International Journal of Computational Intelligence and Informatics, Vol. 4: No. 3, October - December 2014

Analysis of Dimensionality Reduction in Intrusion Detection

Theyazn H Aldhyani
School of Computer Science
North Maharashtra University
Jalgaon, (M.S) India
th0ha0@yahoo.com

Manish R Joshi
School of Computer Science
North Maharashtra University
Jalgaon, (M.S) India
joshmanish@gmail.com

***Abstract*- Intrusion detection system is an important technology in the market sector as well as in the area of research. Intrusion detection is considered a useful security tool that assists in preventing attacker's access to networks or systems. The determination of genuineness of packets is a key issue and various approaches of classification have been presented. The complexity of a classifier is greatly reduced if the numbers of attributes in a data set are reduced.**

Analysis of dimensionality reduction and it is impacting thereof is the objective of our study. An experimental study is carried out to build up a classifier on a standard dataset of network traffic data that includes normal packets and abnormal packets. A rough set theory and information gain approaches are employed to reduce dimensionality of network traffic data set. The features obtained by the rough set theory and information gain are used to train and test the J48 classifier. A comparative analysis of the results obtained a reduced attribute set and original attributes are presented. The results shows that the performance of J48 classifier with the reduced attributes (rough set and information gain) is better, which is at the cost of time

Keyword- Intrusion Detection System, Rough Set Theory, Information Gain, J48 Classifier

I. INTRODUCTION

Network security has become one of the most critical challenges faced by network security communities. Considering the fact that personal, e-commerce, banking and business data being shared on computer networks, security has become one of the major aspects of the internet. Due to rapid development and popularity in information technology, all the connected machines, round the world are becoming the first target for intruders. Moreover, there is no one method to totally protect network against intruders. Hence, network security is identified as the most important problem in subject of securing data. The organization of this paper is as follows: The section II provides detailed description of intrusion detection. Related work is discussed in section III. In the section IV proposed model is discussed. Experimental analysis is presented in section V. In the section VI observations are presented. The comparisons of results are presented in section VII. Finally, section VIII is the conclusion.

II. INTRUSION DETECTION

Anderson in 1980 has been proposed the concept of intrusion detection system (IDS) to attain network security. Intrusion detection system is an essential key of network security. IDS recognize and report the unusual attacks access to secure the networks. Once the intrusion is detected, the system is predictable to alarm the administrators so that corrective and protective action can be possessed. Intrusion detection system is an active area used to identify unauthorized and anomalous behavior in network traffic. Intrusion detection system can be implemented as hardware or software or a set of both that monitors a local system or network against any pernicious activity. The intrusion detection system can be classified as anomaly detection and misuse detection techniques. The misuse detection saves the signatures of identifying attacks in the database and compares new instances with the stored signatures to determine attacks. In addition, anomaly detection learns the normal events of the monitored system and then discovers any difference in it for signs of intrusions. Therefore, anomaly detection techniques can detect new types of intrusion. In this section, we enlist applications and components of intrusion detection system. The detailed description of the IDS is presented in subsequent subsections.

A. Purpose of intrusion detection

a) Analysis and monitoring of local user files and system activity.

b) Intrusion detection system is used to protect and audit of weak points of the network.

c) Ensure the safety of critical system and data files from intruders.

d) Intrusion detection system is hardware or software tool for analysis of activity patterns to discover the matching known attacks.

e) Intrusion detection used to audit and protect the operating system from anomalies.

f) The intrusion detection can detect the viruses, malware, and different types of attacks.

B. Components of Intrusion detection system

There are three main components of intrusion detection system. The description of these three components is as follows.

a) Intrusion Detection System Based Network (IDSBN):

IDSBN use to investigate the information that is captured from the network itself, analyze streams of packets that are passing through the network. Furthermore, The IDSBN checks for intrusion or uneven behavior by testing the contents and header information of all the packets moving over the network. The packets are captured by using tools or sensors.

b) Intrusion Detection System Based Host (IDSBH):

IDSBH uses to evaluate and monitors the information traffic as it flows from a single host and multiple hosts. Moreover, IDSBH targets at collecting information about activity on a particular single system or host. IDSBH employs for monitoring and analyzing information captured from host activities such as system call, application logs, password, file and access list control and host activities.

c) Hybrid Intrusion Detection System (HIDS):

HIDS is a combination of IDSBN and IDSBH for monitoring and analyzing network traffic in terms of network security.

III. RELATED WORK

The intrusion detection has recently increased much attention in network security communities. Large numbers of researchers are reported using data mining approaches. Various researchers have proposed different data mining approaches for detection of genuineness packets.

Neethu [7] presented Naïve Bayes and Principal Component Analysis (PCA) algorithms for intrusion detection. They collected dataset from KDD‟99 cup. Principal Component Analysis obtains the dimensionality reduction of input data. They used a Naïve Bayes approach to analyze datasets into normal and abnormal classes. They observed that the naïve Bayesian network approach achieved better results in terms of false positives in network traffic and it requires less time and lower cast. Yogendra et al. [5] proposed NB and Bayes Net supervised learning algorithm for intrusion detection. They collected dataset from KDD‟99 cup. A dimensionality of the network traffic data set is reduced using the information entropy method. They used Accuracy, Precision, and Recall and F-Measure metrics to evaluate performance of NB, Bayes Net approaches. They compared their result with the RC Staudemeyer result: it is one of the research papers. They shared that their result had better than RC Staudemeyer research paper result. Moreover, a comparative result between NB and Bayes Net is presented. They concluded that the bayes net gave a good performance for intrusion detection.

Yacine et al. [6] introduced two machine-learning algorithms, namely support vector machine (SVM) and decision tree (DT) to detect intrusion in terms of network traffic analysis. The authors collected data set from KDD‟99 cup which contains 24 of attacks. They applied PCA to reduce the dimensionality of the attributes from the entire set of data set. A comparative analysis result between DT with PCA and DT without PCA are presented. They concluded that the DT with PCA achieved little better than DT without PCA. Moreover, they compared between SVM with PCA and SVM without PCA. They shared that SVM with PCA gave good performance. Shailendra et al introduced rough set theory and support vector machine for intrusion detection. They experimented with KDD‟99 cup, which contain 24 attacks. They converted data set from non-numeric value into a numeric value. They applied rough set theory to select most significant attributes from KDD‟99 cup, data set. They experimented with 41 features, 29 features and 6 features from KDD‟99 cup dataset. The accuracy of the SVM approach with different selection attributes is compared. They concluded that when six features selected the SVM approach achieved high accuracy rate. Jashan et al. [3] proposed hybrid model for developing the intrusion detection system by combining C4.5 decision tree and Support Vector Machine (SVM) approaches. They collected data set from KDD‟99 cup. Reduce the dimensionality of a data set of network traffic is used by selecting features methods. They selected 12 attributes between 41 attributes. They applied the hybrid model to detect normal and abnormal classes. A comparative analysis between single approaches and hybrid approaches are presented. They shared that the hybrid approach gives high accuracy and less time to detect intrusion. Ghanshyam et al. [4] proposed increment SVM with RST approaches to detect intrusion. The authors collected data set from KDD‟99 cup. The selection of significant attributes from the network traffic dataset is applied by RST method. Analysis dataset, which already used for training and testing, is used by the increment SVM

method. From data analysis, a comparison between incremental SVM and non-incremental SVM is presented. According to the authors, the incremental SVM approach increased performance for intrusion detection.

Xin Du et al. [8] used K-means clustering data mining technique for intrusion detection. They collected data set from the MIB network with a period. The authors applied information entropy to select most significant attributes from the entire set of dataset. They selected four attributes destination IP, source IP, destination port, and source port. They inserted various types of attacks into the network with interval time. They used K-means clustering data mining to determine normal and abnormal class. They concluded that their approach has given a good performance to select better feature attributes and high accuracy detect rate. Hao Tu et al. [2] proposed binary clustering algorithm and signature extraction for worm defense system. The authors collected real data, which contain the entire header of IP and TCP/DUP/ICMP. The Analysis of IP header to identify suspicious network traffic volume binary clustering algorithm is proposed. They used the computing dispersion method to select most significant attributes from the set of dataset. The position-aware signature extraction based bloom filter method applied to extract the signature with position information to obtain better performance. From the result, they compared their model with Autofocus, NID models. They shared that their model more efficient to analyze network traffic.

IV. PROPOSED WORK

Figure 1 displays a generic model of an intrusion detection system. Firstly, the data is preprocessed by applying rough set theory and information entropy method. These methods are used for reducing the dimensionality of standard network traffic data set. J48 classifier is used for detection of intrusion. Finally, the result of J48 classifier is compared with the original 41 attributes data set and with a reduced data set that obtained by selection feature methods. The detailed description of each step used in the generic model is presented in subsequent subsections.

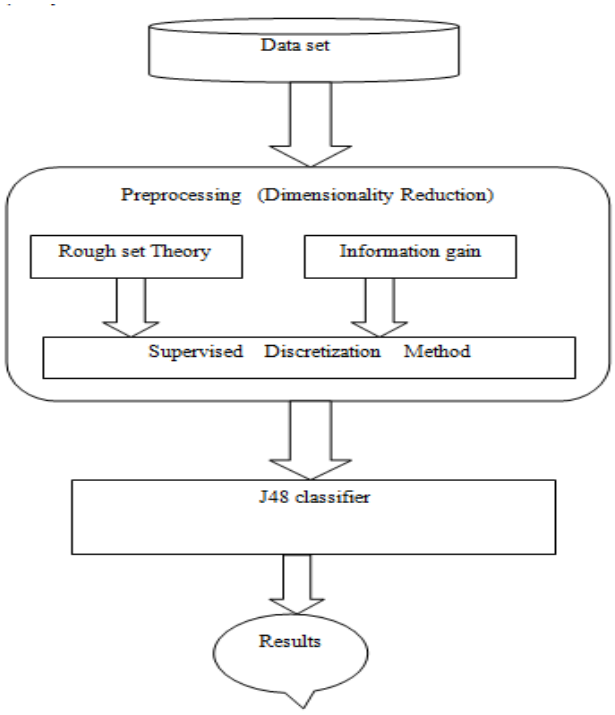

Figure 1. Generic Structure of Proposed Model

A. Data set

We used NSL-KDD intrusion detection data set for experimental purposes. The NSL-KDD dataset contains 41 attributes and 22 types of attacks. The data set contains labels that classify each record as normal or attacks. The attacks report in NSL-KDD data set is divided into four categories is as follows:

a) Denial of Service (DoS)

In the DoS attack, the intruders make server too busy by sending flood of legitimate requests for preventing the local user an access serer. The DoS attacks can have many types such as Neptune, teardrop, smurf, pod, land etc.

b) Remote to Local (R2L)

This attack can rarely happen in the network. In this type of attack, an attacker gets an access into the local user account by sending illegitimate packets into the victim machine over the network. Then, the attackers

become user of that machine. There are different types of R2L attack that are warezclient, warezmaster, multihop, phf, spy, guess_passwd and ftp writes etc.

c) User to Root (U2R)

In this type of attack, an intruder begins to access into the local user of victim machine and then become the root of victim machines. There are various types of U2R attack that are rootkit, Perl, load module and buffer_overflow etc.

d) Probe:

In this type of attack, an attacker can scan the network for collecting information about victim machine. Further, attacker employs this information to attack the victim machine. There are different types of Probe attack, namely: ipsweep, nmap, portsweep and Satan etc.

B. Preprocessing

Preprocessing is data mining technique use to manipulate real world data into an understandable format. Surely, the real world data have been often insufficient and incomplete in specific behavior. Hence, the preprocessing methods are required before applying classification techniques. The preprocessing techniques are vital and important in intrusion detection system due the patterns of network traffic, which have different type of format and dimensionality. In next subsections, we provide detailed descriptions of these methods that are used in our experiment.

a) Feature Selection Methods

The feature selection method uses to reduce the dimensionality of data sets for enhancing the accuracy of data analysis. The rough set theory and information gain methods are presented to select most significant Attributes from NSL-KDD dataset. The detailed descriptions of these methods are presented in next subsections.

b) Rough Set Theory Method

Z. Pawlak is introduced rough set theory in early 1980[14]. Recently, rough set theory is used to study model insufficient and incomplete information and proved useful particularly for machine intelligent system. The Rough Set method is based on the lower and the upper approximation for preprocessing of incomplete data

$Upper\ Approximation: \bar{R} = U\{Y \in U/R : Y \cap X \neq \emptyset\}$

Lower $Approximation: \underline{RX} = U\{Y \in U/R : Y \subseteq X \neq \emptyset\}$

X is roughly B-definable, if $\underline{B}\ (X) \neq \emptyset$ and $\bar{B}(X) \neq \cup$

X is internally B-indefinable, if $\underline{B}\ (X) \neq \emptyset$ and $\bar{B}(X) \neq \cup$

X is externally B-indefinable, if $\underline{B}\ (X) \neq \emptyset$ and $\bar{B}(X) = \cup$

X is totally B-indefinable, if $\underline{B}\ (X) \neq \emptyset\ \ \bar{B}(X) = \cup$ [14].

We applied rough set theory method to extract the significant attributes among 41 attributes from the data set. The rough set theory method was applied by using RSES tool. When Genetic Algorithm was employed, it identified eight significant features out of 41 features. All these features are listed in table1.

TABLE I. EIGHT SIGNIFICANT ATTRIBUTES OBTAINED BY ROUGH SET THEORY METHOD

No	Feature set
1	Duration
2	Services
3	Dst-bytes
4	Count
5	Same-srv-rate
6	Dst-host-srv-count
7	Dst-host-diff-srv-rate
8	Dst-host-some-scr-port-rate

V. INFORMATION GAIN METHOD

The information gain method is used to select the attribute, which contains the highest information for enhancing the classification from the original data set. The computation of the information gain of a set of attributes with respect to all classes calculated as follows. Let S be a set of training set samples with their representing. We consider there are n classes and the training set contains Si samples of class I and S is the total

number of samples in the training set. Thus, required information needed information needed to classify a given sample is calculated by [14].

$$I(S_1, S_2 \ldots S_n) = \sum_{i=1}^{m} \frac{S_I}{S} \; log\; 2\left(\frac{S_I}{S}\right) \quad (1)$$

Feature F with values F_1 , F_2 , …,F_V can divide the training set into v subsets S_1 , S_2 , …, S_V where S_J is the subset which has the value F_J for feature F. Furthermore let S_J contain S_{IJ} Entropy of the feature F is [14].

$$E(F) = \sum_{I=1}^{V} \frac{S_{1_J} + \cdots + S_{M_J}}{S} \; XI\left(S_{1_J} \ldots . S_{M_J}\right) \quad (2)$$

Information gain for F can be calculated as

$$\text{Gain (F)=I(S\_1,}\ldots\ldots \text{├ S\_M)┤ - E(F)} \quad (3)$$

The weka data mining tool was used to apply the Information gain method. After applying the information gain method, 8 attributes were selected that are most significant out of 41 attributes which are listed in table 2.

TABLE II. EIGHT SIGNIFICANT ATTRIBUTES OBTAINED BY AN INFORMATION GAIN METHOD

Rank	Feature set
1.0529431	Diff_srv_rate
1.0453802	Dst-host-diff-srv-rate
1.0323339	Count
1.0189628	Dst_host_srv_count
1.0145247	Src_bytes
1.0092918	Same_srv_rate
0.9829028	Dst-host-same-diff-srv-rate
0.9468344	Flag

c) Supervised Discretization Method

Discretization is a process of mapping the continuous attributes into a nominal attribute. The main objective of the discretization process is to discover a set of cut points, which divide the range into a small number of intervals. Every cut-point is a real value within the range of the continuous values, which splits the range into two intervals one is greater than the cut-point and the other is less than or equal to the cut-point value. Discretization process is an important preprocessing technique for reducing classification time [14]. The supervised method is employed for converting numerical-valued attributes to a nominal-valued attributes in our model. In addition, the utilize the class labels through the discretization process. Discretization is necessary to make NSL-KDD dataset as appropriate input for our experiment. In NSL-KDD data set each connection of the dataset contains 41 attributes. Among 41 attributes there is three (protocol type, service, flag) are non numeric value. So we need discretization method to convert these non numeric values into numeric values. We use weka data mining tool for applying supervised methods the supervised discretization method.We applied supervised discretization method after feature selection methods due to explore the impact of applying J48 classifier with discretization method and without discretization method. There isn"t different if we apply discretization method after feature selection methods. Furthermore, we use supervised discretization for improving the classification time.

d) J48 classifier

J48 classifier is one type of decision tree algorithms. It is an open source Java algorithm implemented in weka data mining tools. The J48 algorithm is updated version of C45 algorithm. It is based on ID3 algorithm that was developed by Ross Quinlan [15]. The j48 classifier uses the concept of information entropy for building decision tree of the training data set. We apply J48 to classify intrusion detection dataset to determine normal and abnormal packets.

VI. EXPERIMENTAL ANALYSIS

We run our experiments on a system with Intel (R) core(TM) 2.40 GHz, i5 2430M CPU and 4 GB RAM running window 7. For all processing are used weka data mining tool. We use benchmark NSL-KDD intrusion detection data set. The original data se contains 18.3 MB data with 1, 25973 instances. In our experiment, we used only 96002 instances. For experimental purpose, we decided to work with three major of attacks namely Neptune, snmpget and Satan. These attacks correspond to 96002 instances out of total 1, 25973 instances.

A. Evaluation metrics

In data mining techniques, many different metrics are used to investigate the classification models. The detection rate, false positive rate, accuracy and time cost metrics are employed for measuring the performance of classifier for different data set. These metrics are using confusion matrix. Each metric is defined as below

Attack detection rate (DR): it is the ratio total number of attacks detected by J48classfier to the total numbers of attacks present in the NSL-KDD dataset. The detection rate is calculated by using equation 4.

$$DR = \frac{Total\ number\ of\ detection\ attacks}{Total\ number\ of\ attacks} * 100\% \quad (4)$$

False positive rate (FPR): it is the ratio of total numbers of incorrect classification by J48 classifier into numbers of normal instances. The false positive rate is computed by using equation 5.

$$FPR = \frac{Total\ number\ of\ misclassified\ processes}{Total\ number\ of\ normal\ processes} * 100\% \quad (5)$$

Accuracy rate (ACR): it is the ratio between the numbers of correct classification by J48 classifier into a number of processes. The computing of accuracy rate is shown equation 6.

$$ACR = \frac{Total\ number\ of\ classified\ processes}{Total\ number\ of\ normal\ processes} * 100\% \quad (6)$$

The detailed description of results obtained when applying J48 classifier with the original data set and with reduced attributes data set is presented in subsequent subsections.

B. J48 classifier with original 41 features

In this subsection, we present the result obtained when applying J48 classifier with 41 attributes original data sets. The result of experiments revealed that, the J48 approach with 41 attributes obtained a good detection rate, false positive rate, and accuracy. However, the main drawback of J48 classifier with 41 features that it consumes more time for building model. The result is described as below:

TABLE III. RESULT OF J48 ALGORITHM WITH ORIGINAL 41 ATTRIBUTES.

Method	Detection Rate (%)	False positive rate (%)	Accuracy (%)	Time (second)
J48 classifier without discretization original data	97.58	3.6	96.94	314.2
J48 classifier with discretization original data	97.40	3.35	96.60	175.6

C. J48 classifier with rough set theory method

We applied J48 classifier with new 8 features selected by rough set theory. Firstly, the supervised discretization method applied to convert numeric attributes to nominal attributes. Then, a comparative analysis of obtaining results between J48 with original 8 attributes and with discretization attributes are presented. We observed that J48 classifier with original 8 attributes an achieved slightly a positive result. However, the time factor required for building the model is more. The experimental results are shown in table 4.

TABLE IV. RESULT OF J48 CLASSIFIER WITH ROUGH SET THEORY

Method	Detection Rate (%)	False positive rate (%)	Accuracy (%)	Time (second)
J48 classifier without discretization	97.55	3.8	96.91	69.46
J48 classifier with discretization	97.50	3.45	96.54	0.21

D. J48 classifier with information gain method

Firstly, we utilized supervised discretization method for converting the continuous attributes to discrete attributes. Then, a comparative analysis of results obtained between J48 algorithm with original 8 attributes and discretization attributes are presented. We noted that the result of J48 algorithm before discretization or after discretization almost same. However, the J48 algorithm with discretization method is better on the cost of time. The results are described in the table 5.

TABLE V. RESULT OF J48 CLASSIFIER WITH INFORMATION GAIN METHOD

Method	Detection Rate (%)	False positive rate (%)	Accuracy (%)	Time (second)
J48 classifier without discretization	96.99	4.73	96.26	68.55
J48 classifier with discretization	97.0	4.75	96.25	0.12

VII. OBSERVATIONS

We observed that dimensionality reduction simplified the classified task. More the numbers of attributes more is the time required for classification. Complexity of classification is also reducing if we can reduce dimensionality of data set. The performance of classification is also hampered due to the reduced attributes.

Moreover, we observe the common features between two reduced attributes dataset obtained using rough set theory and information gain methods. From table1 and table 2, we observed that the four attributes are common between the reducing attribute set. These attributes correspond to the host information. These four attributes have a presence in intrusion detection systems proposed by [11], [12] and [13]. It highlights the significance of these attributes while detecting attacks of Neptune (DoS), Satan (Probe) and Snmpget (U2R) types. The details of these attributes are as follows.

TABLE VI. MOST SIGNIFICANT ATTRIBUTES

Method	Description
Same_srv_rate	Connection to same service
Count	Number of connections to same host
Dst-host-diff-srv-rate	Count of connection has some destination host
Dst_host_srv_count	Count of connection has some destination host

Moreover, from table 4, table 5 and table 3 of empirical result, we apply supervise discretization method for improving classification time. In addition, we realized that the J48 classifier with discretization method gives a positive for reducing the time of building the model. Finally, we observed that accuracy, false positive rate and detection rate result of J48 classifier with original 41 features and selection features (information gain and rough set theory) methods almost same. However, the selection features (information gain and rough set theory) method consume less time for building model. From these reported works, we concluded that a dimensionality pays off in terms of reduced processing time.

VIII. COMPARATIVE ANALYSIS

The Comparison Criteria to evaluate and investigate the generic model of network intrusion detection system are in terms of speed of intrusion detection system and the classification Accuracy. We summarize the results in table 7.

TABLE VII. COMPARISON RESULT OF J48 CLASSIFIER WITH ORIGINAL DATA SET AND WITH SELECTION FEATURE METHODS.

Method	Detection rate (%)	False positive rate (%)	Accuracy rate (%)	Time /second
J48 classifier with original 41 attributes	97.58	3.6	96.94	314.2
J48classifier with rough set theory method				
J48 classifier without discretization	97.55	3.8	96.91	69.46
J48classifier with discretization	97.50	3.45	96.54	0.21
J48classifier with information gain method				
J48classifierwithout discretization	96.99	4.73	96.26	68.55
J48 classifier with discretization	97.0	4.75	96.25	0.12

According to the above table, first we compare J48 with 8 attributes that are generated from selection methods with discretization 8 attribute and without discretization 8 attribute. We explore that the discretization method has positive effects for enhancing the time of classification. Second, a comparative analysis of the results obtained between of 41 original data and dimensionality reduction (rough set theory method and Information gain) approaches is presented. From the Comparison, we concluded that J48 classifier with discretization method perform better to reduce the time of classification. Furthermore, J48 classifier with rough set theory and information gain methods is better due time consumes to build the model is very less.

IX. CONCLUSION

We employ rough set theory and information gain methods for extracting relevant attributes from the dataset. The evaluation metrics are utilized with respect to investigating the performance of J48 classifier. From the experimental result, a comparative analysis of the results obtained with reduce attribute set (using rough set theory and Information gain approaches) and with original attributes is presented. The results shows that the J48 classifier with the rough set and information gain preprocessing approaches performs better, which is at the cost of time. We observed that with reduced attribute the classifier resulted in almost same accuracy of classification.

However, the dimensionality pays off in terms of reduced processing time. Furthermore, we have successfully concluded that the discretization method assist to improve time for building model.

REFERENCES

[1] Y. Bouzida, F. Cuppens, N. Cuppens-Boulahia and S. Gombault "Efficient Intrusion Detection Using Principal Component Analysis" Departement RSM GET/ ENST Bretagne 2, France.

[2] H.Tu, Z. Li, B. Liu "Mining Network Traffic for Worm Signature Extraction" IEEE, 2008.

[3] J. Koshal, M. Bag " Cascading of C4.5 Decision Tree and Support Vector Machine for Rule Based Intrusion Detection System" Computer Network and Information Security, vol. 8, pp. 8-20, 2012.

[4] G. P.Dubey, N. Gupta, R. K Bhujade "A Novel Approach to Intrusion Detection System using Rough Set Theory and Incremental SVM" .International Journal of Soft Computing and Engineering IJSCE 2231-2307, vol. 1, 2011.

[5] Y.Kumar Jain, Upendra "Intrusion Detection using Supervised Learning with Feature Set Reduction" International Journal of Computer Applications, vol. 33– No.6, 2011.

[6] S.K. Shrivastava and P.Jain "Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine"International Journal of Computer Applications, vol 18–No.3, 2011.

[7] B. Neethu "Classification of Intrusion Detection Dataset using machine learning Approaches" International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956.

[8] X. Du, Y. Yang, X. Kang "Research of Applying Information Entropy and Clustering Technique on Network Traffic Analysis" IEEE 2008.

[9] S. K. Shrivastava, P. Jain "Effective Anomaly based Intrusion Detection using Rough Set Theory and Support Vector Machine", vol. 18– No.3., 2011.

[10] http://nsl.cs.unb.ca/NSL-KDD.

[11] A. Zainal, M. Aizaini Maarof and S. M. Shamsuddin "Feature Selection Using Rough Set in Intrusion Detection" IEEE, 2006.

[12] Jeya, P. Gifty; Ravichandran, M.; Ravichandran, C. S." Efficient Classifier for R2L and U2R Attacks" International Journal of Computer Applications; vol. 45, pp. 28, 2012.

[13] M.T. Myo Win, K. Thet Khaing "Analyze knowledge Based Feature Selection to Detection Users to Root and Remote to Local Attack" International Conference on Computer Networks and Information Technology, vol 2, No 5, 2013.

[14] P.Ghosh, C. Debnath, D. Metia3, R. Dutt, "An Efficient Hybrid Multilevel Intrusion Detection SysteminCloud Environment"IOSR Journal of Computer Engineering (IOSR-JCE), vol 16, Issue 4, 2014.

[15] Upendra, "An Efficient Feature Reduction Comparison of Machine Learning Algorithms for Intrusion Detection System" International Journal of Emerging Trends & Technology in Computer Science, vol. 2, Issue 1, 2013.