International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# DDoS Attack Detection in Cloud Computing Using Deep Learning Algorithms

**Marram Amitha*[1], Dr. Muktevi Srivenkatesh[2]**

**Submitted**: 10/05/2023 **Revised**: 17/07/2023 **Accepted**: 08/08/2023

**Abstract:** Distributed cloud computing and its reliance on internet connectivity have more challenges. They offer a great deal of flexibility, and these assets are accessible through the Internet using popular requirements, forms, and protocols for networking according to the cloud service-providing organizations. Attacks like distributed denial of service are a few of the most frequent attacks that severely harm the cloud and lower its performance. Internal attacks cannot be identified using established methods of detection such as firewalls. The attackers frequently modify their skill strategies, because of the increasing amount of data created and stored, conventional detection techniques are inefficient in identifying novel DDoS attacks. Radial Basis Function (RBF) networks are a type of artificial neural network commonly used for function approximation, pattern recognition, and classification tasks. While they have been used in various domains, they are not typically used directly within convolutional neural networks (CNNs) for DDoS (Distributed Denial of Service) detection. This paper presents a hybrid model of Radial Basis Function (RBF) and LSTM networks-based approach for DDoS attack detection and mitigation, aiming to enhance the overall security of cloud computing infrastructures. Our proposed method is evaluated on benchmark dataset CICDDoS2019, demonstrating its effectiveness in identifying DDoS attacks and mitigating their impact on cloud systems.

***Keywords:*** *Cloud computing, Deep Learning, distributed denial of service*

## 1. Introduction

Distributed Denial of Service (DDoS) attack is an immense threat to the Internet-based system and its resources. Researchers employ statistical, machine/deep learning, information theory, etc., based detection methods to protect the victim system from DDoS attacks. Cloud computing is an Internet-enabled platform that allows businesses to share computer resources with consumers in organizations on a large scale while simultaneously reducing costs for that organization. In recent years, cloud computing has become popular as a choice for sharing massive volumes of accessible data. All electronic gadgets, including computers, phones, and tablets, can use cloud services. The computing cloud environment's structure is depicted in figure1. Most cloud computing services are of the pay-on-demand variety, where each user is given access to a certain pool of data mining equipment.

Infrastructure as a Service, Software as a Service, and Platform as a Service are the three main categories of cloud computing services. By providing an assortment of online resources in the manner of services, cloud computing helps companies and people reduce the cost of infrastructure. In the world of cloud computing, organizations pay for the service time that really use, in keeping with the paying-as-you-go policy. Security in cloud computing was the greatest challenge to the service providers. According to the Kaspersky Lab report, DDoS attack incidents do not only increase in number but also grow by attack duration and volume size[1]. There are several reasons behind this, such as the exponential growth of less-secure IoT devices, readily available user-friendly attack tools, security flaws in the network, the decentralized architecture of the Internet, etc.

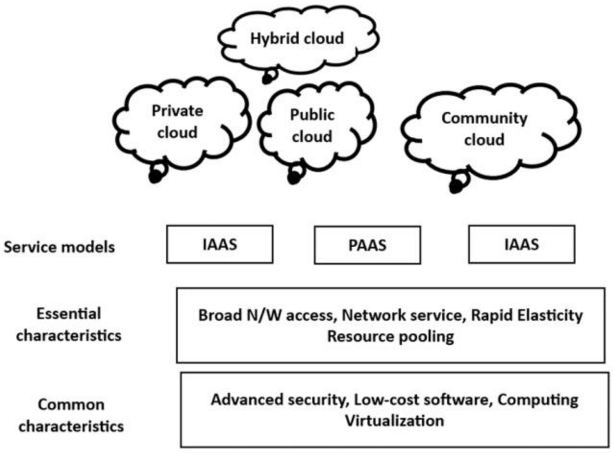
Hybrid cloud
Private cloud
Public cloud
Community cloud
Service models
IAAS
PAAS
IAAS
Essential characteristics
Broad N/W access, Network service, Rapid Elasticity Resource pooling
Common characteristics
Advanced security, Low-cost software, Computing Virtualization

**Fig. 1.** The cloud computing environment architecture

### 1.1. DDoS Attacks in Cloud Computing

Denial of service attacks occur when an attacker attempts to block an everyday process of transformation. The attacker will transform everyday information into zombies and unleash a flood to block routine data.

There are a total of four phases to a DDoS attack, involving

[1] *Department of Computer Science GITAM Deemed to be University, India ORCID ID : 0000-0002-0526-1707*
[2] *Department of Computer Science GITAM Deemed to be University, India ORCID ID : 0000-0001-9631-6402*
** Corresponding Author Email: 121962504006@gitam.in*

monitoring, detection, prevention, and mitigation. The DDoS assault is identified in the detection phase. DDoS attacks are an increasingly common kind of cyber-attack that are utilized by attackers to stop other people from accessing services by providing unauthorized and disrupted services to network users. The life cycle of a DDoS attack is shown in Figure 2.

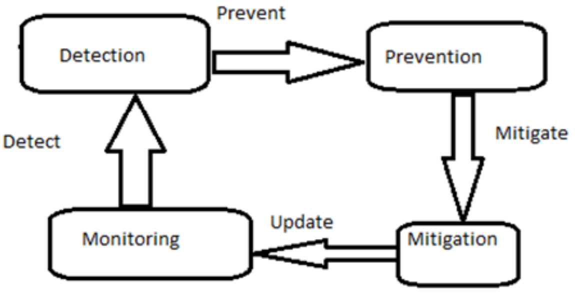

**Fig.2**. Attack Life Cycle of DdoS

A DDoS attack involves the use of multiple compromised systems to flood a target system with an overwhelming amount of traffic, rendering it unable to respond to legitimate requests [1]. Cloud computing systems are particularly vulnerable to DDoS attacks due to their highly distributed and resource-sharing nature [2]. Several types of DDoS attacks have been identified, including volumetric attacks, protocol attacks, and application-layer attacks [3].

### 1.2 DDoS Attack Detection Techniques

These techniques can be broadly classified into signature-based, anomaly-based, and hybrid approaches [4]. Signature-based techniques rely on pre-defined patterns or signatures of known DDoS attacks to identify potential threats. These methods are effective in detecting known attacks but are unable to detect new or unknown attack patterns [5]. Anomaly-based techniques monitor the network traffic and system behavior for deviations from a predefined normal baseline. These techniques can recognize unidentified attacks, but they could have massive false-positive rates [6]. The strengths of anomaly-based and signature-based approaches are brought together in hybrid approaches, increasing the performance of identification [7] as shown in Figure 3.

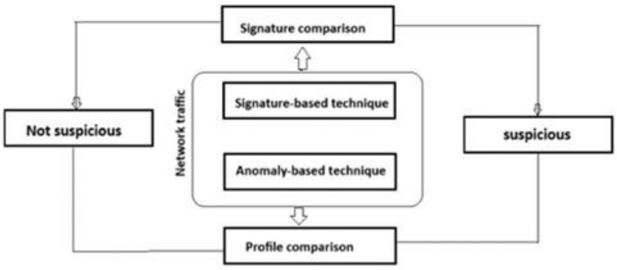

**Fig 3.** The architecture of signature and anomaly-based techniques

### 1.3 Deep Learning for DDoS Attack Detection

Deep learning algorithms give good results and overcome the limitations of traditional DDoS attack detection techniques [8]. These algorithms can automatically learn complex patterns and relationships xz in data, making them well-suited for detecting DDoS attacks in cloud environments [9]. The most effective method to avoid attacks using DDoS is to act immediately as they occur. When machine learning and deep learning reveal their great potential across many fields, businesses and researchers are looking into ways for Machine learning and deep learning to combine for DDoS prevention. Machine learning methods such as random forest, KNN, and Naive Bayesian, threats can be recognized more precisely and efficiently. DNN is a possible way of spotting attacks in social networks because it includes an accumulation of numerous levels of computational units and is asymmetric for modification and extraction characteristics. When an attack is identified, minor modifications in the pixel tend to identify image changes as over 99 percent of new attacks are minor mutations of previous attacks. If a binary classification algorithm is utilized to recognize attacks from new combined representations, deep learning gets more efficient at detecting minute variations between attack representation sequences from a dataset that is imbalanced [5].

To detect the DDoS attack in Network, K- medoid clustering and K Nearest Neighbor algorithm was used and provided better cyber security and protects critical, (liu et al., 2018) [24] infrastructure in network.

Zareapoor et al. (2019)[19] proposed the Artificial Neural Network (ANN) model of detecting the unknown attacks in network. DDoS attack in Network and this ANN model of DDoS Detection technique given the results in an efficient manner and it was evaluated under the three categories accuracy, sensitivity, and specificity.

### 1.4 DDoS Attack Mitigation Techniques

In addition to detecting DDoS attacks, it is crucial to develop effective mitigation strategies to minimize their impact on cloud systems [10]. Some of the commonly used DDoS attack mitigation techniques include traffic filtering, rate limiting [11], and IP blocking [12]. However, these traditional methods may not be sufficient to handle sophisticated DDoS attacks in cloud environments. Deep learning algorithms have also been explored for DDoS attack mitigation [13]. These approaches can learn to adaptively respond to evolving attack patterns and develop more targeted mitigation strategies.

#### 1.4.1. Reinforcement learning (RL)

Reinforcement learning (RL) can be applied to enhance DDoS mitigation strategies by creating adaptive and dynamic defense mechanisms. RL is a machine learning paradigm where an agent learns to take actions in an environment to maximize a reward signal over time. In the context of DDoS mitigation, RL can help in building more intelligent and responsive defense systems (Y. Liu et.al 2019).[11] While RL offers the potential for adaptive and intelligent DDoS mitigation, it is important to note that implementing such systems can be complex and requires a good understanding of both reinforcement learning and network security. Additionally, due to the potential risks of false positives or misinterpretation of actions, integrating RL-based mitigation with traditional security measures is recommended for a comprehensive defense strategy.

## 2. Literature Survey

R. K. Gupta et al. 2022 [7] present a cutting-edge method to detect HTTP DDoS attacks in an online environment. A time-based window sliding technique is applied within the Open Stack system to evaluate the level of randomization in the network headers that represent a characteristic of the traffic that arrives signal.

Khuphiran Panida, et al 2018 [8] proposed an unusual detection technique in the virtualization layer to reduce the activity of DDoS attacks. The developing neural network developed the recommended detection method. Particle swarm optimization (PSO) and neural networks combine in the evolutionary neural network to recognize DDoS attacks and classify traffic data. [9]. They used KDD CUP 99 and NSL-KDD datasets to evaluate models.

Cholleti et al., 2023[13] analyzed different machine algorithms and DDoS Detection techniques based on anomaly detection. He concluded in his research that machine learning algorithms are smart to detect DDoS attacks. Traditional approaches are not suitable for anomaly detection of DDoS attacks.

Sharaf et al., 2022[14], conducted a Comparative study between the data sets using different machine-learning algorithm types. The author concluded that machine learning algorithms based on unsupervised models are suitable for anomaly detection. Supervised learning models are not suitable for detecting unknown attacks.

Srikanth Yadav M et.al 2022 [25], proposed A model for deep learning called Non-symmetric Deep Autoencoder based on shallow machine learning to perform Random Forest. Compared to the encoder-decoder architecture of a typical autoencoder, NDAE simply includes an encoder. The use of a model based on deep learning was selected to address the challenges imposed on the shallow machine learning framework having extended periods of training as well as greater memory and processing demands [9]. Therefore, NDAE was picked since it has an increased degree of accuracy while utilizing less CPU memory and training time. The distributed denial of service (DDoS) detecting model's accuracy was evaluated by employing the datasets KDD-NSL and CIC-IDS2017. In the CIC-IDS2017 and NSL-KDD data sets, the NDAE model received accuracy scores of 99.60% and 99.24%, respectively, establishing that it is suitable for recognizing attacks.

The Multimodal Deep Auto Encoder (M2-DAE) model was developed by Rabbani et al. [18] with the objective of detecting intrusions in the IoT. This approach was chosen since it provides distributed ideas that are extremely efficient and adaptable while additionally preserving privacy. However, this methodology wasn't used to evaluate the attack classes. kingma et al. [12] organized the network attacks utilizing machine learning. Here, an advanced array of features was taken into consideration for the initial classification. Wang [16] recommend using an ANN in the IDS that detects unusual behavior on the network to identify DDoS attacks. The artificial neural network (ANN) technique has been shown to be more precise when it was independently tested in research.

G. Oke et,al [26] proposed a model to detect DDoS attacks using Circular Radial basis function (CRBF), Neural Network RBF Superior accuracy, and global approximation using a neural network with a feed-forward algorithm model. An input layer, a hidden layer, and an output layer are in fact all three layers of RBF. A node known as RBF units, which is a node representing a Gaussian function, may be found in the hidden layer. The localization function center and width of an RBF neural network are determined by two essential factors. When the center and width of the CRBF neurons are chosen at random, the order that the data points that appear inside the input area could not be exactly equal. A typical CRBF neural network is a locally weighted network that emphasizes certain portions of the training data set. In training, the hidden layer's "base" is CRBF, and the input vector is moved immediately to the hidden space. [16].

## 3. Methodology

Cloud computing has revolutionized the way organizations store, process, and manage their data, offering cost-effective and scalable solutions for a wide range of applications. However, the increasing reliance on cloud services has made them attractive targets for cybercriminals. Among various cyber threats, Distributed Denial of Service attacks have emerged as a significant challenge, causing severe disruption to cloud-based services, and affecting the availability and reliability of resources. DDoS attacks are typically launched by overwhelming targeted systems with massive amounts of traffic from multiple sources, making it difficult for the system to distinguish between legitimate and malicious requests. The impact of DDoS attacks can be devastating, leading to substantial financial losses, reputational damage, and loss of customer trust. Therefore, early detection and mitigation of DDoS attacks are crucial for ensuring the security and availability of cloud services. In numerous areas such as recognizing images, natural language processing, and cyber security, deep learning algorithms have had amazing results. These algorithms have the potential to learn complex patterns and relationships within data, making them well-suited for detecting DDoS attacks in cloud environments.

### 3.1 Random Forest

As the title of the methodology suggests, this methodology includes a huge volume of Trees of individual choice acting as an ensembling model. Every tree of choice in the random forest churns out a group forecasting and the group with the majority votes turns out the forecasting of the framework. The core idea behind this methodology is collective wisdom, a plain yet strong one. The rationale that this methodology paradigm performs so well in data science as any of the behaviors of individual models will be surpassed by a huge volume of relatively uncorrelated frameworks working as a committee. The main aspect is the low association between the frameworks. When low-correlation portfolios (such as stocks and bonds) come together to construct unrelated frameworks may provide ensemble forecasts that are more trustworthy than any one of the many projections for a portfolio that is higher than the total of its parts. This magnificent effect has been explained by the trees defending each other (as long as they do not all err in the same direction) from their mistakes. While some trees are wrong, numerous other trees are accurate, since they travel as a cluster in the proper direction.

### 3.2 Support Vector Machine (SVM)

The major aim of this methodology is to determine a hyperplane that separates into various groups in a space that consists of N attributes. Various possible hyperplanes can be chosen to differentiate between the two information point groupings. The major aim of this methodology is to determine a plane that has the highest margin, i.e. the maximum gap among all data points that belong to various classes. Enhancing the width disparity provides some assistance in classifying additional trust into possible information items. The data points belonging to various classes will be separated with the aid of decision boundaries which are nothing but hyperplanes. The number of features decides the dimension of the hyperplane. The data points nearer to the hyperplane and those points that can impact the position, as well as the hyperplane alignment, is termed vectors of support. These support vectors play a vital role in maximizing the gap among the various classifiers. These support vectors are helpful in building an SVM-based model.

### 3.3 Deep Sequential Model

Whenever both the input and the output are sequences of data, deep sequential models are implemented. The data points can be placed into sequences so that observation at a single instance in a sequence can be used to infer significant details regarding observation at other points in the sequence.

When a parameter is a sequence and an output is a single data point, such as in the instances of video action identification, sentiment classification, and stock price predictions, the sequence learning issue can arise. Managing continuous supervised learning tasks is necessary for sequence data.

Detecting Distributed Denial of Service (DDoS) attacks using deep sequential models is a complex task, DDoS attacks involve overwhelming a target system with a flood of incoming requests, causing it to become slow or completely unavailable. Deep sequential models, such as Recurrent Neural Networks (RNNs) or Long Short-Term Memory Networks (LSTMs), can be used to analyze the temporal patterns of network traffic data and identify abnormal behavior associated with DDoS attacks.

In other scenarios, including in the synthesis of speech, composing music, and image closed-captioning the output may be an assortment of points of data and the input only includes one information point.

Deep learning neural networks have mostly been used in the areas of analysis of images, voice recognition, and natural language processing in which they have shown the ability to encode exceedingly complex input and output mapping.

This idea eventually resulted in the development of multiple deep-learning time series forecasting structures that exceed conventional methods in terms of accuracy and effectiveness.

### 3.4 Long Short-Term Memory Networks

Sequence processing of input neural network types includes recurrent neural networks. Previously predicted amounts can use as inputs because of hidden states. A multilayer perceptron is an RNN. It has been through a pattern. Input, output, and a hidden layer serve as its framework. A multilayered perceptron's n layers are chosen by the order in which they are generated. The deep learning algorithm was developed using the assistance of the Keras software platform. A structure must be maintained as data enters, is retained by the algorithm, and accesses pointless use of three gates: an input gate, a memory gate, and an output gate. The three of these gates, which constitute most of the model known as LSTM, are in the position of regulating everything's monitoring as shown in Figure 3. The part of the gate that forgets will decide which components of the LSTM should now be discarded, according to equation 1, utilizing a combination of the previously concealed state and the data item being processed by the sequencing. The input portion of the gate's computational equation is denoted by equation 2.

$$F(t) = \sigma\left(w_f\left[h_{(t-1)}, X_t\right] + b_f\right) \quad (1)$$

$$I(t) = \sigma\left(w_i\left[h_{(t-1)}, X_t\right] + b_i\right) \quad (2)$$

$$f(x) = \frac{1}{1+e^{axt}} \quad (3)$$

$$\tanh(x) = \frac{2}{1+e-2^x} - 1 \quad (4)$$

The output gates must generate the new hidden state. The decision that follows was selected as a result of the relationships between the most recent input data, the least current hidden state, and the most current actual cell state.

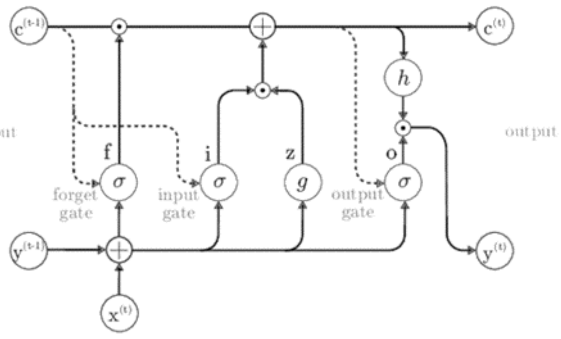

**Fig.4.** Architecture of LSTM

The values of the weights for the forget gate, input gate, and output gate were Wf, Wi, and Wo, respectively. Equation 4 indicates that the most current input and the hidden layer input that was provided previously it were both sources of information used by the formula operator sigmoid. The (tanh) function is utilized for sharing with data regarding the parameters associated with the gate's input, the present source, and its previously concealed state. The variety of the tanh function is -1 to 1, however the range of a sigmoid () function's value is 0 to 1.

### 3.5 Radial basis function (RBF) Neural Network

Radial Basis Function within a feed-forward neural network model with exceptional performance and global approximation. RBF has three layers: an input layer, a hidden layer, and an output layer. A node known as RBF units, which is a node representing a Gaussian function, may be found in the hidden layer. The localization function center and width of an RBF neural network are determined by two essential factors. The order of appearance of the data points inside the input area may not be equal when the center and width of the RBF neurons are chosen at random. A typical RBF neural network is a locally weighted network that emphasizes certain portions of the training data set. In training, the hidden layer's "base" is RBF, and the input vector is moved immediately to the hidden space. A proportional weighted average of the hidden unit's output represents what an RBF artificial neural network generates for its output. The connection of the hidden layer space to the output space within an RBF neural network creates a linear mapping relationship around its center node.

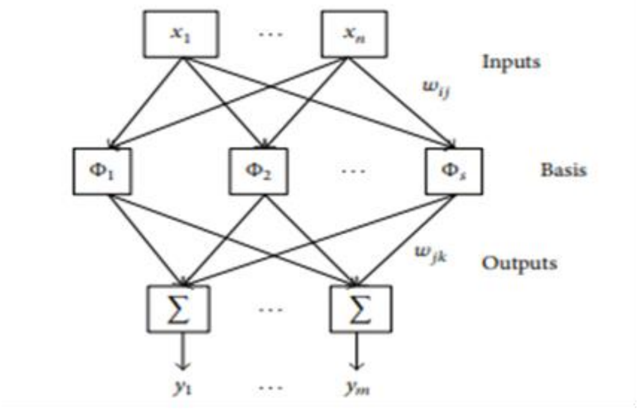

**Fig.5.** Structure of RBF neural network

Among them, the hidden layer's function is to use the kernel function to map the vector in low dimensions to high dimensions, permitting low dimensions that are linearly indivisible to be transferred to larger dimensions and become linearly separable. These are the results of the RBF network:

$$y = \sum_{i=1}^{n} w_i h_i(x) \quad (5)$$

n is the number of hidden layer neurons, Wi is the weight of the connection between the i hidden layer neurons and the i output layer neurons, hi(x) is the activation function of the hidden layer neurons, and the activation function typically takes the form of the Gaussian function, which is defined as follows. Where Wi is the amount of weight of the connection between the i hidden layer neurons and the i neurons in the output layer, n is the number of hidden layer neurons, and y is the output of the RBF neural network.

$$h_i(x) = \exp\left(\frac{1}{2\sigma_i^2}||C - \mu_i||^2\right) \quad (6)$$

The output expression of the radial base network used in this method is as follows, and clustering can be viewed as the process of optimizing neural network output and weights.

### 3.6 Hybrid Model

Creating a hybrid model that combines an LSTM (Long Short-Term Memory) network and a Radial Basis Function Neural Network (RBFNN) is an interesting idea.

The basic idea is to use the LSTM to process sequential data and capture temporal dependencies, while the RBFNN can handle the non-linear relationships and interpolate between data points.

## 4. Data Preprocessing

### 4.1. Dataset

The CICDDoS2019 datasets have been collected by cyber security using Wireshark in modelled scenarios. They consist of two different patterns of use, multiple DoS, and DDoS attacks, in addition to multiple phase’s attacks. The information collected is pre-processed using the CICFlow Metre. It features 88 internet traffic abilities that produce various DDoS and DoS attacks traffic statistics. The data collected from the collection, and saved in CSV format, includes an assortment of traffic elements [18]. We use a network of bots to send an enormous amount of resolved queries to an IP once an individual performs a DNS-based DDoS destruction. In an LDAP-based attack, an attacker makes requests to a compromised server which is available to everyone in order to generate large responses that are subsequently transmitted to the systems being attacked. [20].

This dataset contains a variety of current reflected DDoS attacks, including PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP attacks. Attacks were then carried out during this time.

### 4.2 Data Preprocessing

It is one of the most important procedures before data analysis. In addition to substantial amounts of vital and useful information, raw data also contains a sizable quantity of noise, duplicate values, missing values, inaccuracy, etc. Therefore, it is crucial to improve the quality of the raw data in order to boost the efficacy and simplicity of data analysis. Data pre-processing makes this significantly and successfully possible. The data pre-processing process employs several strategies for various goals. Data cleansing has been employed in this project as a pre-processing step for the data. Data cleaning, also known as data scrubbing or data cleaning, is a processing method used to identify mistakes in raw data, remove duplicates, fill in blanks, or remove erroneous data.

The CICDDoS2019 dataset is in CSV format and includes a huge number of data packets. In order to ensure that the sample is random, the method of random sampling is used while importing the data. Since these columns do not have a numerical value and instead contain infinite, these rows of data are taken out from the dataset. The set of data had been decreased by 17 features with little impact on accuracy [21].

For the purpose of organizing DDoS attacks, the data set has been separated into two groups: benign and attacks. "BENIGN" is assigned the value "0" in the dataset created for recognizing a network attack, while other attacks are set to "1." For classification purposes, the attack methods have been divided into two primary groups: attacks based on exploitation and attacks based on reflection. For purposes of classification, reflection-based attacks, and exploitation-based threats were divided into distinct categories. The data is normalized to bring it into the 0–1 range and sent through the LSTM to obtain restructuring.

## 5. Experimental Results

### 5.1. Model Evaluation

Finally, we evaluate the performance of the proposed hybrid model to detect DDoS attack detection and mitigation models using metrics such as accuracy, precision, recall, and F1 score. We also compare our approach to traditional DDoS detection techniques and other deep learning-based methods to demonstrate the effectiveness of our methodology.

In summary, our proposed methodology leverages deep learning techniques to detect and mitigate DDoS attacks in cloud computing environments. By combining feature extraction, model training, and adaptive mitigation strategies, our approach offers a robust and scalable solution for enhancing cloud security against DDoS attacks.

### 5.2. Performance evaluation Metrics

To successfully assess machine learning and deep learning algorithms, appropriate performance criteria must be chosen. For the objective of this analysis, we used mainly the performance measures precision (P), accuracy (A), recall (R), and F1-score (F1).

$$precision = \frac{True\ positive(Tp)}{True\ positive(Tp) + False\ positive\ (Fp)} \quad (7)$$

$$Recall = \frac{True\ positive(Tp)}{True\ positive(Tp) + False\ Negative\ (Fn)} \quad (8)$$

$$Accuracy = \frac{Tp + TN}{Tp + TN + FP + FN} \quad (9)$$

$$F1\ score = 2 * \frac{Recall * precision}{Recall + precision} \quad (10)$$

In this work, we run the experiment ten times and train our model on the NVIDIA GTX 1060 GPU. We also run our model in google colab. In order to choose the best model during the training stage, we feed the training data into the LSTM module and use 20% of the training data as a verification set.

We implement our model on the CICDDoS2019 Dataset which is separated into two categories: a training segment and a testing segment. The training and test datasets have been used to evaluate both proposed LSTM models. The results of the Random Forest classifier, K-nearest neighbor, SVM Classifier, Ensemble learning, and Proposed Model are shown in Table 1, and their accuracy, precision, recall, and F1 score are examined.

**Table 1.** Evaluation of output parameters of models

| **Model** | **Accuracy** | **Precision** | **Recall** | **F-measure** |
|---|---|---|---|---|
| Random Forest classifier | 0.99808 | 0.99852 | 0.99651 | 0.99772 |
| K-nearest neighbour | 0.99715 | 0.99678 | 0.99665 | 0.99672 |
| SVM Classifier | 0.99371 | 0.99107 | 0.99450 | 0.99792 |
| Ensemble learning | 0.99790 | 0.99812 | 0.99705 | 0.99792 |
| Proposed Model | 0.99947 | 0.99942 | 0.99965 | 0.99953 |

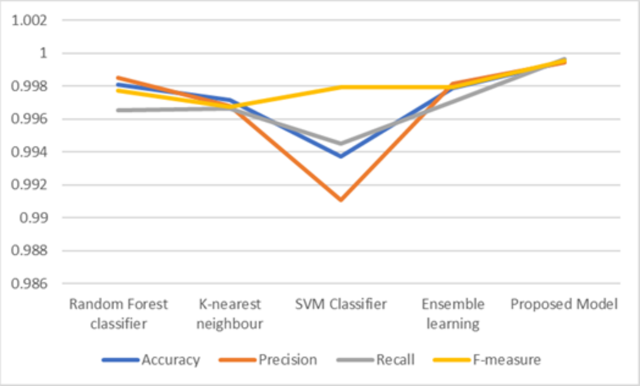

**Fig 6**. Comparison of output metrics of different models

The research study using the proposed LSTM algorithm at a rate of learning of 0.0001 and epoch value 25 provides the highest accuracy, a rate of 98 percent when compared to KNN and DNN. Having efficiency displayed on the y-axis and epoch on the x-axis, Figure 6 shows the connection between training and validation accuracy [23]. The graph illustrates the relationship between accuracy and epoch value, showing the effectiveness associated with the offered method.

The connection between validation and training loss can be seen in the following graph, placing the epoch on the horizontal axis and loss on the vertical one. Graph shows how losses reduce as the epoch number rises, showing the viability of the approach from the point of view of business.

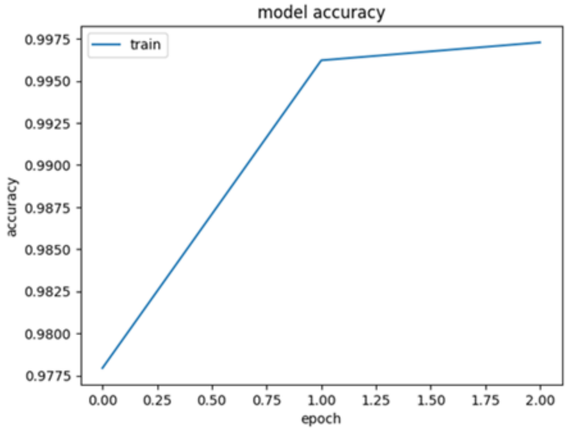

**Fig 7.** Epochs and loss within a plot

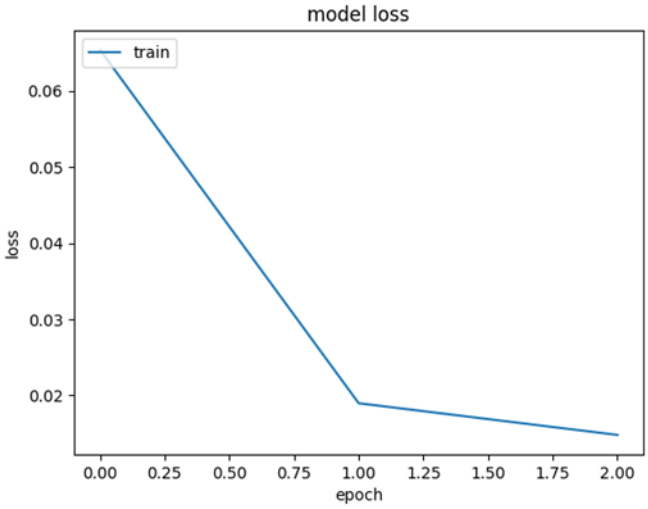

**Fig 8**. Plot combining Epochs and Accuracy

## 5 Conclusion

The successful implementation of our model highlights its potential in improving the security and stability of cloud computing systems by promptly detecting and mitigating DDoS attacks, and minimizing their impact on cloud resources and services. DDoS attacks on networks will be classified using a hybrid deep learning model, which is more effective than a model developed via machine learning. Since the LSTM model includes feature selection and extraction into its model, it is preferred above deep learning techniques as a framework for this research. The Radial basis function (RBF) Neural Network model, a deep learning model used in the present research, was applied to determine the benign and developing categories on the CICDDoS2019 dataset. The accuracy rate for DDoS attacks is approximately 99.95%, which is significantly greater than the accuracy of KNN and other machine learning models. We can apply transfer learning methods to get good results on higher volume of data.

### Conflicts of interest

The authors have no conflicts of interest.

## References

[1] Masdari, M., and Jalali, M.: 'A survey and taxonomy of DoS attacks in cloud computing', Security and Communication Networks, 2016, 9, (16), pp. 3724-3751

[2] Song Wang, Juan Fernando Balarezo, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan, Muhammad Rizwan Asghar, Giovanni Russello, "Detecting flooding DDoS attacks in software defined networks using supervised learning techniques", Engineering Science and Technology, an International Journal, Volume 35,2022,101-176, ISSN 2215-0986,

[3] Rawashdeh, A., Alkasassbeh, M., and Al-Hawawreh, M.: 'An anomaly-based approach for DDoS attack detection in cloud environment', International Journal of Computer Applications in Technology, 2018, 57, (4), pp. 312-324

[4] Wani, A.R., Rana, Q., Saxena, U., and Pandey, N.: 'Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques', in Editor (Ed.)^(Eds.): 'Book Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques' (IEEE, 2019, edn.), pp. 870-875

[5] Idhammad, M., Afdel, K., and Belouch, M.: 'Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest', Security and Communication Networks, 2018, 2018

[6] Hezavehi, S.M., and Rahmani, R.: 'An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments', Cluster Computing, 2020, pp. 1-19

[7] R. K. Gupta et al., "An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large Scale 5G", Wireless Communications and Mobile Computing 2022.

[8] Khuphiran, Panida, et al. "Performance comparison of machine learning models for ddos attacks detection." 2018 22nd International Computer Science and Engineering Conference (ICSEC). IEEE, 2018.

[9] Farnaaz, Nabila, and M. A. Jabbar. "Random forest modeling for network intrusion detection system." Procedia Computer Science 89 (2016): 213-217.

[10] Sahi, A., Lai, D., Li, Y., and Diykh, M.: 'An efficient DDoS TCP flood attack detection and prevention system in a cloud environment', IEEE Access, 2017, 5, pp. 6036-6048

[11] Chen, Z., Jiang, F., Cheng, Y., Gu, X., Liu, W., and Peng, J.: 'XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud', in Editor (Ed.)^(Eds.): 'Book XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud' (IEEE, 2018, edn.), pp. 251-256

[12] Kingma, D. P., & Ba, J. (2015). Adam: a method for stochastic optimization. 3rd International Conference for Learning Representations, San Diego. Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019).

[13] Chollet F., "Keras: Python Deep Learning Library," https://keras.io, Last Visited, 2022. [27] University of New Brunswick. DDoS Evaluation Dataset (CIC-DDoS2019). 2019. Available online: https://www.unb.ca/cic/ datasets/ddos-2019.html (accessed on 20 december 2021).

[14] Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–8

[15] Cheng, J.; Yin, J.; Liu, Y.; Cai, Z.;Wu, C. DDoS attack detection using IP address feature interaction. In Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative Systems, Thessalonika, Greece, 24–26 November 2010; IEEE: Piscataway Township, NJ, USA, 2009; pp. 113–118.

[16] Wang, C.; Zheng, J.; Li, X. Research on DDoS attacks detection based on RDF-SVM. In Proceedings of the 10th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 9–12 October 2017.

[17] Prathyusha, D.J., and Kannayaram, G.: 'A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment', Evolutionary Intelligence, 2020, pp. 1-12

[18] Rabbani, M., Wang, Y.L., Khoshkangini, R., Jelodar, H., Zhao, R., and Hu, P.: 'A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing', Journal of Network and Computer Applications, 2020, 151, pp. 102507

[19] Zareapoor, M., Shamsolmoali, P., and Alam, M.A.: 'Advance DDOS detection and mitigation technique for securing cloud', International Journal of Computational Science and Engineering, 2018, 16, (3), pp. 303-310

[20] Xu, Y., Sun, H., Xiang, F., and Sun, Z.: 'Efficient DDoS Detection Based on K-FKNN in Software Defined Networks', IEEE Access, 2019, 7, pp.

160536-160545

[21] Velliangiri, S., and Pandey, H.M.: ‘Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms’, Future Generation Computer Systems, 2020

[22] Kesavamoorthy, R., and Soundar, K.R.: ‘Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system’, Cluster Computing, 2019, 22, (4), pp. 9469-9476

[23] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, “An ensemble deep learning-based cyber-attack detection in industrial control system,” IEEE Access, vol. 8, pp. 83965–83973, 2020.

[24] Y. Liu, M. Dong, K. Ota, J. Li and J. Wu, "Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks," 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 2018, pp. 1-6, doi: 10.1109/CAMAD.2018.8514971.

[25] Srikanth yadav M., R. Kalpana, “Recurrent nonsymmetric deep auto encoder approach for network intrusion detection system, Measurement: Sensors, Volume 24, 2022, ISSN 2665-9174

[26] G. Oke, G. Loukas and E. Gelenbe, "Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network," 2007 IEEE International Fuzzy Systems Conference, London, UK, 2007, pp. 1-6, doi: 10.1109/FUZZY.2007.4295666.

[27] LV Y, Le Q-T, Bui H-B, Bui X-N, Nguyen H, Nguyen-Thoi T, Dou J, Song X. A Comparative Study of Different Machine Learning Algorithms in Predicting the Content of Ilmenite in Titanium Placer. Applied Sciences. 2020; 10(2):635. https://doi.org/10.3390/app10020.

[28] Singh, C. ., Gangwar, M. ., & Kumar, U. . (2023). Improving Accuracy of Integrated Neuro-Fuzzy Classifier with FCM based Clustering for Diagnosis of Psychiatric Disorder. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 244–248. https://doi.org/10.17762/ijritcc.v11i2s.6143

[29] Hernandez, A., Hughes, W., Silva, D., Pérez, C., & Rodríguez, C. Machine Learning for Predictive Analytics in Engineering Procurement. Kuwait Journal of Machine Learning, 1(2). Retrieved from ttp://kuwaitjournals.com/index.php/kjml/article/view/124