PERFORMANCE ANALYSIS OF MACHINE LEARNING CLASSIFIERS FOR INTRUSION DETECTION USING UNSW-NB15 DATASET

Geeta Kocher[1] and Gulshan Kumar[2]

[1]Research Scholar, Department of Computational Sciences,
MRSPTU, Bathinda, Punjab, India
[2]Assosiate Professor, Department of Computer Applications, SBSSTC,
Ferozpur, Punjab, India

ABSTRACT

With the advancement of internet technology, the numbers of threats are also rising exponentially. To reduce the impact of these threats, researchers have proposed many solutions for intrusion detection. In the literature, various machine learning classifiers are trained on older datasets for intrusion detection which limits their detection accuracy. So, there is a need to train the machine learning classifiers on latest dataset. In this paper, UNSW-NB15, the latest dataset is used to train machine learning classifiers. On the basis of theoretical analysis, taxonomy is proposed in terms of lazy and eager learners. From this proposed taxonomy, K-Nearest Neighbors (KNN), Stochastic Gradient Descent (SGD), Decision Tree (DT), Random Forest (RF), Logistic Regression (LR) and Naïve Bayes (NB) classifiers are selected for training. The performance of these classifiers is tested in terms of Accuracy, Mean Squared Error (MSE), Precision, Recall, F1-Score, True Positive Rate (TPR) and False Positive Rate (FPR) on UNSW-NB15 dataset and comparative analysis of these machine learning classifiers is carried out. The experimental results show that RF classifier outperforms other classifiers.

KEYWORDS

Intrusion Detection System, Random Forest, KNN, UNSW-NB15, Machine Learning Classifiers

1. INTRODUCTION

Nowadays, to secure the confidential data from the eye of attackers is becoming a crucial and difficult task. The traditional methods like firewall and antivirus are not sufficient to tackle all types of attacks. So, there is a need for additional security along with traditional methods. Intrusion Detection System (IDS) play a significant role in this regard. It carefully keeps a track on the network traffic data and distinguishes whether the data is normal or attack.

An IDS is used to monitor the network traffic for detecting malicious activity. It can easily detect the attacks that are bypassed by the firewall. It continuously monitors the network, finds vulnerable parts of the network and communicates the administrator about intrusions [1]. It can be separated into two classes: anomaly detection and misuse detection. Misuse detection operates with prior prepared patterns of known attacks also called signatures [2]. It has high accuracy and low false alarm rates (FAR) but unable to detect novel attacks [3]. One of the solutions to address this problem is to regularly update the database which is not feasible and a costly process. So, anomaly detection techniques came into existence. Anomaly Detection deals with profiling user

David C. Wyld et al. (Eds): SIGI, CSTY, AI - 2020
pp. 31-40, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.102004

behaviour [4]. In this approach, a certain model of user normal activity is defined, and any deviation from this model is known as anomalous. Fig. 1 shows the diagram of IDS.

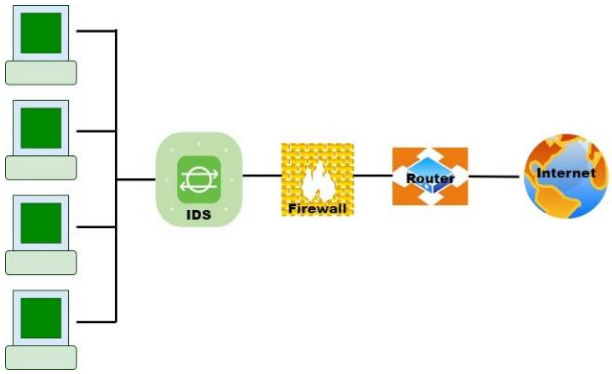

Fig 1: Intrusion Detection System

In literature, different types of machine learning (ML) classifiers are used for intrusion detection. From the literature, it is found that there is limited work done on comparative analysis of ML classifiers. Hence, the motive of this paper is to find performance comparison of several ML classifiers using recent dataset for intrusion detection. The structure of the paper is divided into seven sections. Section 2 gives a brief literature survey related to this research work. In section 3, taxonomy of the classifiers is discussed. A brief introduction about the dataset used for experimental work is described in Section 4. In Section 5, a methodology to pre-process the dataset is presented. Experimental work is shown in Section 6 and Section 7 gives Conclusion and Future scope.

2. RELATED WORK

This section provides the literature survey on the ML classifiers. The main motive of this section is to give an overview of the research work done in the field of intrusion detection. It is found from the literature that researchers have put a lot of efforts on ML classifiers and some of their contributions are described below:

Narudin et. al. (2014) [5] described an evaluation using ML classifiers namely RF, J-48, Multilayer Perceptron (MLP), NB and KNN to detect mobile malware using two datasets namely MalGenome and Private. Weka Tool was used for the evaluation. The performance metrics namely TPR, FPR, precision, recall and f-measure were used to validate the performance of ML classifiers. The accuracy obtained by RF Classifier is 99.99% during experimental work on MalGenome dataset. The author has suggested to improve the results by using selected features for future work.

Belavagi & Muniyal, (2016) [6] designed a Network Intrusion Detection System (NIDS) with the various supervised machine learning classifiers. NSL-KDD dataset was used to check the performance of various classifiers. The result shows that RF classifier outperforms other classifiers. It results in lowest FPR and a highest TPR and accuracy obtained is 99%. But still, there is a need for classifiers that can be used for the multiclass classification.

Ashfaq et al, (2017) [7] described a semi-supervised learning (SSL) approach based on novel fuzziness. In order to improve the classifier performance, it utilizes unlabelled samples along with a supervised learning algorithm. NSL-KDD dataset was used for evaluation of this model.

The limitation of this model was that its performance was studied only for the Binary classification task.

Yaseen et al, (2017) [8] described a multilevel hybrid intrusion detection model using Support Vector Machine (SVM) and Extreme Learning Machine (EVM). The evaluation was done on KDD 99 dataset. The accuracy obtained was 95.75% and shorter training time in this proposed model. This technique is better only for known attacks and for novel attacks, efficient classifiers are required.

Aljumah, (2017) [9] described a trained algorithm to detect DDoS attacks which was based on Artificial Neural Network (ANN). ANN shows 92% accuracy when it was trained with older data sets and when the system is trained with updated datasets, the accuracy obtained was 98%. The accuracy of the ANN model depends upon the dataset. So, there is a need for the up-to-date and balanced dataset.

Roshan et al., (2018) [10] discussed an adaptive design of IDS based on Extreme Learning Machines (ELM). The NSL-KDD dataset was applied for the evaluation. It was found that it can detect novel attacks along with known attacks with an acceptable rate of detection and false positives.

Ali et al., (2018) [11] proposed a PSO-FLN classifier for intrusion detection. The benchmark dataset KDD99 was used to validate the results. PSO-FLN has outperformed ELM and FLN classifiers in terms of accuracy. But for some classes like R2L, it does not show accurate results.
From the literature survey, it is concluded that most of the researches have been validated using older datasets. These datasets lack novel attacks and contains imbalanced network audit data. Non-uniform distribution of data may lead to biased training of ML classifiers and this problem needs to be resolved. The new dataset can be used to detect novel attacks. The RF classifier shows better results as compared to other classifiers. A lot of work is done on binary classification and still there is a need to work more on multi-classification.

3. TAXONOMY OF CLASSIFIERS

The classifiers are divided into two learning methods i.e. lazy learners and eager learners [12-15]. The taxonomy of classifiers is proposed based on theoretical analysis and is shown in Fig. 2.

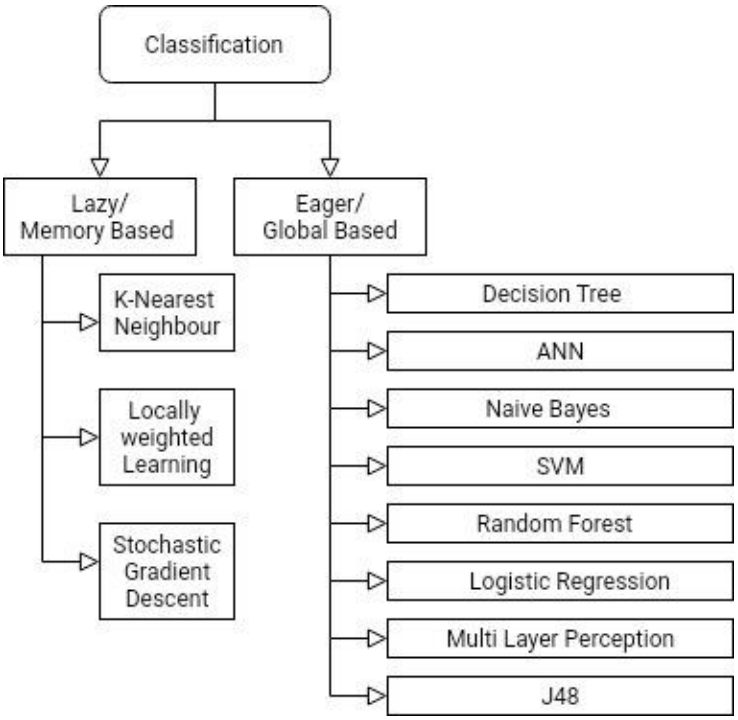

Fig 2: Taxonomy of classifier

The lazy learners can store examples and solve multiple problems with these examples. These learners adapt automatically to changes in the problem domain and easy to maintain. But the limitation of these learners is that they stored the same kind of examples many times and due to this require high memory and time-consuming learners. Eager learners firstly build a classification model on given training data and then perform a classification. These learners take more time for learning and less time for classifying the data.

From the above taxonomy of classifiers, KNN, SGD, DT, NB, RF and LR are used for experimental work in this paper. The description of these classifiers which are explored for experimental work is given below:

3.1. Lazy Learners

These learners use the training data for storage and wait for testing data to appear. KNN, Locally weighted learning (LWL) and SGD are examples of Lazy learners.

3.1.1. K- Nearest Neighbour

It is a lazy learning algorithm that firstly stores all the training data. At the time of classification, it uses this data and tries to find the similarities between the new data and the available data. It places the new data in the category that is most similar to the available data. It is based on the Euclidean distance [16]. The test data is allotted to the class of its K nearest neighbours. As you increase the value of K, accuracy might increase. It can be used for both regression and classification but is often used for classification problems.

3.2. Eager Learners

Eager learners take a long time for training and less time for predicting. DT, NB, LR, SVM, RF, MLP and J48 are examples of eager learners.

3.2.1. Decision Tree

It is a popular and powerful tool for prediction and classification. The structure of DT is like a tree structure in which each internal node represents a test on an attribute, each branch interprets a result of the test, and each leaf node shows a class label. DT perform classification without requiring much computation and able to handle both categorical and continuous features. This tree structure is computationally expensive to train and shows errors in multi-classification problems [17].

3.2.2. Logistic Regression

It is applied to solve both binary class and multiclass classification problems. The probability of occurrence of an event is predicted by giving fitting data to Logistic function. The output of this function lies between 0 and 1. The middle value i.e. 0.5 is considered as the threshold between class 1 and class 0. The output greater than 0.5 is considered as class 1 and if output is below 0.5, then it is considered as class 0[6].

3.2.3. Random Forest

It is proposed by Breiman in 2001. This method is based on the proximity search and can be used both for regression and classification. It is a decision tree-based classifier. In this technique, random samples are used to create decision trees, and then prediction is done from each tree and the best solution is found out by voting [16]. Random forest has many applications like image classification, feature selection and recommendation engines.

3.2.4. Naive Bayes

It is a classification algorithm used both for two class and multi-class classification problems. It assumes that probabilities of every feature belonging to each class are used for prediction [6]. It also assumes that the probability of every feature belonging to a given class value is independent from other features. For the known value of the feature, probability is known as conditional probabilities. Prediction can be attained by calculating the instance probabilities of each class and by selecting the class value of highest probability [12].

4. DATASET USED

The benchmark datasets used in the literature are older datasets and contains repeated records due to which ML classifiers give unfair results. So, selected ML classifiers are tested using UNSW-NB15 dataset which is novel dataset [18]. This dataset is composed of 49 attributes including a class label and contains 25,40,044 labelled instances, each being labelled either normal or attack. A detailed description about the features is given in Table 1.Table 2 gives the details of attacks.

Table 1: Description of the attributes of UNSW-NB15 dataset

S.No.	Type of attributes	Name of attributes	Sequence No.
1	Flow	Script, Sport, Dstip. Dsport, Proto	1-5
2	Basic	State, Dur, Sbytes, Dbytes, Sttl, Dttl, Sloss, Dloss, Service, Sload, Dload, Spkts, Dpkts	6-18
3	Content	Swin, Dwin, Stepb, Dtcpb, Smeansz, Dmeansz, trans_depth, res_bdy_len	19-26
4	Time	Sjit, Djit, Stime , Ltime, Sintpkt, Dintpkt, Tcprtt, Synack, Ackdat	27-35
5	General Purpose	is_sm_ips_ports, ct_state_ttl, ct_flw_http_mthd,is_ftp_login, ct_ftp_cmd	36-40
6	Connection	ct_srv_src , ct_srv_dst , ct_dst_ltm, ct_src_ ltm ,ct_src_dport_ltm,ct_dst_sport_ltm,ct_dst_src_ltm	41-47
7	Labelled	attack_cat, Label	48-49

When UNSW-NB15 dataset is used for evaluation, out of 49 attributes, we got 45 attributesonly. The four ID attributes are combined together to make a single attribute as ID from flow attribute category and two attributes of time category (Stime and Ltime) are combined together in one attribute known as Rate. The 42 attributes of UNSW-NB15 dataset are used to carry out experiment on ML classifiers. The dropout attributes are ID, Duration and attack_cat.

Table 2: Types of attacks in dataset

Type	**Whole**	**Training**
	No. of Records	**No. of Records**
Normal	2218761	56000
Fuzzers	24246	18184
Analysis	2677	2000
Backdoors	2329	1746
DOS	16353	12264
Exploits	44525	33393
Generic	215481	40000
Reconnaissance	13987	10491
ShellCode	1511	1133
Worms	174	130
		175341

5. METHODOLOGY

The pre-processing steps are shown in Fig.3 and Fig. 4 shows methodology used. In pre-processing, first of all the null values present in the dataset are handled. The categorical data is converted into numerical form with the help of label encoder. Then one hot encoder is used to break the relation between the values obtained through label encoder.

After this, the pre-processed data is separated as training and testing. The KNN, LR, NB, SGD, DT and RF classifiers are used to construct the models. Then the prediction of labels of test data is done using these models. A comparison is carried out between actual labels and predicted labels. The performance metrics used to evaluate the models are accuracy, precision, mean square error, recall, f1-score, TPR and FPR.

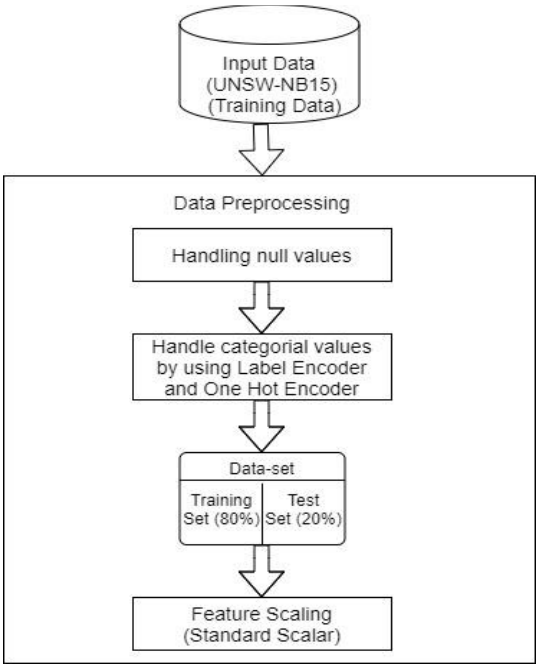

Fig. 3 Pre-processing steps on the UNSW-NB15 dataset

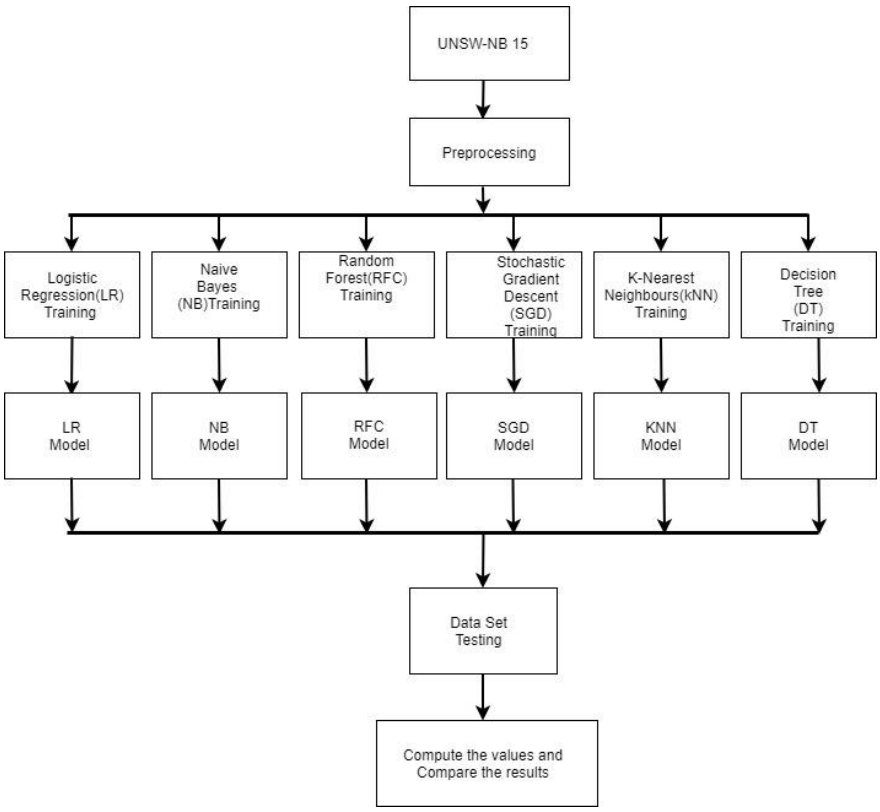

Fig. 4 Methodology

The procedural steps to construct the models are given below:

1. Start with pre-processing of dataset.
2. Divide dataset in to two parts i.e. training and testing.
3. Construct the classifier model using training data for KNN, LR, NB, RF, SGD and DT.
4. Take the test data
5. Testing of classifier models using training data
6. Calculate and compare Accuracy, Recall, Precision, F1-Score and Mean Squared Error for the selected models.

6. EXPERIMENTAL WORK

The selected ML classifiers namely LR, NB, RF, SGD, KNN and DT are tested on UNSW-NB15 dataset, the novel dataset for intrusion detection. The experimental work is done on Intel Core (TM) i3-1005G1 CPU @1.20 GHz, 4GB RAM using Python. After performing pre-processing steps, dataset is divided into two parts: training and testing. Then six classifiers are used for training as shown in Fig. 4 and performance is evaluated on the basis of several parameters as shown in Table 3. Fig. 5 shows the pictorial representation of accuracy of selected classifiers.

It can be observed from the results shown in Table 3 that the RF classifier out performs the other methods in terms of accuracy 95.43%, FPR 0.08 and mean squared error 0.046 whereas the NB shows the highest mean squared error 0.519 and lowest accuracy 48.03% in the selected group of classifiers.

Table 3: Performance comparison of selected classifiers using UNSW-NB15 dataset with train test split method

Classifier	Accuracy	Precision	Recall	F1-Score	Mean Squared Error	TPR	FPR
LR	93.23	0.92	0.99	0.95	0.068	0.99	0.19
NB	48.03	1.00	0.23	0.38	0.519	0.23	0
RF	95.43	0.96	0.97	0.97	0.046	0.97	0.08
SGD	93.29	0.91	1.00	0.95	0.067	0.99	0.21
KNN	93.71	0.94	0.96	0.95	0.063	0.96	0.12
DT	94.20	0.93	0.98	0.96	0.058	0.98	0.14

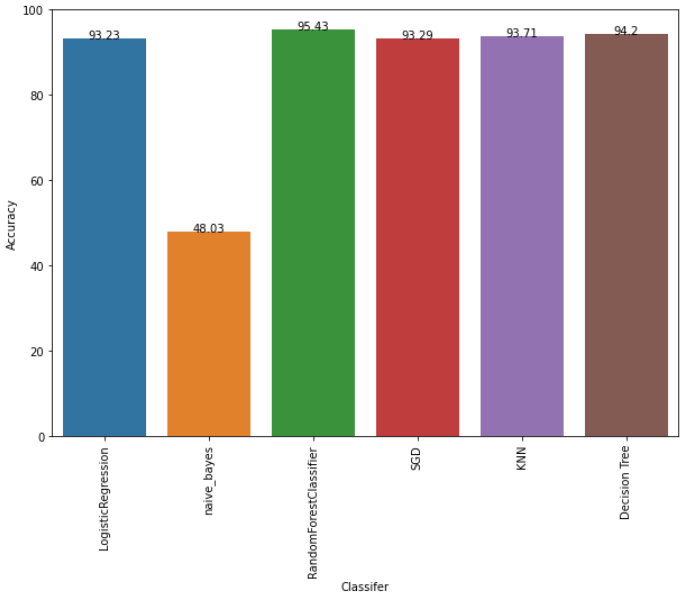

Fig. 5: Accuracy of selected classifiers using UNSW-NB15 dataset with train test Split method

7. CONCLUSION AND FUTURE SCOPE

The taxonomy of classifiers is proposed in terms of lazy and eager learners. The experimental work has been carried out to evaluate the performance of the selected ML classifiers based on proposed taxonomy namely KNN, LR, NB, DT, SGD and RF for detection of intrusion. These classifiers are tested on UNSW-NB15 data-set. The classifiers are compared on the basis of precision, MSE, recall, F1-Score, accuracy, TPR and FPR. The results show that RF classifier is better than other classifiers on UNSW-dataset using selected parameters. The accuracy of RF classifier comes out to be 95.43%. In future, this work can be extended for selective attributes and multiclass classification for detection of intrusion.

REFERENCES

1. Sarmah, A. (2001). Intrusion detection systems: Definition, need and challenges.
2. Omer, K. A. A., & Awn, F. A. (2015). Performance Evaluation of Intrusion Detection Systems using ANN. *Egyptian Computer Science Journal*, *39*(4).
3. Diro, A. A., &Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761-768.
4. Khan, J. A., & Jain, N. (2016). A survey on intrusion detection systems and classification techniques. *Int. J. Sci. Res. Sci., Eng. Technol.*, *2*(5), 202-208.
5. Narudin, F. A., Feizollah, A., Anuar, N. B., &Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*, *20*(1), 343-357.
6. Belavagi, M. C., &Muniyal, B. (2016). Performance evaluation of supervised machine learning algorithms for intrusion detection. *Procedia Computer Science*, *89*, 117-123.
7. Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484-497.
8. Al-Yaseen, W. L., Othman, Z. A., &Nazri, M. Z. A. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. *Expert Systems with Applications*, *67*, 296-303.
9. Aljumah, A. (2017). Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *8*(8).

10. Roshan, S., Miche, Y., Akusok, A., & Lendasse, A. (2018). Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines. *Journal of the Franklin Institute*, *355*(4), 1752-1779.
11. Ali, M. H., Al Mohammed, B. A. D., Ismail, A., &Zolkipli, M. F. (2018). A new intrusion detection system based on Fast Learning Network and Particle swarm optimization. *IEEE Access*, *6*, 20255-20261.
12. Bhavani, D.D., Vasavi, A. & Keshava P.T. (2016). Machine Learning: A Critical Review of Classification Techniques. IJARCCE, 5(3), 22-28.
13. Wei, C. C. (2015). Comparing lazy and eager learning models for water level forecasting in river-reservoir basins of inundation regions. Environmental Modelling & Software, 63, 137-155.
14. Rafatirad, S., & Heidari, M. (2018). An Exhaustive Analysis of Lazy vs. Eager Learning Methods for Real-Estate Property Investment.
15. https://towardsdatascience.com/machine-learning-classifiers-a5cc4e1b0623
16. Narudin, F. A., Feizollah, A., Anuar, N. B., &Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. Soft Computing, 20(1), 343-357.
17. https://www.geeksforgeeks.org/decision-tree/
18. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), 18-31

AUTHORS

Ms. Geeta Kocher

She is MCA, M.Tech, M.Phil. She is pursuing Ph.D in the field of Artificial Intelligence-Deep learning. She has published more than 15 papers in various conferences and journals. She has more than 16 years experience in teaching.

Dr.Gulshan Kumar

Dr. Gulshan Kumar has received his MCA degree from Guru Nanak Dev University Amritsar (Punjab) India in 2001, and M.Tech. Degree in Computer Science & Engineering from JRN Rajasthan Vidyapeeth Deemed University, Udaipur (Rajasthan)-India, in 2009. He got his Ph.D. from Punjab Technical University, Jalandhar (Punjab)-India. He has 17 year of teaching experience. He has 56 international and national publications to his name. Currently, he is working as Associate Professor in Computer Applications department at Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab)-India. He has supervised 06 M. Tech. students for their final thesis, students for projects MCA and supervising 02 PhD research scholar. His current research interests involve Artificial Intelligence, Network Security, Machine Learning and Databases.