International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Enhancing Cloud Security: A Novel Approach to Intrusion Detection Using Feed Forward Neural Networks and Optimization Algorithm

Dr. N. Rajkumar[1], Dr. S. Megala[2]

[1]Assistant Professor, Department of Computer Science, Manbumigu Puratchi Thalaivar M. G. R. Government Arts & Science College, Kattumannar Koil

[2]Assistant Professor/ Programmer, Department of C. I. S., Annamalai University, Annamalai Nagar

Abstract: ***Cloud network is contributing more research options for researchers. Intrusion detection is an important function that can provide information security to the cloud environment. From the research, an Intrusion detection system (IDS) is one of the key areas involving security issues in the cloud environment. In this research paper, we propose an efficient intrusion detection system based on Feed Forward Neural Network (IFF - NN) along with Ant Lion optimization algorithms. The attacks are identified in the network layer of a cloud environment. The goal of the research is to improve the accuracy and error rate. The experimental results prove with high accuracy for detecting the attack. The proposed approach is executed using KDD99 dataset and compared with existing methods.***

Keywords: Intrusion detection, deep learning, algorithm, cloud computing

1. Introduction

Cloud technology is web - based computing, that involves transferring files virtually. The cloud is also called on - demand computing or utility computing. Simple definition, cloud technology is the delivery of technology services, which includes storage, servers, databases, software, networking, and intelligence over the internet with flexibility, innovation, and scale - up [1]. The different types of cloud techniques, public cloud – the cloud services provider (CSP) initiate the resources through Software as a Service (SaaS) to individual machine and virtual machine (VM) and also bare metal (BM). In the public cloud, the CSR manages all the data, server, and infrastructure to the customers [2]. in a private cloud environment, the customized and individual infrastructure for individual customers. The hybrid cloud is a combination of private and public clouds. Cloud architecture is having two parts. Front and back end. Communication between front and back end is through the internet or any network. The pictorial representation is shown in fig 1.

Front end:

- It can provide the interface and application to access the cloud - based service.
- The front end is user side application. Generally, the browser act as a front - end application.

Back end:

- Responsible and monitoring all the programs' runs in the front end.
- A large number of storage servers and network infrastructure.

The intrusion detection system (IDS) is monitoring the network traffic and for finding any suspicious activity in the network infrastructure. IDS is a type of software application to monitor unwanted activity in the network. The violation activity was reported to an administrator. An intrusion is defined as an attempt to compromise the CIA (Confidentiality, Integrity, and Availability) or to bypass the security mechanisms of a computer or network [3]. The intrusion was triggered by the attackers through the internet to access the cloud environment. The automatic self - adaption and scalability are two lack of features in existing Intrusion Detection systems deployed in cloud environments. The traditional IDS is not suitable for cloud environments [4]. The IDS classification is as follows: Network intrusion detection system (NIDS), host intrusion detection system (HIDS), Protocol - based intrusion detection system (PIDS), Application based intrusion detection system (APIDS), and Hybrid intrusion detection system (HbIDS). Also, the subset of intrusion detection systems is Signature - based and anomaly - based detection systems. We can detect the intrusion in three different layers, network layer, cloud layer, and compute [5]. The IDS plays a vital role in defence system against the attack. The IDS implementation in cloud environment requires a scalable, efficient and virtualization - based approach. In this research paper, we propose the customized IFF - NN approach along with Ant lion Optimization to reduce the error rate.

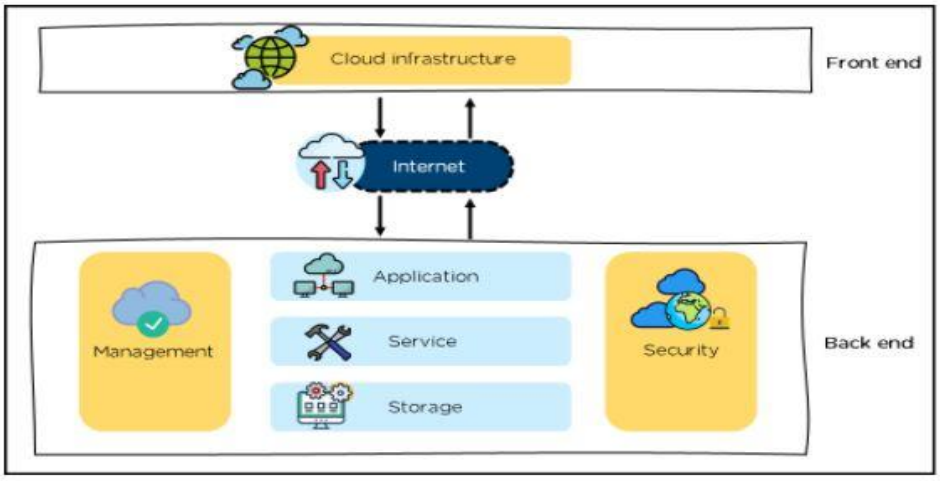

Figure 1: Cloud architecture.

1.1 Contribution of the paper

- The design and implementation of intrusion detection based on FF - NN model. Mostly, the attacks are in the network layer of cloud computing.
- The Ant lion optimization algorithm is used to reduce the error rate.
- The CSE - CIC - IDS2017 dataset is used for analyzing the result with existing methods.

The rest of the paper organizes in the following manner: Section 2 discusses the related work. Section 3 describes the proposed methods. Section 4: result and comparison, Section 5 Conclusion and future work.

2. Related Works

Table 1: Existing methodology

S. No	Paper Name	Author Name	Technique Used	Pros	Cons
1	Anomaly detection and trust authority in artificial intelligence and cloud computing [6]	Kashif NaseerQureshi Gwanggil Jeon Francesco Piccialli	Software - Defined Network - based Anomaly Detection System (SDN - ADS)	Works well in different parameters.	Very few attacks are considered for analyzing the report.
2	A novel intrusion detection system using a hybrid clustering - optimization approach in cloud computing [7]	Jitendra Kumar Samriya, Narander Kumar	Fuzzy - based Artificial Neural Network. Spider monkey algorithm.	High accuracy, Precision, and TP rate.	Low accuracy in very high traffic
3	A deep learning approach for proactive multi - cloud cooperative intrusion detection system [8]	Adel Abusitta, Martine Bellaiche, Michel Dagenais and Talal Halabi	Machine learning - based cooperative IDS. Denoising Autoencoder (DA)	Enhanced cooperative intrusion detection accuracy.	Distribution overhead between nodes is very low.
4	Intrusion detection based on improved density peak clustering for imbalanced data on sensor - cloud systems [9]	Ming Yan Yewang Chen Xiaoliang Hu Dongdong Cheng Yi Chen Jixiang Du	Density peak (Dpeak) clustering. Rotation - DPeak. Oulier detection algorithm.	Effective result in an imbalanced dataset. High accuracy.	Very low accuracy in
5	Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques [10]	Mohamed Idhammad Karim Afdel Mustapha Belouch	Distributed machine learning - based IDS. Time - based sliding window algorithm.	High detection performance.	No real - world implementation
6	Intrusion detection for network - based cloud computing by custom RC - NN and optimization [11]	T. Thilagam R. Aruna	Recurrent Convolutional Neural Network. Ant Lion Optimization.	High accuracy	Attack type not mentioned in the model.
7	A high precision intrusion detection system for network security communication based on a multi - scale convolutional neural network [12]	Jing Yu Xiaojun Ye Hongbo Li	Deep learning techniques. Shortcoming techniques.	High detection accuracy.	Yet to be implemented in the cloud environment.
8	GTM - CSec: Game - theoretic model for cloud security based on IDS and honeypot [13]	Komal SinghGill SharadSaxena AnjuSharma	Honeypot based detection method.	Automatically choose the technique based on the attack. Very less energy consumption.	Energy consumption is high when we give the same variable to all the methods.
9	Intrusion detection for cloud	Bahram Hajimirzaei	Multilayer perception	Efficiency is	No real

	computing using neural networks and artificial bee colony optimization algorithm [14]	Nima JafariNavimipour	network layer. Artificial bee colony algorithm. Fuzzy network.	improved due to three methods.	implementation
10	Artificial Intelligence - based Network Intrusion Detection with hyper - parameter optimization tuning on the realistic cyber dataset CSE - CIC - IDS2018 using cloud computing	V. Kanimozhi T. Prem Jacob	Artificial Intelligence	High accuracy. Low faulty score.	Suitable only for a large data set.

3. Proposed Method

3.1 Intrusion Detection system model with Optimization

The cloud infrastructure stores a large volume of data which leads to a few security issues like availability, integrity, and confidentiality. The intruders and cyber attackers are playing a major part in cloud security. In general, security issues are:

- Physical layer security issue
- Virtualization issue
- Network layer security layer.
- Application - level issue.

We propose a work based on the detection only in the network layer of a cloud computing environment. Hence the cloud data accessed through the web browser, the network layer plays a vital role. Feed forward neural networks are also called deep feed forward networks. A Feed Forward Neural Network (FF - NN) is an artificial neural network in which the connections between nodes do not form a cycle [16]. FF - NN is a simple method in neural networks and the data is processed in one direction. The data may be passed through many hidden nodes but must be in a single direction mentioned in fig.2. In FF - NN method is a simple and also efficient method. The serious of input is entered the layer and multiplied based on the weight. The added value to becomes the output of the input. These methods shown in fig.3. The threshold value is set initially. The value of the output is above the threshold, and then the output value is 0. The sum of the output is less than a threshold, the value is - 1.

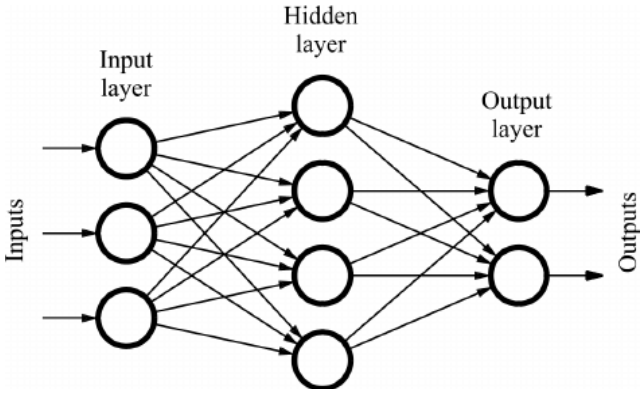

Figure 2: FF - NN Data Direction overview

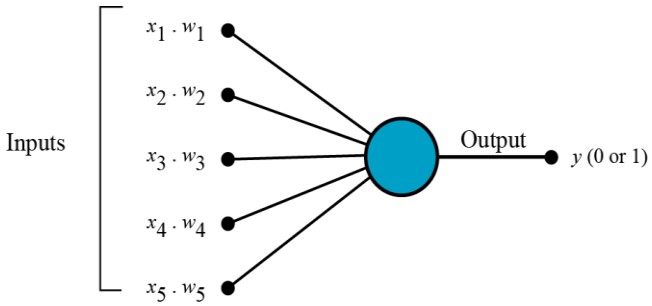

Figure 3: FF - NN Data flow method

3.2 KDD99 Dataset

The KDD dataset was originally invented in the year 1999. From the beginning, the KDD dataset is highly used by the researchers. There are 41 different features in the KDD dataset. It consists of 48.98, 430 dataset which is larger than another dataset.

Category of KDD dataset:

- Basic feature (feature 1 to 9)
- Content feature (feature 10 to 22)
- Time - based traffic feature (feature 23 to 31)
- Host - based traffic feature (feature 32 to 41)

The KDD dataset is used to build the IDS. The disadvantage of KDD dataset is replication is more than another dataset. The fig.4 shows the distribution of KDD 99 train dataset.

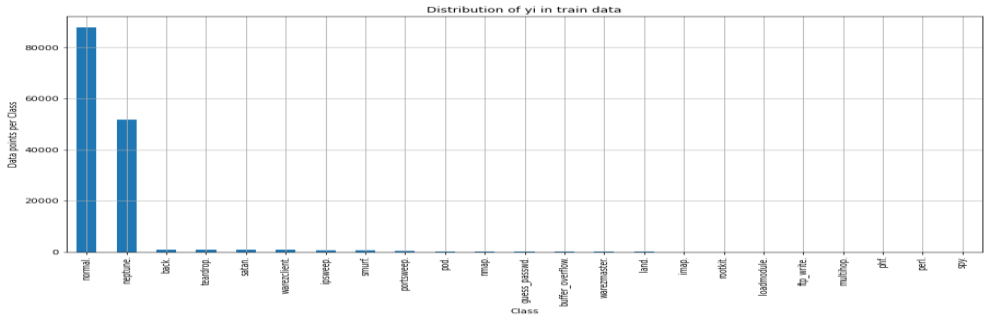

Figure 4: Distribution of KDD train data

3.4 Ant lion Optimization Algorithm

The ant lion optimizer (ALO) was introduced in the year 2015 [18] and inspired the hunting behavior of ant lion. The custom layer is used to declare the variable. The ALO values are declared in a custom layer. The ALO inspired the interaction between ant and ant lion. The Ant lion moves stochastically when searching for food [18]. The equation for random movement is X (t) = [0, cumsum (2r (t1) - 1), cumsum (2r (t2) - 1), …cumsum (2r (tn) - 1))

The advantage of the ant lion algorithm is producing a very less error rate. In every iteration, the intensity of the ants is reduced or decreased, which leads to improving the convergence rate. In addition, the proposed method utilized bilstm architecture hence the data flow in bidirectional. The bilstm methods show in fig.5.

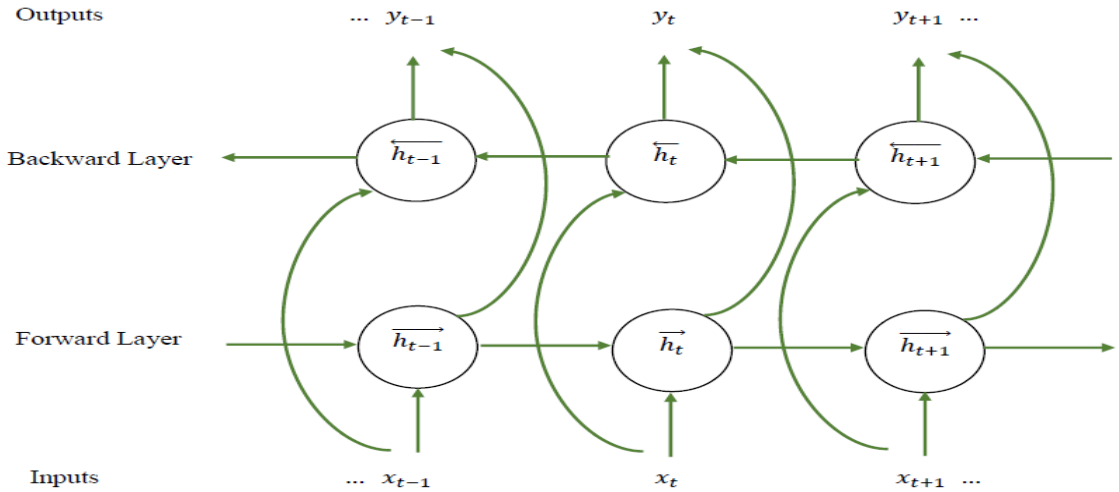

Figure 5: BILSTM architecture

3.5 Algorithm for Proposed FF - NN based IDS model

Input: KDD 99 Dataset
Output: Intrusion types
Function Used:
ALO (N, lb, Max_iter, ub, fobjdim)
func_plot: (func_name)
Get_Functions (F)
initialization (dim, SearchAgents_no, ub, lb)
main. m
Random_walkaround_antlion (lb, Dim, max_iter, ub, current_iter, antlion)
RouletteSelection (weights)

1) Start
2) Initialize the dataset (KDD99)
3) Partition of a dataset (Testing and Training dataset)
4) Creating chart for table
5) Pre - processing the data
6) Convert: Document to Image
7) Create a custom layer for ALO
8) Initialize the parameter
9) threshold value for optimizer is 1
10) Set initial learn vale ($3e^{-4}$)
11) Analysing with FF - NN
12) Classify the attack
13) End

4. Simulation Results

In this paper, the deep learning approach feed forward neural network along with Ant lion optimization algorithm is utilized. The experimental analysis using Python 3.10.1 language.

KDD99 Dataset
The existing data sets affect the performance of the systems. The results are very poor. To solve the issue, a new data set [19] is introduced. The advantage of KDD data sets are as follows:

- No redundant records in the train set, so the classifier will not produce any biased result
- No duplicate record in the test set which has better reduction rates.

- The number of selected records from each difficult level group is inversely proportional to the percentage of records in the original KDD data set.

Attacks in KDD99 Dataset

Classification of KDD99 dataset are followed:

- DoS - Denial of service.
- Probing - Surveillance and other probing attacks.
- U2R - Unauthorized access to local superuser.
- R2L - Unauthorized access from a remote machine.

Table 2: Different attack in data set simulation results

Attacks in Dataset	Attack Type (37)
DoS	Neptune, Back, Land, Pod, Smurf, Processtable, Teardrop, Apache2, Mailbomb, Udpstorm, Worm
Probe	Nmap, Satan, IPsweep, Portsweep, Mscan, Sa int
R2L	Guess_password, Ftp_write, Imap, Phf, Multi hop, Warezmaster, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named
U2R	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps

Fig.6 illustrates the distribution attack in KDD data set. Table 3: shows the parameter used in FF - NN deep learning method. The sequence of data is processed through customized FF - NN deep learning techniques. The input sequence is: the filter size is defined by 1 - by - N and the pooling region is 1 - by - L, where N is ngramsize of the customized layer.

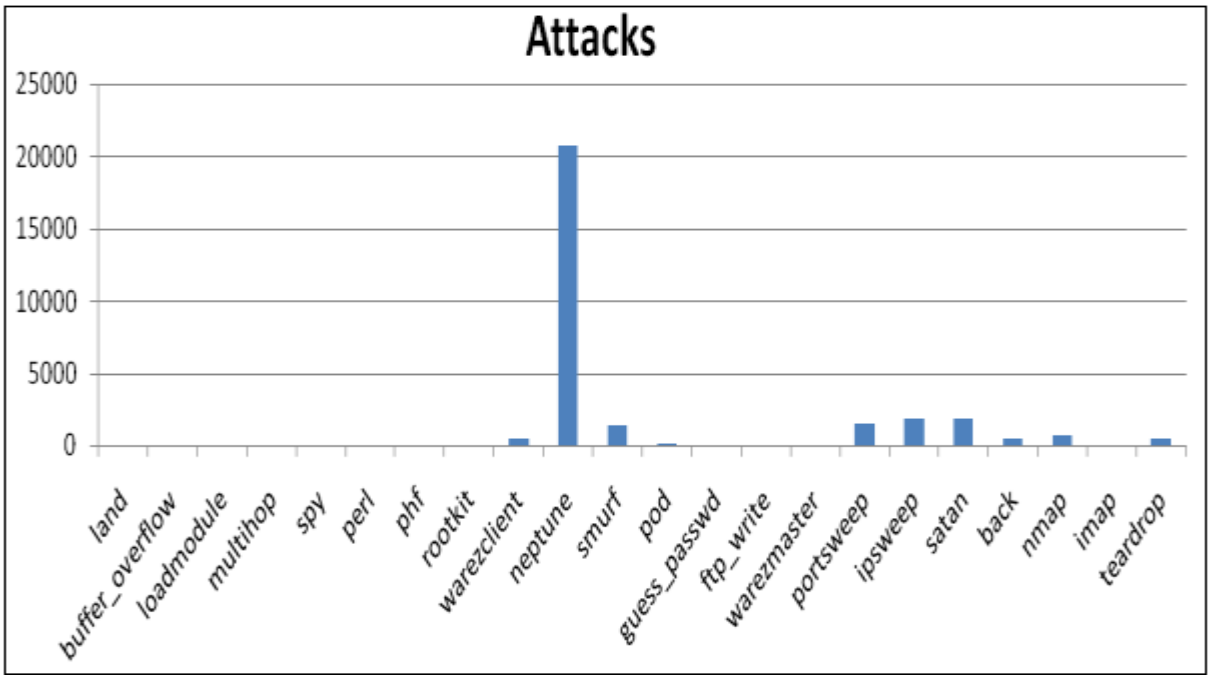

Figure 6: Distribution of attack in KDD

The custom layer is used to connect the filters and sequence of the unfolding layer. The performance evaluation of IDS is based on the confusion matrix [20]. The prediction results of a classifier are presented in the form of a table that separates the correct predictions from incorrect ones for each class. This table is called a confusion matrix [20]. Table 3 shows the confusion matrix used in the proposed model. It has different conditions, such as positive rate, false - positive rate, accuracy, F1score, precision.

Table 3: Confusion Matrix

		Predicted	
		Negative	Positive
Actual	Negative	a	b
	Positive	c	d

The accuracy, Negative rate (NR), and Positive Rate (PR) were calculated using the following formula:

Accuracy: (PC+NC) / (PC+FP)
NR = NC/ (PC+FN)
PR=PC/ (PC+FN)

Where Positive count (PC), Negative count (NC), Negative rate (NR), Positive rate (PR), false positive (FP), and False negative (FN). In fig 7 (a), it is observed, the error rate of the proposed model is very less compared with existing methods like CNN, RC - NN. The accuracy of the algorithm also increased shown in fig 7 (b). from the observation, the accuracy rate is increased by 0.9996 compared to existing methodologies.

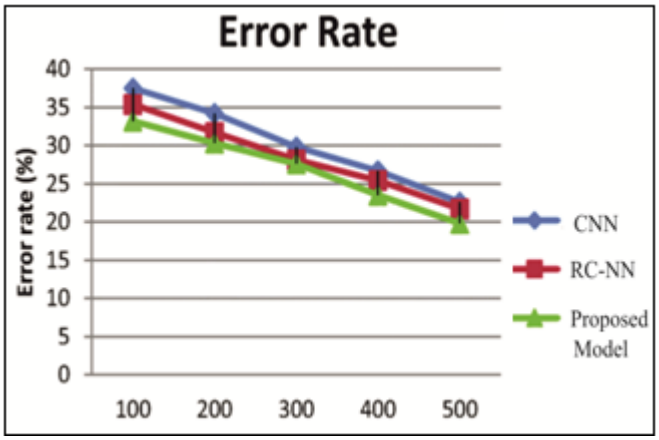

Figure 7: (a) Error rate

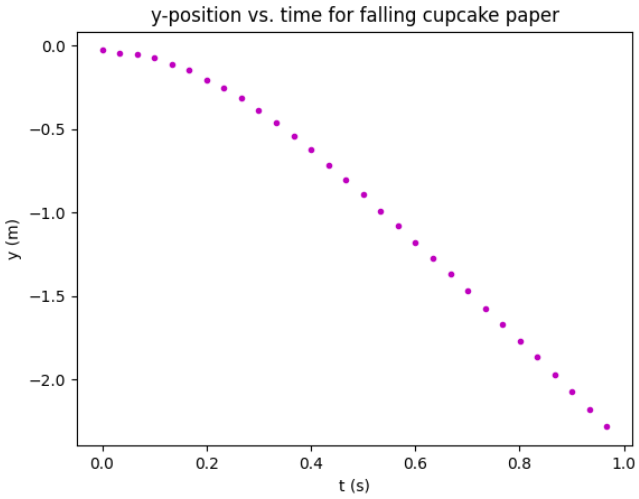

Figure 7 (b): Accuracy

From figure 7 (a), we can conclude the tiny amount of error rate is reduced. From the experimental result, the proposed methodology FF - RR along with Ant lion optimization improves the performance of the network. Table 4 shows the comparative result with other existing methods in terms of accuracy using KDD99 Dataset.

5. Conclusion and Future Work

The Intrusion detection methodology is a type of security provided to the cloud environment. In our research, proposes an FF - NN with an optimization algorithm. From the report, the proposed method is more efficient than existing methods in terms of accuracy and error rate. The proposed method shows the outperforms result in NP and PR. The FF - NN based method can easily detect any attack. We used KDD99 dataset for simulation and ant lion optimization for improving the accuracy. In the future, the work extends to improving precision and network management.

Table 4: Comparison table

Parameters	CNN	RC - NN	Proposed FF - NN with ALO
Accuracy	0.5807	0.9401	0.999
NR	0.9	0.84	0.82
PR	0.0685	0.053	0.0498

References

[1] What is cloud computing? A beginner's guide | Microsoft Azure.
[2] What is Cloud Computing? - India | IBM.
[3] R. Bace, P. Mell, "Intrusion Detection Systems", National Institute of Standards and Technology (NIST), Technical Report, 800 - 31, 2001.
[4] A. Patel, M. Taghavi, K. Bakhtiyari, J. C. Ju´nior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview", Journal of Network and Computer Applications 36 (2013), pp.25–41.
[5] Best Intrusion Detection Techniques In Cloud Computing (uptycs. com).
[6] Kashif Naseer Qureshi, Gwanggil Jeon, Francesco Piccialli, " Anomaly detection and trust authority in artificial intelligence and cloud computing", Computer Networks, Volume 184, 15 January 2021, 107647.
[7] Jitendra Kumar Samriya, Narander Kumar, A novel intrusion detection system using hybrid clustering - optimization approach in cloud computing, Material today.
[8] Adel Abusitta, Martine Bellaiche, Michel Dagenais and Talal Halabi, " A Deep Learning Approach for Proactive Multi - Cloud Cooperative Intrusion Detection System", Future Generation Computer Systems.
[9] Ming Yan, Yewang Chen, Xiaoliang Hu, Dongdong Cheng, Yi Chen, Jixiang Du, " Intrusion detection based on improved density peak clustering for imbalanced data on sensor - cloud systems", Journal of systems Architecture 118 (2021) 102212.
[10] Mohamed Idhammad, Karim Afdel, Mustapha Belouch, " Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques", Procedia Computer Science, Volume 127, 2018, Pages 35 - 41.
[11] T. Thilagam, R. Aruna, " Intrusion detection for network based cloud computing by custom RC - NN and optimization, The Korean Institute of Communications and Information Sciences.
[12] Jing Yu, Xiaojun Ye, Hongbo Li, "A high precision intrusion detection system for network security communication based on multi - scale convolutional neural network", Future Generation Computer Systems, Volume 129, April 2022, Pages 399 - 406
[13] Komal Singh Gill, SharadSaxena, AnjuSharma, " GTM - CSec: Game theoretic model for cloud security based on IDS and honeypot", Computers & Security, Volume 92, May 2020, 101732.
[14] Bahram Hajimirzaei, Nima Jafari Navimipour, " Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm", ICT Express, Volume 5, Issue 1, March 2019, Pages 56 - 59.
[15] V. Kanimozhi, T. PremJacob, "Artificial Intelligence based Network Intrusion Detection with hyper - parameter optimization tuning on the realistic cyber dataset CSE - CIC - IDS2018 using cloud computing", ICT Express, Volume 5, Issue 3, September 2019, Pages 211 - 214.
[16] Feed Forward Neural Network Definition | DeepAI

[17] Guide to Feed - Forward Network using Pytorch with MNIST Dataset - (analyticsindiamag. com)
[18] Seyedali Mirjalili, "Ant lion Optimizer", Advances in Engineering Software, Volume 83, May 2015, Pages 80 - 98.
[19] "Nsl - kdd data set for network - based intrusion detection systems. " Available on: http: //nsl. cs. unb. ca/KDD/NSLKDD. html, March 2009.
[20] Amna Rahman, Usman Qamar, A Bayesian classifiers based combination model for automatic text classification, in: 2016 7th IEEE International Conference on Software Engineering and Service Science, ICSESS, IEEE, 2016, pp.63–67.