DEPARTMENT OF COMMUNICATIONS ENGINEERING
AHMADU BELLO UNIVERSITY, ZARIA - NIGERIA

Proceedings of the 1st National Communication Engineering Conference 2018

A Novel Model for Network Anomaly Detection based on Naïve Bayes using Wrapper Approach

John OcheOnah and Shafi'i Muhammad Abdulhamid,
Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.
jhonchekzy@gmail.com, shafii.abdulhamid@futminna.edu.ng

ABSTRACT—The drastic increase in network attack has been a major concern in cyber security especially now that internet usage and connectivity is at high demand. In a way of combating some of these network attacks, data mining technique for network anomaly detection and network event classification attack has proven efficient and accurate. This research presents a novel feature selection approach that eliminates extraneous features to minimise time complexity as well as building an improved model that predict result with a higher accuracy based on wrapper approach for intrusion detection. Attack types are predicted based on Naïve Bayes - the base classifier. From the experiment, our proposed model demonstrates a higher overall performance of 99.73% accuracy, keeping the false positive rate as low as 0.006. Our model performed better than models like as Markov chain, K-Nearest Neighbors (KNN), Hidden Naïve Bayes (HNB) and Boosted Decision Tree (DT). The NSL-KDD is used in experimental setup as benchmark data set using Weka library functions.

***KEYWORDS—component, formatting, style, styling, insert** (key words)*

INTRODUCTION

Recently, they have been a high increase in the computer network intrusion incidents and network hacking tools due to the increase in technology and computer networks vulnerabilities. As threats on networks keep increasing, there is an urgent need to develop more accurate and sensitive intrusion detection system that will reduced these threats. Intrusion detection system is usually designed and installed on networks in other to protect the network and systems on the network form known and unknown vulnerabilities, threats and malicious attacks. Based on the nature of attacks on a network, Intrusion detection can be categorised in two (2) major forms, namely; anomaly detection and misuse(signature-based) detection [1]. Patterns of normal network behaviour and usage are used to pinpoint various anomalies or attacks as in the case of anomaly detection approach [13] whereas, patterns and behaviours of known attacks are used to detect attack types that are already known as in the case of signature-based misuse detection. Various approaches of identifying anomaly and misuse of a system are achieved through the application of various techniques of data mining and machine learning methods that involve single classifier [5][22] and ensemble classifiers [16] have been widely used by researchers. Researchers have been using different classifiers to identify pattern-based attacks but the degree of accuracy of these classifiers which is based on the various algorithms and how they are been trained have been a major concern. In other to reduce the learning run time and accuracy of the algorithm, best features must be selected for the feature vector of the algorithm [1].

Feature selection is an essential criterion in dataset training as it removes irreverent features and reduce dimensionality and thereby improves the predictive accuracy [25]. It is very useful in the field of intrusion detection, pattern recognition, data mining, image processing and machine learning, as it maps out only useful features (subset of features) for data and pattern. It thereby builds a high accuracy model since its eliminate inappropriate features and reduces time complexity. Levent*et al.*, (2012) [12] classified feature selection model into Filter, Wrapper and Embedded method.

Classification on the other hand, is a data mining technique where each instance in a dataset is assigned to a particular class. Important data classes are defined to extract data models and these models are called as classifiers. In this technique learning and classification are two steps for data classification. In the learning step a classifier is formed and the class labels for the data are predicted by using this classifier. In the classification technique every data in the dataset has an attribute value that defines class and all the classes are predefined so that the analyst has a prior knowledge [1]. Classification can also be used to label every record in the data set and the records can be classified in predetermined set.

I. BRIEF DESCRIPTION OF GENETIC ALGORITHM AND NAÏVE BAYES

A. Genetic Algorithm

Genetic algorithm is derived from the theory of Darwin on natural selection [17]. It is an optimization algorithm which comprise of genetic information known as chromosome for optimizing the problem set by encoding the solution of the candidate (i.e. individuals). Genetic information is represented by binary strings such as 0's or 1's and the problem set solution is encoded with sets of bits. The two major operators involved in genetic algorithm are crossover and mutation that are applied on the individuals for the next generation. The selected strings of bit from the parent are duplicated by the crossover operator producing two posterity strings. While on the other hand, mutation arbitrarily alters the value of string bits. The increased in the probability of a single bit survival is guaranteed by fitness function increased throughout the evolutionary process [4]. Genetic algorithm is more effective and has huge space for searching with a small probability of achieving local optimal solution as compared to other algorithms. Genetic algorithms work productively to select subset of features with a less computational prerequisite for classification using stochastic optimization strategy [11].

B. Naïve Bayes

In data mining, Naïve Bayes algorithm as an effective inductive learning algorithm is a straightforward type of classifier derived from classical statistical theory "Bayes theorem." The "naïve" is established on Bayes Rule which shows that the features are conditionally independent from each other with respect to the class [3]. In the literature, the Naïve Bayes algorithm has demonstrated its adequacy in different spaces, for example text classification [6], improving search engine quality [10], image processing [27][23], and medical diagnoses [2].

The working of Naive Bayes classifier is as follows: let X be a vector of random variables representing the observed attribute values in the training set X = [x_1, x_1,… x_n] to certain class label c in the training set. The probability of each class given the vector of observed values for the predictive attributes can be computed using the following formula [8]:

$$P(c/x) = \frac{P(x/c)\ P(c)}{P(x)}$$

$$P(c/X) = P(x_1/c) \text{ x } P(x_2/c) \text{ x}\ldots\text{x } P(x_n/c) \text{ x } p(c)$$

Where:

P(c/x) is the posterior possibility of class (target) given predicator (attribute)

P(c) is the prior possibility of class.

P(x/c) is the possibility which is the probability of predicator given class.

P(x) is the prior possibility

Adequacy of Naïve Bayes algorithm in classification and learning is ascribed to several attributes, for example.

High computational effectiveness when contrasted with other wrapper strategies since it is economical, it is viewed as linear time complexity classifier.

Low variance due to less searching.

Incremental taking in light of the fact that NB functions work from estimate of low-order probabilities that are derived from the training data. Thus, these can be quickly updated as new training data are obtained.

i. High ability to deal with noise in the dataset.

ii. High ability to deal with missing values in the dataset.

In addition, Naïve Bayes implementation has no required adjusting parameters or domain knowledge. The real downside of NB just lies in the assumption of features independence. Despite this, Naïve Bayes often delivers competitive classification accuracy and is broadly applied in practice especially as benchmark results.

II. RELATED STUDIES

A list of research has been done on enhancing the performance of intrusion detection system in order to beat the impediment of old-fashioned systems by consolidating machine learning techniques with different detection approaches.

Muniyandi et al., (2012) [14] combined k-means clustering and C.45 decision tree method for classification method called Cascading developed to ease the dominating of k-means technique and forced assignment. The k-means breakdown the training dataset into k-subsets then C.45 is created for the broken-down subsets. Also, Natesan et al (2012) [15] in their work proposed an improved single weak classifier using AdaBoost. Bayes Net, Naïve Bayes and Decision Tree (DT) were used as weak performed better than those with AdaBoost. However, the major problem is that, it lacks mechanism for detecting novel attacks that have signature similar to known attacks leading to low detection possibly.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Govindarajan and Chandrasekaran [9] introduced a hybrid-based detection architecture-entailing ensemble and base classifiers for detection system. The ensemble module was built using the result of both Radial Basis function (RBF) neural networks and Multilayer Perceptron (MLP). This experiment result showed this hybrid architecture was better than the individual RBF and MLP classification model in terms of performance. However, the drawback hybridising the classification models is overhead since each connection is examined by the individual classifier models.

A cuttlefish optimization-based algorithm (CFA) was proposed by [1] for optimally selecting from KDD cup 99 dataset, subset features with an accuracy of 91.986 %. Another feature selection framework was put forward by (Yang and M. T, 2011) [24]. Their approach involves combing genetic algorithm and K-nearest neighbour for optimal feature selection and weighting. Originally during the training step, 35 features were weighted and in light of their weight the top ones were picked for the testing stage implementation. 19 features were considered and give an accuracy of 97.42% for known attacks, actually, accuracy rate of 78% was recorded when 28 features were considered for obscure attacks.

Ranker based Boosted model was proposed by Yung-TsungHou (2010) [26] with an accuracy of 96.14%. whileLevent et al. (2012) [12] carried out the Hidden Naïve with accuracy of 93.72% in intrusion detection system though suffers from dimensionality. Shun-Sheng [21] in 2011 came up with a ranker search based Adaptive Response Theory on SVM with accuracy of 95.13% accuracy in intrusion detection system. A Markov chain intrusion detection system having an accuracy of 90.0% is proposed by Seongjun (2013) [19] based on advance probabilistic approach.

An adaptive and hybrid neurofuzzy system ensemble (NFBoost algorithm) was proposed by Selvakumar and Kumar P. A. Raj [18] in their research to identify both known and novel attacks of DDoS, it reduces total error thereby improving the accuracy of the detection. They developed the base classifier using Neuro-Fuzzy Inference System (ANFIS). The final classification conclusion or decision is gotten by the combination of the ensemble classifier's output and Neyman Pearson cost minimization strategy.

FC-ANN IDS as a proposed work of Gang Wang et al. [7] is a final product of Fuzzy Clustering (FC) and Artificial Neural Network (ANN). The Fuzzy Clustering method is part of FC-ANN that split training dataset into several similar subsets. This simplify each training subset by decreasing the complexity and improving the detection performance. It means, while the Fussy Clustering technique splits the training dataset, diverse ANN Classifier are trainedby the generated training subset trains the Produced preparing subsets. Fuzzy aggregator, at last is employed to integrate the outputs of individual classifiers into a unified one for final prediction.

Levent et al. [12] carried out experiments on KDD99 dataset to ascertain the accuracy of Naïve Bayesian (NB) and its six subcategories; Averaged One-Dependence Estimators (AODE), DTNB, Weightily AODE (WAODE), Tree-Augmented Naïve Bayesian (TAN), Decision Tree (NBTree), Hidden Naïve Bayesian (HNB) as regards to DDoS attacks. The results demonstrated the high accuracy rate of HNB using proportion K-Interval discretization method as regars to the other variants experimented with.

Shi-Jinn Horng et al. [20] designed an IDS combining hierarchical clustering and Support Vector Machine (SVM). The hierarchical clustering algorithm part transformed the training dataset to a reasonable sizable dataset for SVM to train large dataset with reduced time. This transformed dataset is partitioned into five categories which is used for training four SVM classifiers. The final result is the outputs of the merged classifiers.

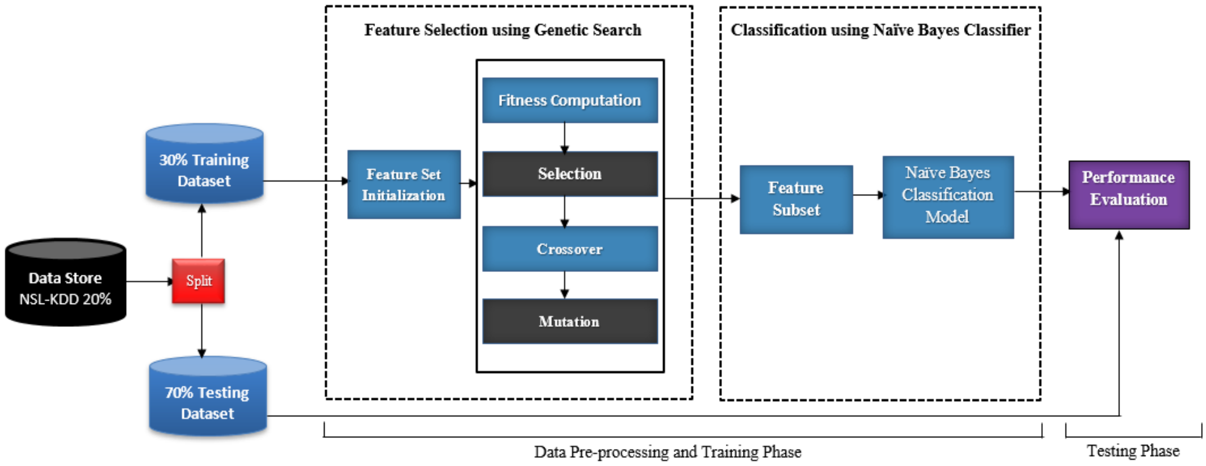

Fig. 1 Proposed Wrapper-Based Naïve Bayes Classification Framework

III. PROPOSED FRAMEWORK

The operation of this proposed framework is in two stages. Stage 1 involves the feature selection process using a wrapper approach with Genetic Search algorithm while stage 2 is about the classification of Test instances using Naïve Bayes.

Process involved in stage 1 is screening and removing redundant features and a wrapper feature selection is proposed for the purpose of getting a better accuracy. Genetic search as the search algorithm used for searching through the space of possible features and Naïve Bayes based model employed on each subset for evaluation. At the end, feature subset is been selected based on the performance while, stage 2 entails building a classification model using a Naïve Bayes algorithm. Finally, an instance of a test is by the new Naïve Bayes based built classification model as shown by Fig. 1 followed by the algorithm.

Algorithm: Proposed Wrapper Based Naïve Bayes Attack Detector (WBNAD)

Input: Dataset

Output: Class labelled test instance

Step 1: Generate randomly, an initial population, *P*.

Step 2: Compute *e(x)* for each member *x* Ɛ *P*.

Step 3: Define a probability distribution *p* over the member of *P* where *p(x) α e(x)*.

Step 4: Select two population members *x* and *y* with respect to *p*.

Step 5: Apply crossover to *x* and *y* to produce new population members *x'* and *y'*.

Step 6: Apply mutation to *x'* and *y'*.

Step 7: Insert *x'* and *y'* into *P'* // *The next generation.*

Step 8: if |*P'*| < |*P*|, goto 4

Step 9: Let *P* ⟵ *P'*

Step 10: if there are generations to still process, goto 2.

Step 11: Return *x* Ɛ *P* where *e(x)* is highest.

Step 12: Given a training set, for each Class c_iƐC

i. Estimate the prior probability: $P(c_i)$

ii. For each feature *x*, estimate the probability of that feature value given Class c_i: $P(x_j/c_i)$

Step 13: for each Class c_iƐC, compute: $P(c_i) * \prod_{j=1}^{n} P(x_j/c_i)$

Step 14: Select the most probable Class $C = \underset{c_i \mathcal{E} C}{\mathrm{argmax}}\, P(c_i) * \prod_{j=1}^{n} P(x_j/c_i)$

EXPERIMENTAL SETUP

The experiment run on an Intel® Core™ i5-2410M CPU @2.45Ghz,~2.4GHz with 4.00 GB memory running on 64-bit Windows 10. The experiment was carried out with the aid of JAVA programming language, WEKA 3.8 machine learning apparatus and Weka Library functions for feature selection techniques. We used a well-known NSL-KDD benchmark dataset created by the MIT Lincoln Lab for the experiment with aim of juxtaposing the performance of different intrusion detection techniques. Dataset of NSL-KDD containing classes which are grouped into five, namely: normal and four types of attacks such as R2, Probing, DoS, and U2R.

20% NSL-KDD dataset is utilized in the experiment for both training and testing with further splitting of the 20% dataset into 30% of the instances as training instance and the rest 70% as testing instance. Table 1 demonstrates the details of the 41 features of the dataset [16].

Table 1. 41 Features of NSL-KDD Data Set [16]

Feature No.	Feature Name	Type	Feature No.	Feature Name	Type
1.	Duration	Con.	22.	is_guest_login	Dis.
2.	protocol_type	Dis.	23.	Count	Con.
3.	Service	Dis.	24.	srv_count	Con.
4.	Flag	Dis.	25.	serror_rate	Con.
5.	src_bytes	Con.	26.	srv_serror_rate	Con.
6.	dst_bytes	Con.	27.	rerror_rate	Con.
7.	Land	Dis.	28.	srv_rerror_rate	Con.
8.	wrong_fragment	Con.	29.	same_srv_rate	Con.
9.	Urgent	Con.	30.	diff_srv_rate	Con.
10.	Hot	Con.	31.	srv_diff_host_rate	Con.
11.	num_failed_logins	Con.	32.	dst_host_count	Con.
12.	logged_in	Dis.	33.	dst_host_srv_count	Con.
13.	num_compromised	Con.	34.	dst_host_same_srv_rate	Con.
14.	root_shell	Con.	35.	dst_host_diff_srv_rate	Con.
15.	su_attempted	Con.	36.	dst_host_same_src_port_rate	Con.
16.	num_root	Con.	37.	dst_host_srv_diff_host_rate	Con.
17.	num_file_creations	Con.	38.	dst_host_serror_rate	Con.
18.	num_shells	Con.	39.	dst_host_srv_serror_rate	Con.
19.	num_access_files	Con.	40.	dst_host_rerror_rate	Con.
20.	num_outbound_cmd	Con.	41.	dst_host_srv_rerror_rate	Con.
21.	is_host_login	Dis.			

A. Performance Metric

True Positive (TP): TP is an Alarms setup to be alerted when there is successful and accurate identification of normal behaviours.

False Positive (FP): FP is an Alarm setup to go on immediately an abnormal behaviouris incorrectly identified as normal.

Accuracy: It is the proportion of correctly classified classes.

Precision: It estimate the probability of a positive prediction that are being correct.

It is paramount to keep the false alarm rates as low as possible and to ensure the security of the system, the false negative alarms should be at the barest minimum

B. Experimental Result and Evaluation

With respect to the NSL-KDD dataset used which comprised of a normal type of class label and class label for 4 attack type such as R2, Probing, DoS, and U2R. A well-known classification system called k-fold cross validation that is capable of eliminating over-fitted classification was used based on 10-fold cross validation

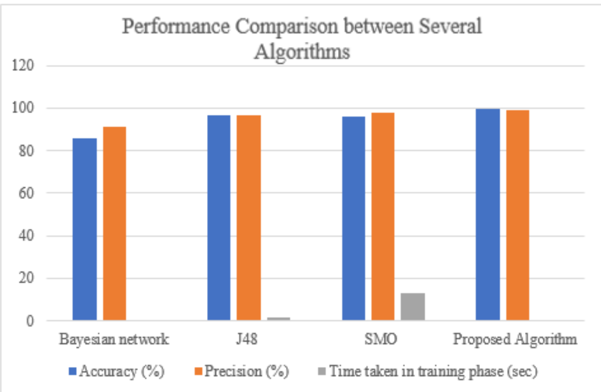

Fig. 3. Performance Comparison between Several Algorithms

Table 2 demonstrated the general performance of the proposed IDS model. Clearly the proposed model performed better with the follow results: true positive rate of 97.3%; low false positive rate of 0.6%; and ROC area of 99.7% as compared to the other models marking our model to have performed excellently. It suffices to know that the benchmark for ROC area is greater or equal to 95%.

Table 3 below shows the result of proposed algorithm as

Table 2. Overall Performance of the Proposed IDS

Class	True Positive Rate (TPR) (%)	False Positive Rate (FPR) (%)	ROC Area (%)
Normal	97.5	0.6	99.7
U2R	73.5	0.2	93.5
R2L	77.1	0.1	99.1
DoS	96.9	0.6	99.7
Probing	93.4	0.4	99.2
Average Weight	98.1	0.6	99.7

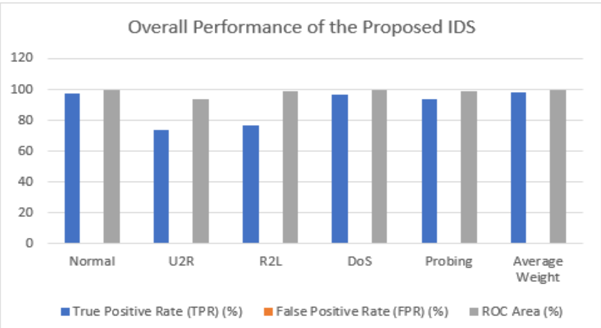

Fig. 2. Overall Performance of the Proposed IDS

compared to some other algorithms. It is evident that the proposed system performed better with an accuracy rate of 99.73% whereas other algorithms such as Bayesian Network gave an accuracy rate of 85.76%, algorithm SMO gave an accuracy of 95.99% and a decision tree J48 algorithm gave 96.43%. The time taken for training phase of the classification model in the proposed algorithm is very low, 0.18 sec compared to Naive Bayes, J48 and SMO which takes 0.2, 1.73, and 13.1 respectively as graphically represented in Fig. 3.

Table 3. Performance Comparison between Several

Algorithms	Bayesian Network	J48	SMO	Proposed Algorithm
Accuracy (%)	85.76	96.43	95.99	99.73
Precision (%)	91.4	96.5	97.6	99. 1
Time taken in training phase (sec)	0.20	1.73	13.01	0.18

Our proposed wrapper approach in terms of performance as compared with some other well-known feature selection techniques is demonstrated in Table 4 and depicted in Fig. 4. Out of 41 features, our proposed wrapper approach performed better than a Consistency Feature Selection (CFS) technique with 16 important features selected. CFS technique using rank search gave 93.13% accuracy while CFS using filter approach gave 94.88 % accuracy rate and finally, 91.13% was recorded using CFS type filter based genetic search which obviously is considerably low as compared to our proposed wrapper approach for feature space searching.

IV. Conclusion and Future Work

In this research work, a novel model termed Wrapper Based Naïve Bayes Attack Detector (WBNAD) for intrusion detection is proposed. WBNAD is based on wrapper approach for feature selection and Naïve Bayes Classifier. The process involved the preparation of a proper NSL-KDD train dataset with features16 out of 41 as final features selected. Classification of test instances followed using Naïve Bayes classifier. Our proposed model recorded 0.006 as False Positive Rate (FPR) and a 98.1% True Positive Rate (TPR). The result of the proposed model appeared to be reliable and outdone other classifiers with respect to their performances in efficiency and accuracy. Conclusively, the wrapper approach using reasonable features performs excellently as regards to anomaly intrusion detection.

The study from this experiment revealed a method in which an intrusion detection can be observed by using fewer features leading to the reduction of time as well as the

Table 4. Performance Comparison between Several Feature Selection Techniques

Algorithm	Feature Selected	Accuracy (%)
BestFirst+ConsistencySubsetEval	9	96.99
GeneticSearch+CfsSubsetEval	23	91.13
GreedyStepwise+CfsSubsetEval	11	92.81
RankSearch+CfsSubsetEval	14	94.88
RankSearch+ConsistencySubsetEval	26	93.13
Nil	41	92.68
Proposed Wrapper Approach	16	99.73

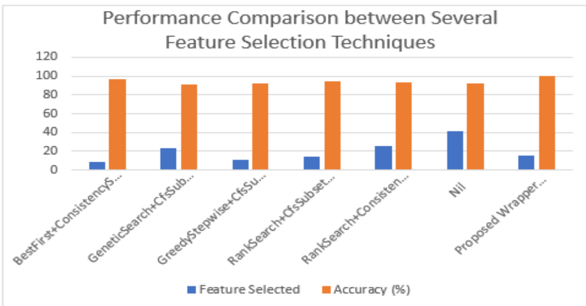

Fig. 4. Performance Comparison between Several Feature Selection Techniques

complexity involved in both the training and testing stage. Future research areas can be in the following aspects: An easy feature selection approach should be developed by exploring other techniques for efficient and effective feature selection. Experimenting this proposed method using actual cloud data for the purpose analysis real-time results.

References

[1] S. E. Adel, O. Zeynep, and M. A. B. Adnan, "A Novel Feature-Selection Approach Based on the Cuttlefish Optimization Algorithm for Intrusion

Detection Systems," Expert Systems with Applications, Vol. 42, pp. 2670-2679, April 2015.

[2] M. Anbarasi, E. Anupriya and N. Iyengar, "Enhanced Prediction of Heart Disease with Feature Subset Selection using Genetic Algorithm," International Journal of Engineering Science and Technology, Vo. 2, pp. 5370–5376, October 2010.

[3] C. Anuradha and T. Velmurugan, "A Comparative Analysis on the Evaluation of Classification Algorithms in the Prediction of Students Performance," Indian Journal of Science and Technology, Vol. 8, pp. 1 – 12, July 2015.

[4] T. Chih-Fong, E. William and C. Chi-Yuan, "Genetic Algorithms in Feature and Instance Selection,". Expert Systems with Applications, Vol. 39, pp. 240 – 247, February 2013.

[5] Y. Y. Chung and N. Wahid, "A Hybrid Network Intrusion Detection System using Simplified Swarm Optimization (SSO)", Applied Soft Computing Journal, Vol. 12, pp. 3014 – 3022, September 2012.

[6] G. Feng, J. Guo, B.-Y. Jing, and L. Hao, "A Bayesian Feature Selection Paradigm for Text Classification," Information Processing and Management, Vol. 48, pp. 283–302, March 2012.

[7] G. Wang, J. Hao, M. Jian and Huang L., "A New Approach to Intrusion Detection using Artificial Neural Networks and Fuzzy Clustering," Expert Systems with Applications vol. 37 pp. 6225–6232, September 2010.

[8] M. Gaurav and R. C. Ravi, "A Review Paper on IDS Classification using KDD 99 and NSL KDD Dataset in WEKA. International Conference on Computer", Communications and Electronics, Vol. pp. 553 – 558, July 2017.

[9] M. Govindarajan, and R. M. Chandrasekaram, "Intrusion Detection using Neural based Hybrid Classification Methods," Computer Network, Vol. 55, pp. 1662 – 1671, June 2011.

[10] H. T. T. Nguyen and D. K. Le, "An Approach to Improving Quality of Crawlers using Naïve Bayes for Classifier and Hyperlink Filter," Computational Collective Intelligence. Technologies and Applications, pp. 525 – 532, 2012.

[11] T. Karthikeyan and P. Thangaraju, "Genetic Algorithm based CFS and Naive Bayes Algorithm to Enhance the Predictive Accuracy," Indian Journal of Science and Technology, Vol. 8, pp. 1 – 8, October 2015.

[12] K. Levent, A. M. Thomas and S. Shahram, "A Network Intrusion Detection System Based on a Hidden Naïve Bayesian Multiclass Classifier," Expert Systems with Applications, vol. 39, pp. 13492–13500, December 2012.

[13] S. Ming-Yang, "Real-time anomaly detection systems for Denial-of-Service Attacks by Weighted K-nearest-Neighbor Classifiers," Expert Systems with Applications, vol. 38, pp. 3492–3498, April 2011.

[14] P. Muniyandi, R. Rajeswari and R. Rajaram, "Network Anomaly Detection by Cascading K-Means Clustering and C.45 Decision Tree Algorithm," Procedia Engineering, Vol. 30, pp. 174 – 182, 2012.

[15] P. B. Natesan and G. Gowrison, "Improving the Attack Detection Rate Intrusion Detection using AdaBoost Algorithm," Journal of Computer Science, Vol. 8, pp. 1041 – 1048, August 2012.

[16] F. H. Nutan, R. O. Abdul and M. S. Faisal, "An Ensemble Framework of Anomaly Detection using Hybridized Feature Selection Approach (HFSA)," SAI Intelligent Systems Conference, pp. 689 – 995, November 2015.

[17] S. Sharma, S. Kumar, and M. Kaur, "Recent Trend in Intrusion Detection Using Fuzzy-Genetic Algorithm," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, April 2014.

[18] S. Selvakumar and A. P. R. Kumar, "Detection of Distributed Denial of Service Attacks using an Ensemble of Adaptive and Hybrid Neuro-Fuzzy Systems", Computer Communications, vol. 36, pp. 303–319, February 2013.

[19] L. Seungmin, K. Hyunwoo and K. Sehun, "Advanced Probabilistic Approach for Network Intrusion Forecasting and Detection. Expert Systems with Applications, Vol.40, pp. 315 – 322, January 2013.

[20] H. Shi-Jinn, S. Ming-Yang, C. Yuan-Hsin, K. Tzong-Wann, C. Rong-Jian, L. Jui-Lin, and C. D. Perkasa, "A Novel Intrusion Detection System Based on Hierarchical Clustering and Support Vector Machines," Expert Systems with Applications, Vol. 38, pp. 306–313, January 2011.

[21] W. Shun-Sheng, Y. Kuo-Qin, W. Shu-Ching and L. Chia-Wei, "An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", xpert Systems with Applications, Vol. 38, pp. 15234 – 152443, December 2011.

[22] S. Siva, S. Sivatha, S. Geetha and A. Kannan, "Decision Tree Based Light Weight Intrusion Detection Using a Wrapper Approach," Expert Systems with Applications, Vol. 39 pp.129–141, January 2012.

[23] M. C. Yang, C. S. Huang, J. H. Chen, and R. F. Chang, "Whole Breast Lesion Detection Using Naive Bayes Classifier for Portable Ultrasound," Ultrasound in Medicine and Biology, Vol. 38, pp. 1870–1880, November 2012.

[24] S. Ming-Yang, "Real-Time Anomaly Detection Systems for Denial-of-Service Wttacks by Weighted K-Nearest-Neighbor Classifiers," Expert Systems with Applications, Vol. 38, pp. 3492 – 3498, April 2011.

[25] H. Yoon, P. Cheong-Sool, K. Jun-Seok and B. Jun-Geol, "Algorithm Learning Based Neural Network Integrating Feature Selection and Classification". Expert Systems with Applications, Vol. 40, pp. 231–41, January 2013.

[26] H. Yung-Tsung, C. Yimeng, C. Tsuhan, L. Chi-Sung and C. Chia-Mei, "Malicious Web Content Detection by Machine Learning," Expert Systems with Applications, Vol. 37, pp. 55-60, January 2010.

Z. Zhang, Q. Zhu, and Y. Xie, "A Novel Image Matting Approach Based on Naïve Bayes Classifier," Intelligent Computing Technology, pp. 433–441, July 2012