connect everything to the Internet, allowing for data sharing and smart recognition, tracing, positioning, surveillance, and management. Patel et al, (2016) proposed that IoT aims to enable connections between things at anytime, anywhere, with anyone, and with anything, ideally across available network and using available assistance. The Internet of Things (IoT) revolution is reshaping modern healthcare and altering the delivery and reliability of healthcare in great portion due to growth in wireless technology, sensor systems, portable devices, and cloud - based services. A recent innovation that is a part of the IoT is the Internet of Medical Things (IoMT).

Remote monitoring of patients has improved because to the IoMT. By establishing a connection between patients with respective clinicians and facilitating the exchange of health information across a secure network, it lessens the need for unneeded hospitalizations and the strain on healthcare systems. IoMT, which enables patients to communicate health relevant information to clinicians, has the potential to provide more accurate diagnoses, reduced mistakes, and cheaper healthcare expenses. Because the COVID-19 worldwide pandemic is limiting in-person medical visits, which stops the spread, this is currently essential necessary. It is a setting where many medical devices are geared at monitoring people's health, including smart glucose monitoring, smart blood pressure monitors, smart pacemakers, and smart pulse oximeters. These devices are interlinked and share information with one another to transmit private clinical records that is used by hospitals, doctors, and other healthcare professionals to deliver top-notch treatment and assistance (Wang et al., 2020). The gateway stores this private information on a few data centers before sending it to the relevant end users (Priya et al., 2020). Figure 1 shows the IoMT architecture, which links numerous medical smart gadgets and communicates with physicians to deliver efficient care and assistance.

[1]Research Scholar, Department of Computer Science, Bishop Heber College, Trichy. Affiliated to Bharathidasan University Trichy.
ORCID ID : 0009-0000-8821-2152
[2] Associate Professor, Department of Computer Science, Bishop Heber College Trichy. Affiliated to Bharathidasan University Trichy.
ORCID ID : 0000-0002-5219-1502
** Corresponding Author Email: jithumap@gmail.com*

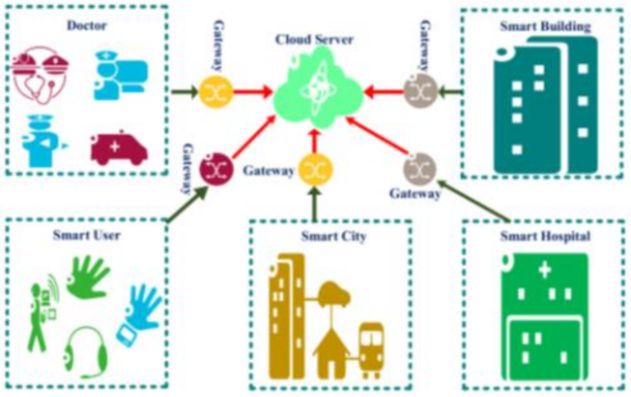

Fig. 1. Architecture of IoMT

In addition to improving the healthcare industry, the IoMT also makes it possible to provide treatment and healing in a more humane way. Although there are many benefits to internet-connected medicinal appliances, there are also remarkable privacy and security concerns, especially considering how frequently healthcare regulators engage with highly sensitive and life-threatening clinical information (Sun et al., 2018). The primary causes of IoMTs being vulnerable to numerous harmful attacks are: (i) Sensitive patient data is mainly exchanged in health care settings. (ii) Compatibility issues and complexity brought by connecting a large number of devices to diverse networks. (iii) Because it is a new industry, healthcare manufacturers are adopting IoMT solutions at a rapid rate without taking security concerns into account. New security challenges including confidentiality, integrity, and availability occur as a result. (iv) As the preponderance of Internet of Things (IoT) elements transmits and get data wirelessly, IoMT is at susceptible to security breaches in wireless sensor networks (WSN). (v) Application risks, including failures in permission and verification, as well as the application's basic safety and accessibility, are also very important. (vi) a few security calculations require a significant amount of processing power.

According to statistics, the healthcare sector has been the target of the most cyberattacks in recent years. Attacks on online-connected medical equipment have the ability to seriously harm patients' physical health and put their lives in peril. For instance, hacking on insulin pumps used in medicine can result in overdosing on the drug, which could result in patient death. The lives of patients may be at peril if connected cardiac devices, like pacemakers, are hacked. The safety, privacy, and accessibility of vital systems can be endangered by a variety of assaults against medical equipment, including message manipulation, false information injection, and attacks of denial of service (DoS) (Yaqoob et al., 2019). Numerous IoT security breaches also impact IoMTs, but some are targeted at IoMTs explicitly since health data is so sensitive. The ability of facilities to deliver patient care may be interfered with by distributed DoS assaults or malware that endangers the security of systems and the confidentiality of patients. Hospitals are not able to manage IoMT devices, obtain electronic health data, and conduct study and other tasks when DoS attacks take networks offline. The healthcare system must have a way to track and carefully examine all incoming and outgoing network traffic in order to quickly identify malicious activity.

It is crucial to figure out how to turn the massive amount of data that the healthcare sector constantly manages from many sources into information that clinicians can use. A rapidly expanding trend right now is machine learning (ML) in security. In cyber security, machine learning is used to enhance threat analysis and attack and security incident response. Building the proper models that can do the proper task by utilizing the proper features is the goal of ML. Deep learning (DL) is a branch of ML that models complex relationships between data by using numerous layers to represent the input data. In deep learning, a layer is made up of neurons that can connect to neurons on different layers along with neurons on the same layer. Different network types have different methods for creating these connections. In a deep learning network, each layer computes and modifies the data before passing it to the layer below (Deng et al., 2013).

This scheme focuses on developing an DDOS detection system (IDS) that can withstand the most recent cyber threats without relying on conventional rule-based techniques. The IDS must defend digital medical records against all attacks. Convolutional neural networks (CNNs), the primary study topic in deep-learning pattern identification, have produced outstanding findings in the categories of computer vision systems, voice recognition and processing natural-language. It is segregated into three primary categories: input, hidden, and output layers with the hidden layer being made up of a number of convolutional, activation, pooling, and fully connected layers. CNN differs from DNN and RNN due to its structure. In comparison to other neural networks, CNN has a smaller number of weights, making it better suited for detection of network DDOSs. Compared to conventional feature selection algorithms, it can automatically learn superior features. As a result, DDOS detection in this study uses an improved new type of CNN. The paper's primary contributions are listed below:

- To solve issues with the identification of unidentified DDOSs in healthcare IoT, a promising DDOS classification framework utilizing deep learning methodology is proposed.
- To provide accurate and realistic DDOS analyses, two types of healthcare-related datasets that incorporate network traffic and biometrics data are collected and examined.

- In order to assess whether a security attack has occurred, the system monitors network traffic and patient biometrics. To identify those attacks utilizing distinct set of features, the system assesses the effectiveness of several machine learning techniques.

The remaining portions of this work are structured as follows: The efforts on DDOS detection and machine learning that are relevant are covered in Section 2. The proposed enhanced new CNN model is described in Section 3 along with its network architectural model. The experimental results of the suggested algorithm on two different types of datasets will be shown in Section 4; the study's conclusions will be presented in Section 5.

2. Literature Review

This study by Ahady et al. (2020) aims to show that integrating networks with biometrics data as features enhances performance compared to combining just a single type of feature. A test bed for the improved healthcare monitoring scheme is created that continuously tracks network flow data along with biometrics of patients. For further diagnosis and treatment options, the observed data is sent to a distant server. A collection comprising thousands of records of legitimate and malicious health information has been developed using man-in-the-middle cyber-attacks. After then, the system uses several machine learning techniques to train and test the database for such threats. Results demonstrate the suggested system's reliability in providing accurate DDOS detection (Ahady et al., 2020).

In this study, Arunachalam et al. (2019) examined the issue of detecting prescription fraud. The unique methodology suggests breaking up the domain of the six-dimensional features into a number of sub-domains while taking into account the degree of interaction between the features. The methodology entails filling up incident matrices for every domain before implementing a fresh data-mining strategy for each ordered and categorical domain. The very specialized properties of the prescription data are used to create a model for this technique that will meet the demands placed on it. Using this data-mining methodology, the risk formulations produce riskiness scores for every prescription and every domain. A Matlab method is created to perform batch auditing of the database at hand using this riskiness score, which is scaled to a range of 0 and 1 (Arunachalam et al., 2019).

A machine learning-based multi-class security incident classification model was put forth in this paper by Lee et al. The suggested method was developed utilizing real-time data and a multiclass DDOS classification approach based on neural networks for four classes. In this work, network events were categorized into four separate groups using a machine learning technique using data collected from actual gadgets, accurately capturing the intricate network traffic and features of a real-world healthcare IoT system (Lee et al., 2021).

Inaccurate data gathering by devices might result in incorrect diagnosis and treatment because of security breaches on routes of communication or malicious programs in sensor equipment. Therefore, the confidentiality of health records is of the utmost importance and must be managed with care. Saif et al., (2022) examined new developments in security measures for protecting health data. By examining the conventional architecture, numerous security assaults on clinical information, security needs, accessible solutions, and case studies, this chapter can assist readers in gaining an outline of secure health care. Also highlighted are the unanswered questions in this field, which could serve as an inspiration for researchers.

To discover features and recreate security data, Xu et al., (2021) suggests using a set of CNN techniques that are built on feature correlations. The associations between the features are first measured by computing feature correlation coefficients. The data is subsequently sorted by columns and the correlation coefficients in decreasing order. With the intention to cope up with the grouped data enabling feature learning and reconstruction, a 1D group CNN model is constructed using numerous 1D convolution kernels as well as 1D pooling filters. Third, the recovered characteristics are fed into network threat prediction shadowing ML models. In comparison to the fundamental 1D CNN, grouped CNN can minimize parameters, running time, and Floating Point of Operations (FLOP).

IoT network security has been achieved through a variety of techniques, but there is still much need for improvement. The use of machine learning has been suggested as a means of enhancing IoT security. Susilo et al., (2020) examines a number of ML and DL techniques as well as common datasets for boosting IoT security effectiveness. Using a deep learning algorithm, a denial-of-service (DoS) attack detection system is created. Python is employed in this study along with three different kinds of packages. It is discovered that a DL algorithm might improve accuracy so that an IoT network's ability to mitigate assaults as effectively as possible.

Deep learning has demonstrated its ability to identify trends across a variety of study topics through effective implementation. Cyber-attacks are launched using ever-evolving and unique means. Ullah et al., (2021) has presented a paradigm for IDS for IoT networks. It is based on a DL method with gated recurrent units and a CNN. On six datasets of actual network traffic, the model's efficacy for multiclass as well as binary classification is examined. Comparing the suggested multiclass as well as binary classification models to existing classification methods and contemporary deep learning models, the proposed models showed high values with regard to the examining metrics. The findings gained show the usefulness of the suggested method.

In order to keep a patient record in healthcare networks, this research article by (Akram et al., 2021) presented ANFIS. Utilizing an IDS dependent on ANFIS, the main goal is to find people who have gained access to the network without authorization. The presented security method assists in gathering information regarding malicious activity from network traffic. With the use of an if-then rule phrase and data classification based on ANFIS, it can be used to establish whether or not the network database server was compromised. Researchers can take preventative efforts to offset the loss or block the unauthorized inbound communication if the system is able to recognize the sort of assault.

In order to speed up examinations and provide better treatment recommendations, (Kavitha et al.,2022) proposed a revolutionary smart healthcare framework for monitoring the physical behaviors of adult individuals using IoMT and deep learning algorithms. The IoMT devices broadcast the data collected from various wearable sensors placed on the user's body to the integrated cloud and the data analysis layer. The MapReduce model is ideal for the complex-valued deep CNN with an upgraded political optimizer technique. This is used to categorize the movements made by different body parts since it is more flexible and performs better than other classifiers. The system's greatest value accuracy is regarded as the best method for identifying bodily actions and, consequently, for monitoring the clinical settings of elderly persons.

Sohail et al., (2022), hybrid intelligent IDS based on machine learning and metaheuristic techniques are presented for IoT-based applications like healthcare. Biomedical sensors collect critical health data for IoT-based smart healthcare, which is then delivered to a cloud server for archival and analysis. Security and privacy concerns apply to health information kept in an electronic health record. This research focuses on using anomaly-based DDOS detection to find security assaults on cloud systems. The widely used NSL-kDD dataset has been used to assess how well the suggested technique performs. Metaheuristic methods are utilized to identify the best features, and supervised learning methods are utilized to accurately classify the normal and attack classes dependent on specific characteristics. Additionally, a hybrid strategy for selecting features and categorization has been described.

3. Proposed Methodology

The major objective of this research project is to improve DDOS detection accuracy through the development and use of detection models utilizing deep learning algorithms and to perform an assessment of such through common classification benchmarks. Due to the fact that they use convolution and pooling layers instead of fully linked hidden layers like classic neural networks do, CNNs fall under the genre of regular neural networks (Aminanto et al., 2016). This study proposes a novel type of CNN that can be useful for DDOS detection by learning the content aspects of abnormalities. DL based anomaly detection method have also been compared to well-known classification algorithms such as the decision tree, the K-nearest neighbor (KNN) and also the support vector machine (SVM).

3.1. Dataset Description

Datasets used for DDOS detection and response purposes fluctuate dramatically over time as cyber security vulnerabilities are always changing and evolving, and newer threats are launched every day. The suggested algorithm's performance is assessed using the two types of datasets listed below.

KDDCUP99 dataset: This KDD99 data set, a well-known open data set in the domain of DDOS detection, is the one that is used in this analysis. This data collection represents the kind of network traffic that would be generated by intruders in various complicated networks. This data set's network activities are divided into attack patterns (anomalous) and regular patterns (Regular). Every record in the KDD99 data set, which is described using 41 attributes and recorded in a CSV format, is used to identify a network connection. The final column of each record contains a label that specifies whether the network data is regular or anomalous. Five records are extracted from the data set, representing four distinct types of assault pattern and one regular pattern.

CICIDS2017 dataset: The CIC IDS 2017 dataset is the one that the DDOS detection system prefers since it comprises the most recent, benign and common attacks that closely mirror data from the real world. Additionally, it contains the outcomes of the CIC Flow Meter network traffic assessment, labeled flows depending on the date, source and destination IP addresses and port, protocol, and attack. There are 84 features in all, together with their accompanying traffic status, in this labeled dataset. In addition, CIC IDS 2017 includes coverage for malicious traffic as well as a number of assaults, including brute force attacks, heart bleed attacks, botnet attacks, denial of service attacks, and web attacks.

3.2. Data Preparation

Effective sample data preprocessing is required before building an DDOS detection system with excellent performance. Data preparation can reflect the intrinsic association between the real and the sample data more accurately. It consists of the following steps:

Data Set Cleaning: Data cleaning has two purposes: first, it removes duplicate records from the data collection and filters out redundant information; second, it fills in any features that might have missed value so that it won't interfere with the next step in the preprocessing of the data.

A sample Translation of the Attribute Type: The main goal is to convert the distinctive characteristics and classification of the textual data structures in the collection of data into integers and other high dimension binary data formats.

Sample Category Equalization: There are two sorts of popular sample category equalization techniques. Under sampling is used to increase the number of samples in a class with a low probability distribution, whereas oversampling is employed to reduce the number of samples in a class with a high probability distribution.

Sample Normalization of Attributes**:** By normalizing the data sets, any data in the data collection that have an improper magnitude ordering will be changed into a similar order of magnitude. This makes it easier to cross-operate sample attributes and to correlate various qualities.

Sample Gray Image Conversion: Following the aforementioned data preparation procedures, each sample's attribute is numerical in nature, and its values get mapped into the same interval. Every sample of data must first be translated into a 2D matrix, or a sample gray picture, since the input data for CNN models is often a 2D matrix. Every feature corresponds to a grayscale image pixel. The closer a pixel is near black, the higher the value of the attribute.

3.3. Averaged Convolutional Layer (CNN - ACL)

In order to distinguish anomalies from regular data, this study proposes a CNN-based layer. Using data to immediately learn about changes brought on by anomalous data is the strategy employed. The fundamental problem is that the differences between regular and anomalous flows are negligible, thus the CNN must be driven to recognize variations in abnormal flows. It is evident that when conventional form CNNs are employed to detect, features that predominantly reflect regular flow are learned to represent the content (or flow) of an image, which means that the classifier learns training data rather than learning data variances. The strategy employed here, however, is intended to pause the content and gradually learn anomaly traces. To accomplish this, a novel convolutional layer called the averaged convolutional layer (CNN -ACL), designed to be used with IDS activities, is developed.

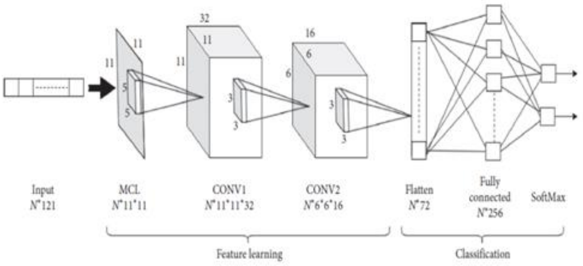

Fig. 2. Proposed Architecture Design

The proposed architecture's general design, comprising each layer in detail, is shown in Figure 2. This framework can uncover new associations between the feature maps of deeper layers by gaining a greater degree of representation for the already discovered regular/abnormal features. The output of the last convolution layer is supplied to the classification block, which consists of a fully connected and a SoftMax layer, after it has been flattened.

In contrast to the CNN designed to perform IDS functions, the CNN-ACL can be positioned differently. Given that flow content is typically excluded from prediction errors, this serves as a means of containing the content while still providing CNN with low-level IDS features. The bottom-level anomalous features enable deeper layers of said CNN to discover top-level features. The CNN-ACL can be defined by the equation below, where M stands for the Mth CNN-ACL, n stands for the nth convolutional filter inside a layer, while(v_p, v_q) denotes the central value of the convolutional filter. The CNN is then made to actively apply particular constraints, which force it to discover prediction error filters:

$$\mu^M = Mean(w^{(M)}(v_p, v_q))$$

$$\begin{cases} w_n^M(p,q) = \dfrac{w_n^M \times \mu^M}{\sum w_n^M}, \qquad (p,q) \neq (v_p, v_q) \\ \qquad w_n^M(p,q) = -\mu^M(p,q) = (v_p, v_q) \end{cases} \quad --- (1)$$

A unique training procedure is used to create CNN-ACL predictions. The Adam method then enters the backpropagation stage, updating the filter weights w_n^M at each iteration. Then, CNN-ACL reinforcement sets the upgraded filter weights into the workable array of prediction error filters, and projection is applied during each training iteration. Algorithm 1 contains this process' pseudo code.

Algorithm 1: Pseudocode of CNN-ACL

```
Create $w'_k$ using $k$ weights that are drawn at random
$i = 1$
$\boldsymbol{while}\ i \le maximum\_iter\ \boldsymbol{do}$
```

```
    Pass feedforward
    Upgrade forever weights using Adam and backpropagation
        faults
    Set the $\mu^M$ = mean of all the filters' central points in layer M
    Using $w_n^M(p,q) = \frac{w_n^M \times \mu^M}{t\sum w_n^M}$, upgrade layer M's weight
    Using the $w_n^M(p,q) = -\mu^M$ values, modify the weights of the
        center points of the n    filters in layer m.
    $i = i + 1$
    If training accuracy converges
    Then
Exit
End
```

Particularly, $f(P)$ is a classifier that makes predictions using the characteristics that are extracted during feature extraction. Additionally, in the event where $g(I)$ is the extracted feature, the whole procedure is produced as $f\big(g(I)\big)$. In the section on feature extraction, we presume a network including one CNN-ACL plus one CNN. The classifier used to generate the output (predictions) when using standard CNN by this equation:

$$f(P) = f\big(g(I)\big) = f\left(\sum_{n=1}^{N} I * w_{nj} + b_{nj}\right) - - - (2)$$

where n indicates the number of channels, w_{nj} represents the weights of the n^{th} channel of the j^{th} filter, and b_{nj} denotes its respective bias term, and f is the classifier function while g represents the feature extraction procedure. Then I represents input data with* representing convolution.

The classifier uses the following equation to find the anomaly:

$$f(P) = f\big(g(I)\big) = f\left(\sum_{n=1}^{N} I * \widetilde{w}_{nj} + b_{nj}\right) - - - (3)$$

where $\widetilde{w}_{nj}$ denotes the weights produced using the CNN-ACL from the j^{th} filter's n^{th} channel. Using equations (1) and (3)

$$f(P) = f\big(g(I)\big) = f\left(\sum_{n=1}^{N} I * \frac{w_n^M \times \mu^M}{\sum w_n^M} + b_{nj}\right) - - - (4)$$

$$f\big(g(I)\big) = f\left(\sum_{n=1}^{N} I * \frac{w_n^M \times Mean(w^{(M)}(v_p, v_q))}{\sum w_n^M} + b_{nj}\right) - - - (5)$$

Since equation (5) lacks the subscript n, it is clear that the $Mean(w^{(M)}(v_p, v_q))$ is derived from all channels. As a result, all channels share the mean value. These operations progress the impact of aberrant changes to be taken into account as the retrieved features while decreasing the effect of regular context to be retrieved as beneficial features.

3.4. Machine Learning Classifiers

The ML-based techniques will analyze the scenario for patient monitoring based on the trained dataset. The following is a brief description of a few supervised machine learning (ML) algorithms for training and evaluating the proposed system for DDOS detection.

Decision Tree: The Decision Tree can be described as a predictor whose aim is to anticipate the labeling of a sample by learning the decision rules deduced from the training set and employing a tree model to this end. A root node serves as the representation's starting point, and each leaf node follows. In order to determine the significance of a feature in a given dataset, a feature selection approach is normally employed as the criterion. Notably, the best feature in a classification task is always positioned at the root node of said tree model, whereas every leaf node carries a particular label. On each subset, this procedure is carried out once again until all leaf nodes are located. Pruning is a step that can be taken towards the final part of the DT technique to prevent overfitting. The tree will be pruned by having its leaves and useless branches cut off. Once the most crucial characteristic has been identified through a feature selection method, it is positioned at the root node and utilized to evaluate if the traffic flow in examination is normal or requires additional analysis in order to be classed as regular or abnormal. The method is reiterated until the traffic flow is categorized as regular or abnormal traffic, at which point the next most crucial attribute is employed if the traffic flow requires additional analysis.

K Nearest Neighbour: The classification uses the analogous k-NN technique is compared to the test record to that of training record which has similarities. When formulating a prediction, it initially stores the entire training dataset and does searches to identify the k training patterns that are the most similar. It contrasts the training examples with the unlabeled data. Each trial in the training dataset has a class name attached to it; the training dataset is a matrix in a multidimensional space. In the classification process, the constant variable k is user-defined, and an unidentified vector is selected by stating the class that occurs as most frequent among some of those k training cases that are closest to the query instance. A common measurement of distance is the Euclidean distance.

Support Vector Machine: SVM classifies the data points using an N-dimensional space hyperplane. N is the total number of features in the dataset. The classifier works by locating a hyperplane that separates two classes in such a manner that the distance in between hyperplane and the nearest point of each class is maximized. By adjusting the use of SVM kernels such linear, polynomial and hyperbolic tangent, various classification tasks can be completed. Although SVM is mostly used for binary classification, it may also be used for multi-class classification by determining the best hyperplane amongst each pair of classes. The SVM utilized for this particular dataset is a parametric technique called linear SVM.

4. Results and Discussion

Two well-known datasets termed KDDCUP99 and CICIDS2017are used in a series of tests and analyses to assess the performance of the suggested methodology. The CNN-ACL model is validated through experimental work, and its performance is compared to that of three other machine learning classifiers. Accuracy, precision, and recall are examples of measures (metrics) that can be employed to evaluate this performance. A confusion matrix is the precursor to a performance matrix. A table called a confusion matrix shows how well a classification algorithm performed when compared to actual classification. The 2 x 2 confusion matrix used for evaluation in this instance defines two classes: regular and anomalous.

Accuracy: The degree to which the projected value and also the actual value are close to one another is shown by this. A method of evaluating classification models is accuracy and it is calculated using equation 6,

$$\boldsymbol{Accuracy} = {\boldsymbol{TP + TN}}/{\boldsymbol{TP + TN + FP + FN}} \quad (6)$$

Precision: This explains how closely the model's anticipated outcomes match the requested data in terms of accuracy. The proportion of accurate positive forecasts to overall positive expected results is hence known as precision,

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \quad (7)$$

Recall: This category provides the ratio of true positives to all true positives with false negatives.

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad (8)$$

where TP, TN, FP, and FN stand for true positive, true negative, false positive, and false negative, respectively

4.1. KDDCUP99 Dataset Analysis

Accuracy Analysis: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over KDDCUP99 Dataset. The following Table 1 and Figure 3 represents Accuracy Analysis of proposed CNN-ACL compared over KNN, DT and SVM. From the results its proved that proposed CNN-ACL produces Accuracy of about 91% which is higher than KNN Accuracy which is 86%, DT Accuracy which is 87% and SVM Accuracy which is 89% respectively.

Table 1. Accuracy Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Accuracy (%)	DT Accuracy (%)	SVM Accuracy (%)	CNN-ACL Accuracy (%)
10	85.24	86.75	88.98	89.78
20	85.85	87.20	89.31	90.15
30	86.20	87.51	89.70	90.55
40	86.80	87.99	89.89	90.80
50	86.99	88.94	89.95	90.89

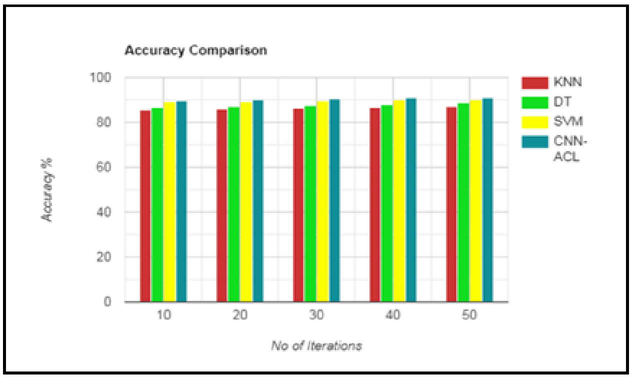

Fig. 3. Accuracy Analysis of CNN-ACL with other Existing Algorithms Graph

Precision Analysis: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over KDDCUP99 Dataset. The following Table 2 and Figure 4 represents Precision Analysis of proposed CNN-ACL compared over KNN, DT and SVM.

Table 2. Precision Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Precision	DT Precision	SVM Precision	CNN-ACL Precision
10	0.81	0.83	0.84	0.86
20	0.83	0.84	0.85	0.87
30	0.84	0.85	0.85	0.89
40	0.84	0.85	0.86	0.90
50	0.84	0.85	0.86	0.91

From the results its proved that proposed CNN-ACL produces Precision of about 0.90 which is higher than KNN Precision which is 0.84, DT Precision which is 0.85 and SVM Precision which is 0.86 respectively.

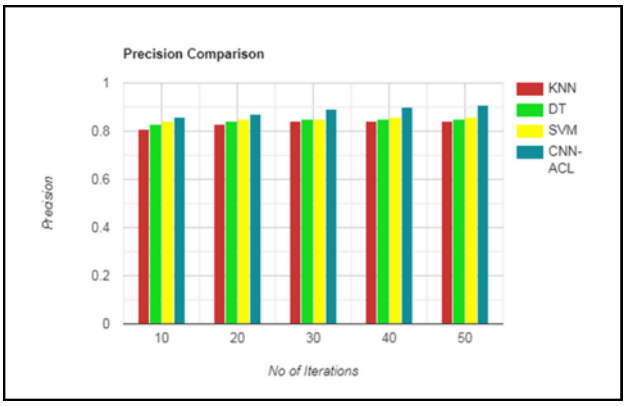

Fig. 4. Precision Analysis of CNN-ACL with other Existing Algorithms Graph

Recall: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over KDDCUP99 Dataset. The following Table 3 and Figure 5 represents Recall Analysis of proposed CNN-ACL compared over KNN, DT and SVM. From the results its proved that proposed CNN-ACL produces Recall of about 0.86 which is higher than KNN Recall which is 0.77, DT Recall which is 0.82 and SVM Recall which is 0.84 respectively.

Table 3. Recall Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Recall	DT Recall	SVM Recall	CNN-ACL Recall
10	0.76	0.80	0.82	0.84
20	0.76	0.81	0.83	0.85
30	0.77	0.82	0.84	0.86
40	0.77	0.83	0.84	0.86
50	0.79	0.83	0.84	0.86

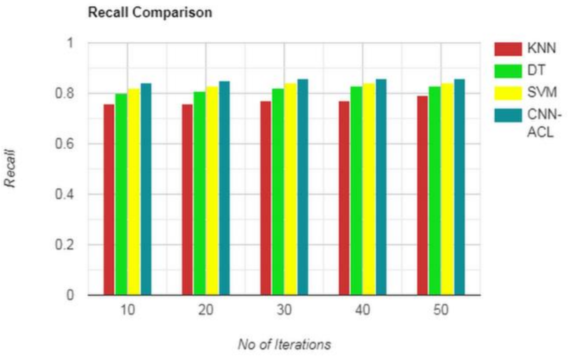

Fig. 5. Recall Analysis of CNN-ACL with other Existing Algorithms Graph

4.2. CICIDS2017 Dataset Analysis

Accuracy: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over CICIDS2017 Dataset. The following Table 4 and Figure 6 represents Accuracy Analysis of proposed CNN-ACL compared over KNN, DT and SVM. From the results its proved that proposed CNN-ACL produces Accuracy of about 91.2% which is higher than KNN Accuracy which is 84%, DT Accuracy which is 88% and SVM Accuracy which is 89.5% respectively.

Table 4. Accuracy Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Accuracy (%)	DT Accuracy (%)	SVM Accuracy (%)	CNN-ACL Accuracy (%)
10	83.55	87.94	89.16	90.15
20	84.24	88.62	89.55	90.45
30	84.36	88.75	89.72	90.57
40	84.75	88.94	90	91.05
50	87.25	89.78	90.15	91.47

Table 1 has the performance values for Accuracy, in percentage.

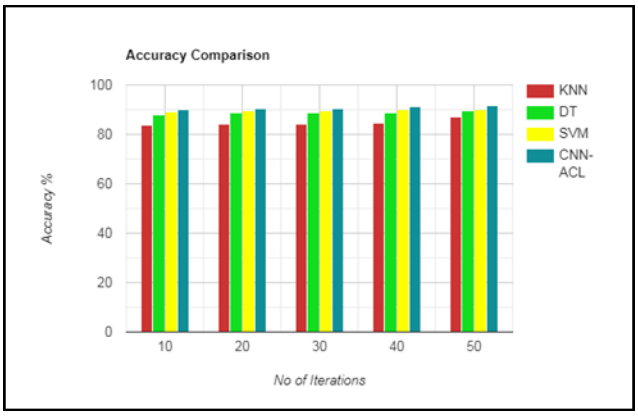

Fig. 6. Accuracy Analysis of CNN-ACL with other Existing Algorithms Graph

Precision: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over CICIDS2017 Dataset. The following Table 5 and Figure 7 represents Precision Analysis of proposed CNN-ACL compared over KNN, DT and SVM. From the results its proved that proposed CNN-ACL produces Precision of about 0.87 which is higher than KNN Precision which is 0.83, DT Precision which is 0.84 and SVM Precision which is 0.85 respectively.

Table 5. Precision Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Precision	DT Precision	SVM Precision	CNN-ACL Precision
10	0.81	0.82	0.84	0.86
20	0.81	0.83	0.84	0.86
30	0.83	0.84	0.85	0.87
40	0.83	0.84	0.85	0.87
50	0.83	0.84	0.85	0.87

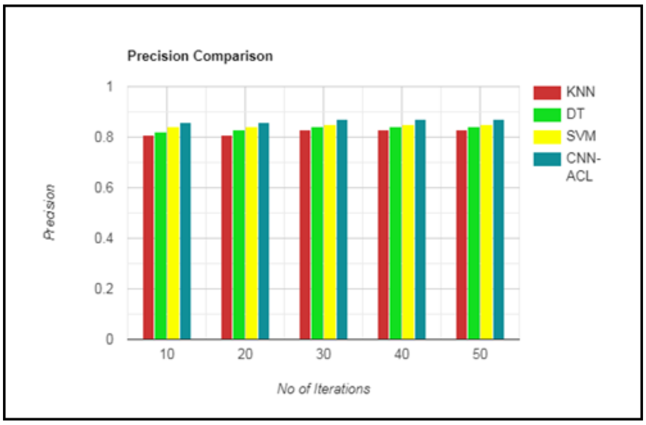

Fig. 7. Precision Analysis of CNN-ACL with other Existing Algorithms Graph

Recall: Now we are going to apply our proposed CNN-ACL algorithm along with existing algorithms such as KNN, DT and SVM over CICIDS2017 Dataset. The following Table 6 and Figure 8 represents Recall Analysis of proposed CNN-ACL compared over KNN, DT and SVM. From the results its proved that proposed CNN-ACL produces Recall of about 0.86 which is higher than KNN Recall which is 0.75, DT Recall which is 0.82 and SVM Recall which is 0.84 respectively.

Table 6. Recall Analysis of CNN-ACL with other Existing Algorithms

No of Iterations	KNN Recall	DT Recall	SVM Recall	CNN-ACL Recall
10	0.74	0.80	0.83	0.85
20	0.75	0.81	0.84	0.86
30	0.75	0.82	0.84	0.86
40	0.76	0.82	0.84	0.86
50	0.77	0.83	0.84	0.86

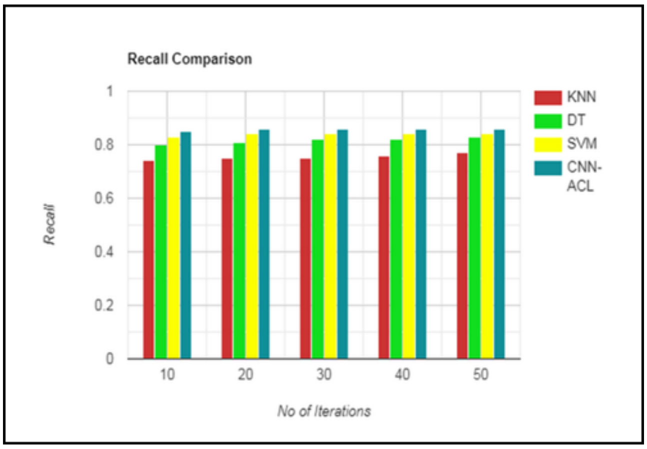

Fig. 8. Recall Analysis of CNN-ACL with other Existing Algorithms Graph

In terms of Accuracy we have evaluated four algorithms with 50 iterations on both datasets. From the Accuracy Table and graph we can analyse that the average Accuracy of KNN is 84%, DT is 88%, SVM is 89% and CNN-ACL is 92%. From the results we can prove that CNN-ACL outperforms other algorithms in terms of Accuracy.

In terms of Precision we have evaluated four algorithms with 50 iterations on both datasets. From the Precision Table and graph we can analyze that the average Precision of KNN is 0.83, DT is 0.84, SVM is 0.85 and CNN-ACL is 0.87. From the results we can prove that CNN-ACL outperforms other algorithms in terms of Precision.

In terms of Recall we have evaluated four algorithms with 50 iterations on both datasets. From the Recall Table and graph we can analyze that the average Recall of KNN is 0.75, DT is 0.82, SVM is 0.84 and CNN-ACL is 0.86.

From the results we can prove that CNN-ACL outperforms other algorithms in terms of Recall.

5. Conclusion

In this study, we used a unique deep learning-based approach to design and create an DDOS detection model for the Internet of Medical Things. The proposed CNN-ACL may inhibit flow content and adjust to learn variation detecting features from data directly, in contrast to the standard CNN that depends on content features. Numerous tests were run on two different datasets, KDDCUP99 and CICIDS2017, to see how well the presented CNN-ACL model performed DDOS detection. The results of the investigations portrayed that it is feasible to train the CNN-ACL such that it will precisely distinguish between regular and anomalous flows as well as different sorts of known attacks. In comparison to well-known machine learning algorithms like SVM, DT, and KNN, the proposed model has demonstrated superior performance in detecting the anomaly. In the upcoming study, we intend to create this DDOS detection system employing fuzzy logic, which is regarded as one of the most effective methods for deliberating under uncertainty in the context of DDOS analysis.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] F. Akram, D. Liu, P. Zhao, N. Kryvinska, S. Abbas and M. Rizwan, "Trustworthy intrusion detection in e-healthcare systems," *Frontiers in public health*, vol. 9, pp. 788347, 2021.

[2] S. Arunachalam, A. Sivasankari and S. Arthi, "Identifying The Fraud Detection in Health Care System Using Machine Learning," 2019. DoI: 10.13140/RG.2.2.17720.88328.

[3] A. A. Hady, A. Ghubaish, T. Salman, D. Unal and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," IEEE Access, vol. 8, pp. 106576-106584, 2020.

[4] E. Aminanto and K. Kim, "Deep learning in intrusion detection system: An overview," In *2016 International Research Conference on Engineering and Technology (2016 IRCET)*, pp 1-12, Seoul, South Korea

[5] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and trends® in signal processing*, vol. 7, no. 3, pp. 197-387, 2014.

[6] IBM 2016 "Cost of Data Breach Study United States," I. Corp, Washington, DC, USA, 2016 September.

[7] D. Kavitha, A. Vidhya, V. Prema, M. Priyadharshini, G. Kumaresan and G. Sangeetha, "An efficient IoMT based health monitoring using complex valued deep CNN and political optimizer," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 12, pp. ett.4610, 2022.

[8] J. D. Lee, H. S. Cha, S. Rathore and J. H. Park, "M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT," Computers, Materials & Continua, vol. 67, no. 2, 2021.

[9] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," Computer Communications, vol. 160, pp. 139-149, 2020.

[10] K. K. Patel, S. M. Patel and P. Scholar, P. "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," International journal of engineering science and computing, vol. 6, no. 5, 2016.

[11] J. Rosen and B. Hannaford, "Doc at a distance," IEEE spectrum, vol. 43, no. 10, pp. 34-39, 2006.

[12] E. K. Wang, C. M. Chen, M. M. Hassan and A. Almogren, "A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain," Future Generation Computer Systems, vol. 108, pp. 135-144, 2020.

[13] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," Security and Communication Networks, pp. 1-9, 2018.

[14] S. Saif, P. Bhattacharjee, K. Karmakar, R. Saha and S. Biswas, "IoT-Based Secure Health Care: Challenges, Requirements and Case Study," In Internet of Things Based Smart Healthcare: Intelligent and Secure Solutions Applying Machine Learning Techniques, pp. 327-350, 2022.

[15] S. Saif, P. Das, S. Biswas, M. Khari and V. Shanmuganathan, "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," Microprocessors and Microsystems, pp. 104622, 2022.

[16] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," *Information*, vol. 11, no. 5, 279, 2020.

[17] I. Ullah, A. Ullah, and M. Sajjad,"Towards a hybrid

deep learning model for anomalous activities detection in internet of things networks," IoT, vol. 2, no. 3, pp. 428-448, 2021.

[18] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3723-3768, 2019.

[19] Y. Xu, X. Zhang, C. Lu, Z. Qiu, C. Bi, Y. Lai, and H. Zhang, "Network threat detection based on group CNN for privacy protection," Wireless Communications and Mobile Computing, pp. 1-18, 2021.

[20] Mr. Bhushan Bandre, Ms. Rashmi Khalatkar. (2015). Impact of Data Mining Technique in Education Institutions. International Journal of New Practices in Management and Engineering, 4(02), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/35

[21] Satyanarayana, K. ., Aharon, S., Subramanyam, M., Chakradhari, C., & Anand, K. (2023). A Hybrid Microgrid Operated by PV Wind and Diesel Generator with Advanced Control Strategy. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 171–181. https://doi.org/10.17762/ijritcc.v11i4s.6325