ISSN 2278-3091
Volume 8, No.1.2, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse0981.22019.pdf
https://doi.org/10.30534/ijatcse/2019/0981.22019

Design of a Hybrid Logic Based Adaboost Decision Tree Model for Identifying Web Attacks

K.Gowsic[1], V.Manikandan[2], Ashish Sharma[3], M.Sivaram[4], V.Porkodi[5]
[1]Associate Professor, Department of Information Technology,
KSR Institute for Engineering and Technology, Tiruchengode
kgowsic@gmail.com
[2, 3, 4,] Assistant Professor, Department of Computer Network,Lebanese French University, Erbil, KR-Iraq
v.manikandan@lfu.edu.krd, ashish.sharma@lfu.edu.krd, sivaram.murugan@lfu.edu.krd
[5] Assistant Professor, Department of Information Technology, Lebanese French University, Erbil, KR-Iraq
porkodi.sivaram@lfu.edu.krd

ABSTRACT

The foremost development in the volume and significance of web communication through the internet has enlarged the necessity of better security protction. The experts in providing security, while protecting the system maintains a record with containing marks of huge amount of support in recognizing attack revealing. Moreover, this limits the system capability as it can identify only the known attacks that are present in the database, in order to overcome this crisis, ensemble classifier to identify unknown attacks in the internet is proposed. This intrusion detection process involves elimination of redundant and irrelevant features using wrapper based and filter based approach. A hybrid Logic based Adaboost Decision tree model is employed here. The anticipated ensemble classifier was utilized in the online available NSL-KDD dataset which is an improved version of KDD cup dataset from 1999. The experimental outcomes demonstrates that the proposed method shows better trade off than the existing methods in terms of accuracy by 88.12 % in detecting the attacks than the traditional methods, while considering low false rejection rates. This proposed method is simulated in MATLAB environment to compute the accuracy.

Key words: Anomaly detection, intrusion detection, Logit based Adaboost, classification, attacks, Decision Tree

1. INTRODUCTION

Wireless Sensor network is a network which is spatially allotted self-reliant sensors who co-operatively far its records to the sizeable area recognized so wretched rank [1-4]. In WSN, nodes fore its data together with wide variety of hops (multiple hops) according to its bad grade to decrease limit bad or after extend the batteries existence as like the control wished in accordance with dispose facts amongst twins nodes is without delay proportional in accordance with scale among the nodes [2]. As the WSN are deployed in far flung locations where human can't reach yet if as soon as deployed, theirs batteries are sturdy in imitation of replace, accordingly it turns in accordance with be an extremely difficult undertaking after construct a battery powered community as execute stand scalable yet namely properly has lengthy existence span. Subsequent assignment over WSN is the wireless habit on communication. As the sensed facts propagate through wireless trough within the structure of radio frequencies, that turns in conformity with keep vital for network governor after protect network statistics out of intruders then attackers. Execution of various protection algorithms certain as like encryption, authentication, jamming detection alongside together with limit supply is a big element of WSN [21, 26].

WSN workshop in an surroundings where like is no consumer intervention and lesser consumer intervention then so is a node capturing risk, therefore it is essential because of sensor nodes in conformity with identify some assaults yet according to absorb corrective moves over its own in imitation of avert attackers beyond draining the complete lifespan about battery [5-9].All legitimate node resources turns to busy state while replying to receiving data packets or authentication packets from attackers thereby making the battery to drain soon. Distributed deniel of service is similar as that of DoS but more than one attacker is involved and cause severe attack. In this investigation, both the insider and the outsider attacks are handled using effectual feature selection and a hybrid classifier model to compute accuracy effectually [16-20].

The reminder of the work is structured as follows: Section II shows the state of the art of existing work that deals with handling the attacks and the related solutions to them [10]. Section III explains about the proposed work that includes selection of dataset (NSL-KDD dataset), followed by feature selection and the design of hybrid classifier to identify both the insider and the outsider attack. Section IV shows the numerical outcomes and discussion of the anticipated work. Section V illustrates the conclusion with the future direction of the work.

2. RELATED WORKS

Priyanka Gulati et al, depicts that every node being an autonomous substance in VANETs can be effectively imperilled by an adversary. Thus, security is a critical issue. Cryptographic methods can't give protection against obscure attacks so an Intrusion Detection framework dependent evolutionary optimized gradient boosted trees has been proposed to combat flooding attack in VANET [11-15]. The anticipated model can identify various malicious nodes with higher accuracy (99.8%) in contrast with existing models. With evolutionary optimization, number of features is decreased to making our model progressively effectual.

In, Longjie Li et al, motivated the success of Gini index and GBDT calculation in different fields, this paper anticipated GINIGBDT-PSO strategy, a novel hybrid intrusion detection model to improve the execution of network intrusion detection frameworks. The anticipated model first concentrates the ideal subset of features from entire dataset by utilizing Gini index. At that point, GBDT algorithm, which is gradient boosting approach, is embraced to identify unusual connections. Likewise, PSO algorithm is utilized to advance parameters of the GBDT algorithm in the anticipated model. This model cannot just upgrade the general execution for network intrusion detection viably yet additionally improve the identification execution for each kind of attack [24].

A simple over-fitting dealing with is utilized in imitation of enhance education results [25]. In the specific occasion of network intrusion detection, the writer uses preliminary weights in imitation of fulfill the trade-off among discovery and forged menace rates. The empiric results display so much the proposed algorithm has paltry false-alarm dimensions along high detection rate, and the conduct velocity about algorithm is faster into study platform contrasted with distributed run speeds concerning prevailing algorithms

3. INTRUSION DETECTION

An intrusion detection system (IDS) is utilized to identify and to produce some alert when intrusion activity is tried onto the network or system. An intrusion detection strategy may generate certain actions to take further alert while some malicious activity happens in the network. If essential deviation from normal behaviour happens, IDS generates an alarm. The approach can identify new kinds of attack however it is complex to generate precise normal profile [22]. Another approach which merge misuse and anomaly detection approaches is termed as specification based detection. This approach is sourced on manually generated specification. Both specification and anomaly based detection techniques identify an attack using deviation from normal profile [23].

4. PROPOSED METHODOLOGY

In this section, a detailed description of the proposed work is given. Initially, a network database known as NSL-KDD dataset for identifying the intrusion in the internet servers is explained in section V. Secondly, Gini index is considered for recognizing the features that are essential for detecting the attack. Thirdly, Logict based Adaboost model with Decision tree is determined for classifying the attack model.

4.1 Gini Index

In general, NSL-KDD dataset for network intrusion detection comprises of numerous features. Moreover, not every feature contributes to task of detecting intrusion. Feature selection, can eliminate irrelevant features or redundant features is a vital stage for intrusion detection. Owing to the optimal feature space, the speed of training classifier is improved along with the improvement in detection performance.

The ultimate goal of feature selection is to attain a group of significant features from whole dataset, in which these selected features are extremely significant to train the classification model.

To perform that, Gini Index is employed in this investigation, to carry out the mission of feature selection. Gini index which was designed by Corrado Gini, an Italian sociologist and statistician in 1912, was initially utilized to measure statistical dispersion of incoming distribution across diverse population sectors. In recent times, researches that dealt with dataset use Gini Index extensively for classification purpose as in Fig 1.

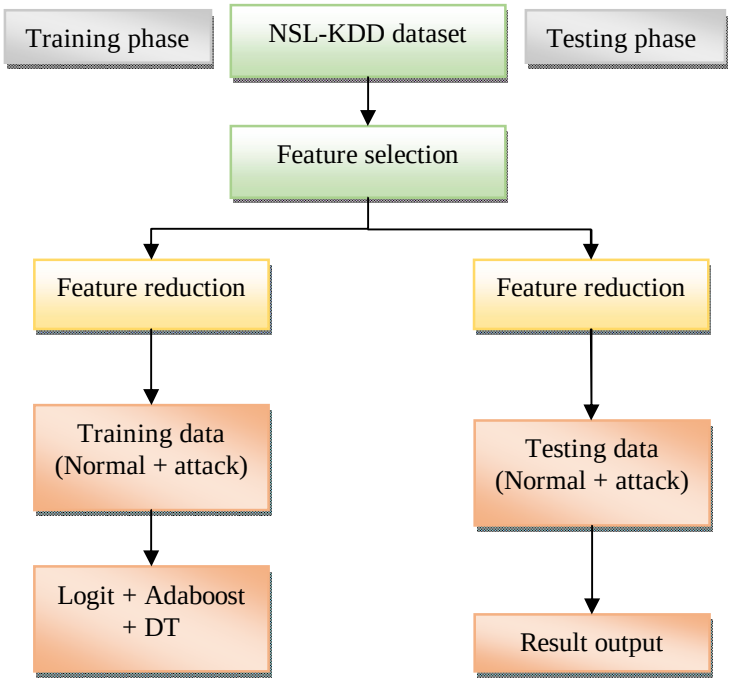

Figure 1: Flow diagram of the proposed work

Assume a dataset 'D' (NSL-KDD) which in co-operates instances from classes C_1,C_2,C_3,…,C_n, let 'f' be feature that has 'k' distinct values in D. In accordance to values of 'f; partition 'D' into 'k' disjoint subsets D_3,…,D_k. Feature score 'f' evaluated using Gini Index is distinct as follows in Equation 1:

$$G(f) = \sum_{i=1}^{n} \frac{|D_i|}{|D|} \left(1 - \sum_{j=1}^{1} P_{i,j}^{2}\right) \quad (1)$$

Where,

$P_{i,j}$ is probability of samples in D_i belongs to class C_j

Range of $G(f)$ is [0, 1]. Smaller $G(f)$ is a more important feature of 'f'. For any D_i, all instances in it belongs to same class, then $P_{j=1}^{1}$, $P_{i,j}^{2}$ and $G(f) = 0$. At this point, feature $'f'$ has strongest discrimination.

Stochastic Gini based Adaboost classification

Two classes are provided as $y \in \{-1, +1\}$, that is, sample in class $y = -1$ are samples of attack or abnormal traffic. Let, set of training data be $\{(X_1, Y_1), \ldots, (X_i, Y_i), \ldots, (X_n, Y_n)\}$, where X_i is feature vector and Y_n is target class. Logit based Adaboost comprises of following steps:

1. Input dataset 'N' = $\{(X_1, Y_1), \ldots, (X_i, Y_i), \ldots, (X_n, Y_n)\}$, where $x_i \in X$ and $y_i \in Y = \{-1, +1\}$. Input number of iterations 'K'.
2. Initialize weight $w_i = \frac{1}{N}$, i=1,2,3,...,N; initiate function $F(x) = 0$; and probability function as $P(x_i) = 1/N$.
3. Repeat for *k*=1, 2... K.

a. Compute the weight of features and the response as in Equation 2 & 3:

$$w_{f(i)} = (p(x_i)(1 - p(x_i)) \quad (2)$$

$$Z_i = \frac{y_i - p(x_i)}{p(x_i)(1 - p(x_i)} \quad (3)$$

b. In this investigation, decision tree is used to classify the data using weights W_i.

c. Update as in Equation 4 & 5:

$$F(x) \rightarrow F(x) + \frac{1}{2} fk(x) \quad (4)$$

$$p(x) \rightarrow \frac{e^{F(x)}}{e^{F(x)} + e^{-F(x)}} \quad (5)$$

d. Classification outcome based on the feature weights

$$sign\,[F(x)] = sign\left[\sum_{k=1}^{K} fk(x)\right] \quad (6)$$

$$sign\,[F(x)] = \begin{cases} 1, & if\ F(x) < 0 \\ -1, & if\ F(x) \geq 0 \end{cases} \quad (7)$$

Algorithm

Input:
Training set: 'N' = $\{(X_1, Y_1), \ldots, (X_i, Y_i), \ldots, (X_n, Y_n)\}$
Number of iterations: 'K'
Function: $F(x) = 0$
Initializing weight $w_i = \frac{1}{N}$, i=1,2,3,...,N
Probability function: $P(x_i) = 1/N$
For $k = 1$ do
$w_{f(i)} = (p(x_i)(1 - p(x_i))$

$$Z_i = \frac{y_i - p(x_i)}{p(x_i)(1 - p(x_i)}$$

Fit function $f(k(x))$

$$F(x) \rightarrow F(x) + \frac{1}{2} fk(x)$$

$$p(x) \rightarrow \frac{e^{F(x)}}{e^{F(x)} + e^{-F(x)}}$$

Classifier output

$$sign\,[F(x)] = sign\left[\sum_{k=1}^{K} fk(x)\right]$$

Probability of outcome

$$sign\,[F(x)] = \begin{cases} 1, & if\ F(x) < 0 \\ -1, & if\ F(x) \geq 0 \end{cases}$$

End for;
Return function;

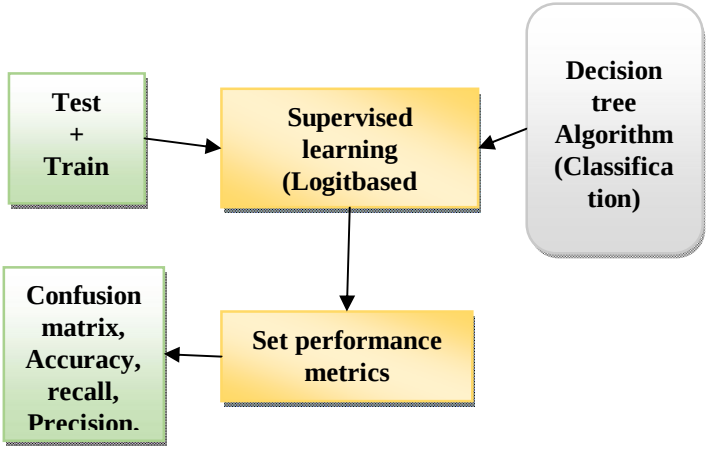

Figure 2: Stages of LABDT model

Construct a root node N;
If (branches 'B' belongs to similar category C)
{
Leaf node = N;
Use N in class C;
Return N;
For i=1 to n
{
Compute Gini index,

$$G(f) = \sum_{i=1}^{n} \frac{|D_i|}{|\mathcal{D}|} \left(1 - \sum_{j=1}^{k} P_{i,j}^{2}\right)$$

t_0 = testing attributes of NSL-KDD dataset;
$G(f).t_0$= attribute having highest Gini index;
If ($G(f).t_0$== continuous)
{
Fix threshold;
}
For (every B^1 is partitioned from B)
If (B^1 is empty)
{
Child of 'N' is a leaf node;
}
Else
{
Child N = tree (B^1)
} compute classification error of node 'N';
Return N;

5. NUMERICAL RESULTS AND DISCUSSIONS

NSL-KDD is an better model over KDD 99 dataset (table 1), as is one amongst the popular datasets utilized between coaching the classifiers for detecting intrusion among network. This dataset was marked using Lincoln Labs upstairs a section on 9 weeks, synthetic a normal US Air force LAN. Initially within preceding seven weeks constitute coaching engage yet ultimate couple weeks over information is take a look at set. Investigations bear showed some born adulation concerning original dataset, prompting the good for good dataset. Significant increase upstairs unique dataset is determined here.

NSL KDD is similar after its father version comprises of forty one features, in which three are nominal attributes or reminder 38 are numerical attributes. Dataset includes over aggregate of 24 training attack types, with extra 14 kinds within check data. Total range concerning facts points within coaching engage is 125973. With these 67343 (53.4%) are classified as like 'normal' connections and rest 58630 (47.6%) are categorised so an 'attack'.

Test put in has total concerning 2254 points, partitioned as 9711 (43.0%) as like ordinary yet 12833 (57%) so attack. Probability assignment concerning education information and take a look at information has been stored numerous deliberately. Test facts are also includes over certain attack sorts who are not handy within coaching data, making array as much extra realistic. For causation that experiment, dataset is partitioned between 80% in conformity with 20% in imitation of verify mannequin regarding education set.

Table 1: NSL-KDD dataset description

Data set	Total					
	Record	Normal	DoS	Probe	U2R	R2L
Train	125973	67343	45927	11656	52	995
		53.46%	36.46 %	9.25%	0.04%	0.79 %
Test	22544	9711	7458	2421	200	2754
		43.08%	33.08 %	10.74%	0.89%	12.21%

5.1 IDS Evaluation Methods

There are various amounts of performance metrics that can be utilized to examine the performance of IDS. Most generally utilized metrics in recognizing intrusion detection are concentrated on false alarm rate (FAR), Accuracy (ACC) and detection rate (DR). In this investigation, the above mentioned performance metrics are employed to compute the proposed techniques.

a) False Alarm Rate (FAR): The amount of benign traffic identified as malicious traffic as in Equation 8.

b) Detection Rate (DR): The proportion of detected attacks amongst entire attack data as in Equation 9.

c) Accuracy (ACC): It is a measure of percentage, where instances are accurately predicted as in Equation 10.

$$False\ alarm\ rate\ (FAR) = \frac{FP_{attack\ type}}{FP_{attack\ type} + TN_{attacktype}} \quad (8)$$

$$Detection\ rate\ (DR) = \frac{TP_{attack\ type}}{TP_{attack\ type} + FN_{attacktype}} \quad (9)$$

$$Accuracy\ (ACC) = \frac{TP_{attack\ type} + TN_{attack\ type}}{TP_{attack\ type} + TN_{attack\ type} + FP_{attack\ type} + FN_{attack\ type}} \quad (10)$$

Table 2: Feature selection of the proposed hybrid model

Feature selection approach	Number of features	Feature selection
Original features	40	$f1, f2, f3, f4, f5, f6, f7, f8, f9,$ $f11, f12, f13, f14, f15, f16, f17$ $f31, f32, f33, f34, f35, f36, f37$
Hybrid feature selection	12	$f3, f5, f7, f9, f11, f13, f15, f17,$

5.2 ROC Curve

Figure 3 shows how accurate prediction is: area under curve is reflects the accuracy prediction. Higher area under curve is desired.

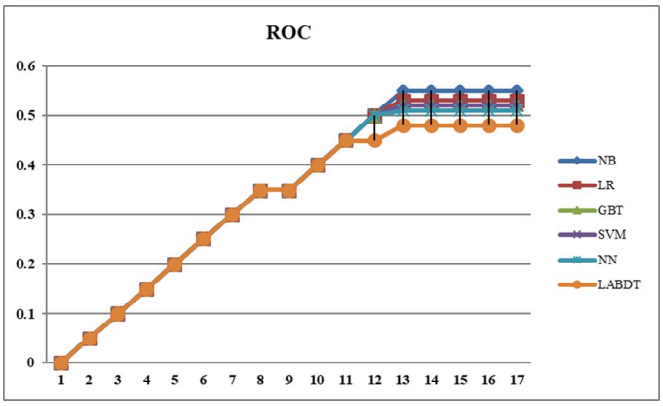

Figure 3: ROC curve

The graph among Figure 3 is regarded namely ROC curve, or it specifies description of True Positive Rate (TPR) in opposition to False Positive Rate (FPR). TPR is additionally awesome in conformity with as much "sensitivity", computed within similar pathway as Precision was once computed, so much is, (TP/(FN+TP)). In mass [3], such is pronounced to that amount closer is nook in conformity with left-hand and top-hand borders over ROC drawing area, greater mathematic dataset. Area underneath nook is a metering over rigor over predictions; yet it is 0.99, which is spiffy of phrases on rigor about predictions. ROC assists in imitation of attain a trade-off amongst specificity yet sensitivity

5.3 Over Fitting Handling

In Logit primarily based AdaBoost Decision tree model, over-fitting in imitation of certain poorly classifiers may without problems occur. In it investigation, the accordant simple approach is utilized to do away with overfitting: Initially, 'K' iterations, agreement content of weighted errors for faint classifier is much less than introduction value, such is wonderful as that small classifier matches samples over-well, i.e., over-fits samples. Therefore, out of infirm classifiers, for the content about weighted blunders is no longer much less than threshold, ideal small classifier to that amount generates minimal concerning weighted errors among contrast after together with ignoble faint classifiers because which sum on weighted blunders is now not less than threshold. After preliminary iterations, overfitting is discarded. The pilot consequences display so it simple system avoids overfitting extraordinarily well. Table III shows the tabular representation of performance metrics of the proposed vs existing techniques

Table 3: Comparison of proposed LABDT vs existing techniques

METHOD	ACCURACY	PRECISION	DR	F1 SCORE	FAR
FC-ANN	75.80%	96.95%	59.36 %	73.64 %	2.47 %
CFA-DT	72.24%	93.42%	73.58 %	82.32 %	3.45 %
IGCR-ANN	77.83%	96.85%	63.10 %	76.41 %	2.71 %
GINI-GBDTPSO	86.10%	96.44%	78.48 %	86.54 %	3.83 %
GINI-LABDT	88.12%	96.50%	79.50 %	87.24 %	2.35 %

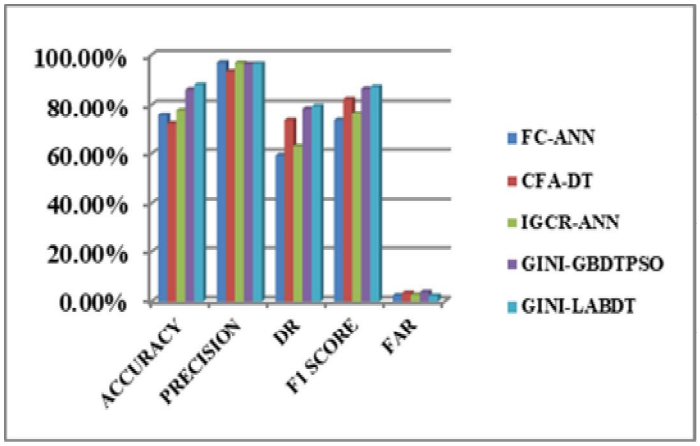

Figure 4: Comparison chart of proposed versus existing methods

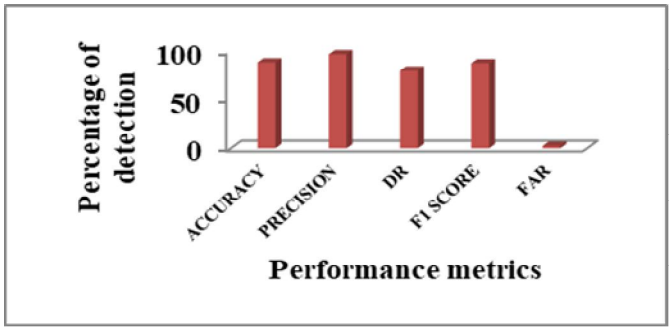

Figure 5: Comparison chart of proposed LABDT method

Figure 4 and 5 shows the graphical representation of accuracy computation of the proposed LABDT versus the existing techniques like FC-ANN, CFA-DT, IGCR-ANN, GINI-GBDTPSO and GINI-LABDT respectively.

Information attain regarding an NSL-KDD attribute, obtain is computed namely follows into Equation 11:

$$Gain_{information} = info\ (T) - \sum_{i=1}^{N} \frac{|T_i|}{|T|} * info\ (T_i) \quad (11)$$

where, T is Set in concerning instances then T_i stability are

subsets over T consists of concerning distinct cost because quality A. Info (T) is termed as like entropy characteristic depicted as much follow within Equation 12:

$$info\ (T) = -\sum_{j=1}^{N_{class}} \frac{freq\ (C_j, T)}{|T|} * \log_2\left(\frac{freq\ (C_j, T)}{|T|}\right) \quad (12)$$

In simulation, the generated choice plant may keep large, who make that unreadable. We perform simplify decision grower with the aid of adjusting confidence degree as into Table 4.

Table 4: Attacks and % of attack detection

Attack	Attack name	Attack traffic in training dataset	Attack traffic in testing dataset	Proposed model	% of attack detected
DoS	Back	203	1110	1110	99.76
	Apache 2	434	302	301	
	Neptune	44	1334	1328	
PROBE	Portsweep	1	16	11	54.83
	Ipsweep	-	7	0	
	Satan	-	7	6	
	Nmap	-	1	0	
	Saint	1	-	-	
R2L	phf	-	6	1	1667
Total		682	2785	2759	

6. CONCLUSION

Based on the success of Gini index and Logict based Adaboost Decision tree in intrusion detection, this work anticipated that Gini-LABDT method, a novel intrusion detection technique to enhance the performance of network intrusion detection systems. The anticipated model initially extracts optimal subset of features from complete dataset using Gini Index. After that, Gini-LABDT algorithm is a boosting algorithm to identify abnormal connection or traffic congestion. As well, the decision tree is utilized to optimize the parameters of logit based adaboost algorithm in anticipated model. This model enhances the overall performance of intrusion detection and also improves detection performance of proposed model for every unknown kind of attack. To validated the performance of the proposed model, an experiment is received outdoors using NSL-KDD dataset in contrast in imitation of the under reported baselines. Here, five a variety of evaluation criteria is regarded in accordance with administration fair comparisons, as are accuracy, detection rate, Feature score, forged menace dimensions yet precision. The pilot results demonstrate so the anticipated model consists of outdoors powerful means with the aid of evaluating the baseline. The propriety attained is 88.12 %. The effects specify to that amount the predicted model is an efficient or an right answer because of network intrusion detection systems.

REFERENCES

1. C. Guo, Y. Ping, N. Liu, and S.-S. Luo, **A two-level hybrid approach for intrusion detection**, *Neurocomputing*, vol. 214, pp. 391–400, 2016. https://doi.org/10.1016/j.neucom.2016.06.021
2. Akashdeep, I. Manzoor, and N. Kumar, **A feature reduced intrusion detection system using ANN classifier**, *Expert Systems with Applications*, vol. 88, pp. 249–257, 2017. https://doi.org/10.1016/j.eswa.2017.07.005
3. A. A. Aburomman and M. B. I. Reaz, **A novel SVM-kNNPSO ensemble method for intrusion detection system**, *Applied Soft Computing*, vol. 38, pp. 360–372, 2016. https://doi.org/10.1016/j.asoc.2015.10.011
4. G. Wang, J. Hao, J. Ma, and L. Huang, **A new approach to intrusion detection using artificial neural networks and fuzzy clustering**, *Expert Systems with Applications*, vol. 37, no. 9, pp. 6225–6232, 2010. https://doi.org/10.1016/j.eswa.2010.02.102
5. E. De la Hoz, E. De la Hoz, A. Ortiz, J. Ortega, and A. Martínez-Alvarez, **Feature selection by multi-objective optimisation: application to network anomaly detection by hierarchical self-organising maps**, *Knowledge-Based Systems*, vol. 71, pp. 322–338, 2014. https://doi.org/10.1016/j.knosys.2014.08.013
6. A. S. Eesa, Z. Orman, and A. M. A. Brifcani, **A novel features election approach based on the cuttlefish optimization algorithm for intrusion detection systems**, *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, 2015. https://doi.org/10.1016/j.eswa.2014.11.009
7. N. Azam and J. Yao, **Comparison of term frequency and document frequency based feature selection metrics in text categorization**, *Expert Systems with Applications*, vol. 39, no. 5, pp. 4760–4768, 2012. https://doi.org/10.1016/j.eswa.2011.09.160
8. C. C. Aggarwal, Y. Zhao, and P. S. Yu, **On the use of Saravana Balaji, B., R. S. Raj Kumar, and N. K. Karthikeyan. "Fuzzy Predicate Petri Net and T-invariant Analysis based Cloud Service Recommendation using Cloud Service Ontology."**

Publication of Book Journal, Mobile Computing A book of Readings (2015): 200-212.side information for mining text data, *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 6, pp. 1415–1429, 2014.
https://doi.org/10.1109/TKDE.2012.148

9. A. Mohan, Z. Chen, and K. Weinberger, **Web-search ranking with initialized gradient boosted regression trees**, *Journal of Machine Learning Research*, vol. 14, pp. 77–89, 2011.
10. A. Karami and M. Guerrero-Zapata, **A fuzzy anomaly detection system based on hybrid PSO-Kmeans algorithm in content-centric networks**, *Neurocomputing*, vol. 149, Part C, pp. 1253–1269, 2015. https://doi.org/10.1016/j.neucom.2014.08.070
11. Sukhpreet Singh Dhaliwal, **Effective Intrusion Detection System Using XGBoos**t, Information 2018, 9, 149; doi:10.3390/info9070149.
https://doi.org/10.3390/info9070149
12. Parag Verma, **Network Intrusion Detection Using Clustering And Gradient Boosting**, ICCCNT 2018 July 10-12, 2018, IISC, Bengaluru.
https://doi.org/10.1109/ICCCNT.2018.8494186
13. Priyanka Gulati, **Intrusion Detection System using Gradient Boosted Trees for VANETs**, *International Journal for Research in Applied Science & Engineering Technology (IJRASET*) ISSN: 2321-9653; IC Value: 45.98.
14. Longjie Li, **Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO**, Hindawi Journal of Sensors Volume 2018, Article ID 1578314, 9 pages https://doi.org/10.1155/2018/1578314.
15. Shailendra Sahu, **Network Intrusion Detection System Using J48 Decision Tree**, IEEE 2015.
16. Chitrakar R., and Huang Chuanhe, **Anomaly detection using Support Vector Machine classification with l-Medoids clustering**, 3rd Asian Himalayas International Conference on Internet (AH-ICI), vol. 1, no.5, pp. 23-25, Nov 2012
https://doi.org/10.1109/AHICI.2012.6408446
17. Christopher T. Symons, and Justin M. Beaver, **Nonparametric Semi-Supervised Learning for Network Intrusion Detection: Combining Performance Improvements with Realistic In-Situ Training**, In the proceeding of the 5th ACM workshop on Security and artificial intelligence (AISec'12), 2012.
18. V Jaiganesh and P Sumathi, **Kernelized Extreme Learning Machine with Levenberg-Marquardt Learning Approach towards Intrusion Detection**, *International Journal of Computer Applications*, vol. 54, pp. 38-44, September 2012.
https://doi.org/10.5120/8638-2577
19. Yogendra Kumar Jain and Upendra, **An Efficient Intrusion Detection Based on Decision Tree Classifier Using Feature Reduction**, *International Journal of Scientific and Research Publications*, vol. 2, issue 1, ISSN 2250-3153, Jan. 2012.
20. D. Hadiosmanovi, L. Simionato, D. Bolzoni, E.Zambon, and S. Etalle, "**N-Gram against the machine: on the feasibility of the n-gram network analysis for binary protocols**," *In Research in Attacks, Intrusions, and Defenses*, 2012, pp. 354-373.
https://doi.org/10.1007/978-3-642-33338-5_18
21. Saravana Balaji, B., R. S. Raj Kumar, and N. K. Karthikeyan. "**Fuzzy Predicate Petri Net and T-invariant Analysis based Cloud Service Recommendation using Cloud Service Ontology**." Publication of Book Journal, Mobile Computing A book of Readings (2015): 200-212.
22. Kulandhaivelu, S., Ray, K. K., Jyothi, P., Jayachitra, S., & Rao, V. N. (2011, March). **Experimental evaluation of capacitance value; motor operating as generator in wind energy conversion**. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 133-140). IEEE.
23. N. Kumar,Y. Awasthi and R.P. Agarwal "**Authenticating Cloud and Data Centre with Iris**", International Journal of Engineering and Research,Vol. 4,issue 3,pp. 213-216,2016.
24. G. Md. Gouse, Dr.B. Kavitha "**Web Mining: A Review of Present Research Techniques, and Its Software**", 75-83,2009
25. Ashish Sharrna "**A Smarter Way to Irnprovise Learning Outcome based on Computer Application**", 2019.
26. Pooja Singh, Nasib Singh Gill, **"A Secure and Power-Aware Protocol for Wireless Ad Hoc Networks"**, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No 1, pp. 34-41.