An Integrating Intrusion Detection Model Using Extreme Learning Machine and Group of classifiers

[1] Rayees Ahmad Sheikh, [2] Aabid Ud Din Wani, [3] Abhishek Bhardwaj

[1] Research Scholar, [2] Research Scholar, [3] Assistant Professor.

[1] Dept. of CSE & IT

CT Group of Institutions,

Jalandhar (Punjab)

Abstract: - There is a fast growth of increasing online systems with these more susceptible chances of intrusions in the systems or the networks can occur. Intrusions are simply intruder gains, or they always in process to gain and broke the systems very well to steal very important and sensitive information. Likewise, replicating databases and running on the pirated software. Their needs to high security models which can achieve maximum accuracy as compared to the existing classifiers. In present and future networks our day by day requirements are basically dependent on the Intrusion detection systems. Many techniques have been traditionally used in Intrusion detection but they are not so providing so much greater accuracy. In recently lot of machine learning algorithms have been used in Intrusion detection. In this paper focus will be on Extreme learning machine it will overcome the issues for large amount of data and large datasets. To study and analyze the performance of existing Intrusion detection techniques with some feature selection techniques and also implement Feature selection with Mutual Information technique and then classify selected features with ELM machine learning technique. Lastly, analyze the performance of proposed MI_ELM technique with the existing Voting technique with respect to accuracy, precision, recall, f-measure and FP rate.

Keywords- Intrusion detection, Extreme Learning Machine, accuracy, Mutual information.

1. INTRODUCTION

Intrusions are activities that in simple terms violate security polices of the networks or systems. Any suspicious activity has been monitored and reports were submitted to a particular system if some bad happens. The mediation of Intrusion detection of a task was recognised by intrusion performance on a system [1]. Intrusion detection have been categorised into mis use [2] and Anamoly based [3] recognition approaches. The network Intrusion detection have a dynamic contribution in surveillances [4]. There are two basic techniques that usually used in Intrusion detection are Misuse/signature based and Anamoly based. The first Misuse diagnosis is significant by with signatures actually intrusion. Attacks which are notorious are detected but unrevealed cannot be detected [5][6][7]. The second technique Anamoly can detect well known and unknown attacks. Anamoly detection can recognize the contemplate deviate tasks from standard convention of attacks [8][9][10]. Therefore, the systems can gain more and much accuracy with a misuse and can cooperate with latest attacks that are suspicious can be easily done by Hybrid in the misuse. Basically, there are several integration of detection systems through sophisticated marked to issue of Anamoly and Misuse [11][12][13]. There are actually much more false positive rates in anomaly detection but presently professional scholars have used many methods to control the drawbacks in anomaly detection. Various efficient standards like SVM [14], Data mining methods [15,16] and Neural networks [17]. Extreme learning machine is specific and latest new data driven tool and a setup of machine learning in which multiple/single layers apply. This is actually second name for multiple or single layer feedforward neural network [18]. There are particular kinds of issues have been solved through the concept of early perceptron and random projection. Also randomly input weights have been given and ELM contains several hidden neurons. It is actually a feedforward network that data goes through series of the layers. Feature selection and mutual information theories are based on and also with alternate two approaches which have been developed [32], [33]. There can be achieving maximum accuracy with intrusion detection with feature selection through mutual information results and reports [34]. In addition to, two techniques for feature selection which have been beneficially proposed for the Intrusion detection [35], [36].

2. Related work:

For creation of Intrusion detection development models by some machine learning methods GA [20], Naive Bayes networks [22], K-nearest neighbour [21], fuzzy logic [23] and decision tree [24]. Thaseen *et* al. [19] have been proposed better crucial features for construction of Intrusion detection and gaining much accuracy. On constitute different learning algorithms the computation time has been reduced very much. The final classifier was taken through majority voting like election protocol. Kausar *et* al. [25] have suggested PCA principal component analysis-based set up for SVM intrusion detection system. The main focus of their work was to have feature possible reduction smoothly with great accuracy by using SVM of the classifiers. Akashdeep *et* al. [26] have proposed the best intelligent system intrusion detection system which have capability to perform correlation and information gain with feature ranking. Zainal *et* al. [27] have proposed the ensemble and sorting of unique class in the model. The techniques are Random forest, LGP, ANFI and Adaptive neural for integrating lot of learning model for maximizing detection. Zhang *et* al. [28] have proposed that the latest compound support of Anamoly detection and misuse detection in a standard way to be integrated. Pietraszek *et* al. [29] have proposed the optimal of the two orthogonal and complementary avenues to reduce the several false positive intrusion detections by data mining and machine learning. Avadhani and Shrinivasu have developed a well intrusion detection form of a group of Neural network and genetic algorithm [30]. Alexandre *et* al. [31] have make an increasing accuracy in Intrusion detection model by multi classifier of a three layer.

3. Research Methodology

3.1 Dataset Collection: The KDD-CUP 99 has been used in containing 49000 relation indexes of 41 attributes. The tanning data is only obtained 10% because data is too much. In network there is an analysis of traffic like anomaly (DOS)and normal of the 41 attributes.

3.2 Data processing management association: Filter the dataset and noise should be removed. It is a data cleaning process with extracting and removing unrelated and unnecessary data.

Data Transfiguration and modification (transformation): It involves the absolute value and it changes into the numeral value. The HTTP, FTP, Telnet etc. Also, these services are containing in the KDD-CUP 99 and TCP as well as UDP as the protocols.

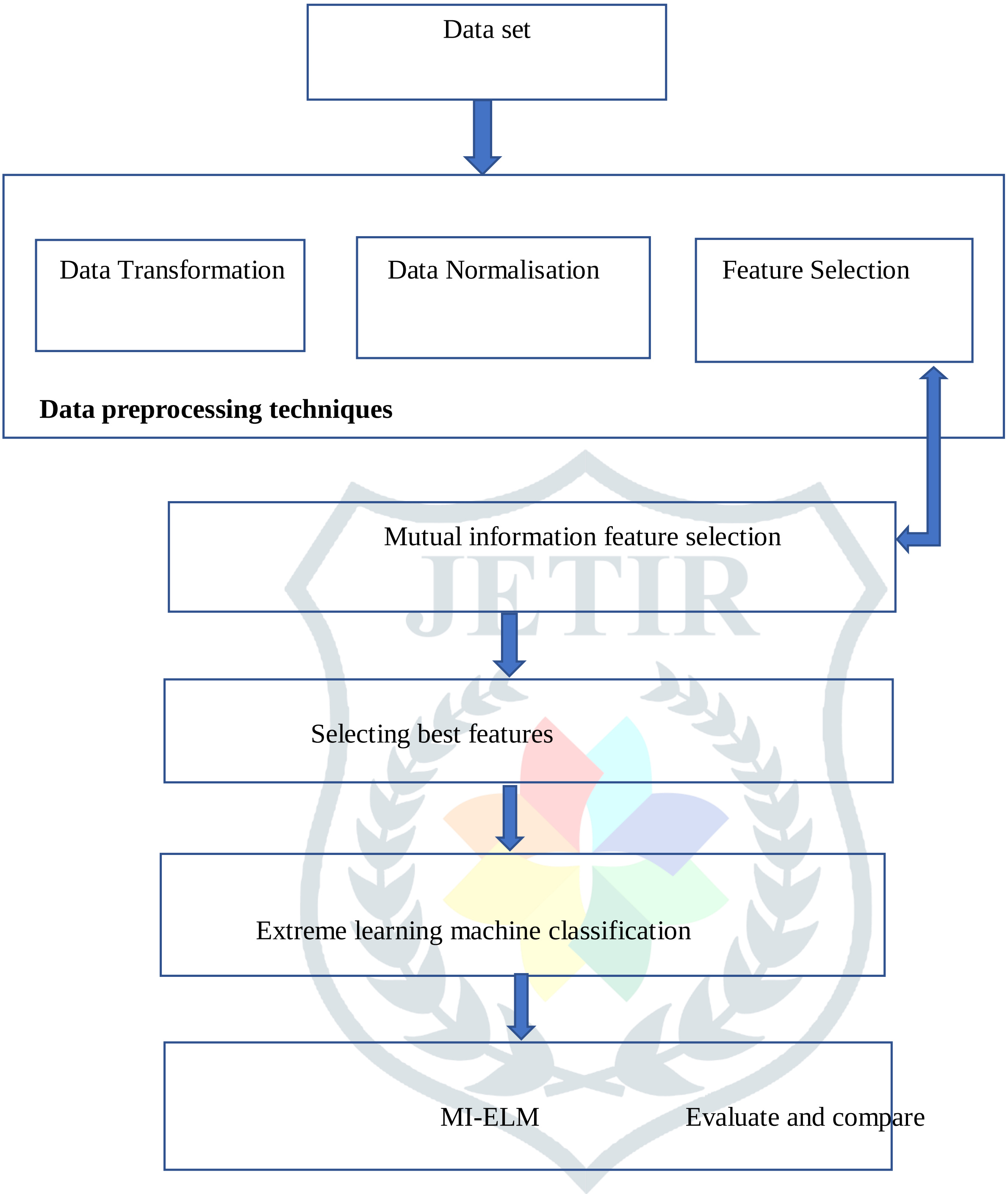
Harmonization and stabilization (Normalization): These are the simply accurate method in which values come in particular domain. The attribute escalade of the new attribute (-1,1) and the (0,1) are recline for connecting or the joining.

Attribute preference (Feature): There are 41 characteristics in dataset of KDD-CUP 99 and all the attributes are totally unrelated with one another to create accurate and efficient model. In short, filter have been used for preferences to recognize related attributes. With help of mutual information 42 characteristics are selected on the basis of ranking.

3.3 Mutual Information (MI) Feature Selection: Collaborative information is an optimal method for a random variable with the mutual dependence or a relation. Transmitted and transferred the quantity dealing in M.I. In brief, defined as transmitted and received amount of information through conditional probability. The Joint entropies are always related to mutual information. In this mutual information it also includes positive values means non negative as well as symmetric and expressed in entropies.

3.4 Classification using ELM: It is a neural network feedforward it indicates data goes through series of one way of layers. The ELM is a specific kind and a neural network-based machine learning expansion in which both multiple and single layers apply. The single feedforward and multiple hidden neural network are the additional name for Extreme learning machine. There is various grouping, non-development, characteristic engineering limitations and the classifications can be easily solved by ELM. In the previous neural networks, the reconciliation of the hidden layer and the input weights are very much tedious of time and in processing costly and also come together with lot of rounds.

Huang et al. have suggested the SLFN to overcome these problems of hidden layer and input weights biases to reduce the tanning time. In complicated data sets it has the capability to do best in very large datasets. The conceptual models can gain more and learn faster than other.



(Fig.1) Intrusion detection proposed model

4.1 Proposed Model

In our proposed model it is very much suitable and efficient for Intrusion detection by integrating Extreme learning machine. The proposed model is implemented on Integrated Intrusion Detection reviews datasets. The data set have network traffic normal as well as abnormal firstly, browsing the data set, Feature selection, Proposed Model, also study and analyse various techniques of IDS. To implement Boosting, SVM, Naïve Bayes and hybrid of these algorithm to detect the intrusion detection system from dataset. To evaluate the performance of the modified work with the existing work using parameters like FP rate, TP rate, Accuracy, F-measure, Recall and precision.

4.2 Experimental Result: In this KDD-CUP99 dataset for the Intrusion detection was designing. The table shows several classifiers of machine learning of the classification. There are different types of parameters have been taken as shown in below table I.

Table I: Detection of Intrusion results

S.no	Parameters	SVM	Naïve Bayes	Boosting	Hybrid	Proposed MI-ELM
1	Accuracy	78.17%	88.57%	90.71%	93.33%	95.63%
2	Correctly classified instances	985	1116	1143	1176	1205
3	Incorrectly classified instances	275	114	117	84	55
4	Kappa statistic	.5594	.77	.81	.86	.9127
6	Precision	.846	.892	.91	.937	.957
7	Recall	.782	.886	.907	.933	.956
8	F-Measure	.813	.889	.648	.938	.956

The performance of the different classifiers of machine learning are compared on the basis of parameters through the confusion matrix. The metrics contains True positive (Tp), True negative (Tn), False positive (Fp) and the False negative (Fn).

4.3 Description Estimation

a) Accuracy: It is one **t**he essential parameter of the measurement of showing presentation of training research study. The actual values are always accurate true or false but the predict values are predicted through algorithm and they vary through confusion matrix.

$$A = \frac{Tp+Tn}{Tp+Fp+Tn+Fn}$$

b) Precision: It is referred as the clearness as well as the exactness. This is the elementary impact of the interpretation on systems and in this case predict values in proportion are always positive.

$$P= \frac{Tp}{Tp+Fp}$$

c) Recall: It is defined as recollection and the estimation of the detection. This recall is also referred as true positive or sensitive.

$$\text{Recall}=\frac{\text{True Positive}}{\text{True Positive}+\text{False Negative}}$$

d) F-Measure: Both Recall and Precision have the harmonic mean in FM for threshold.

F-Measure is preferred when only one accuracy metric is desired as an evaluation criterion.

$$F-\text{Measure}=\frac{2}{\frac{1}{precision}+\frac{1}{recall}}$$

e) Detection Rate: It is calculated as calculation of the ratio with in between total number of intrusions and detection and also correctly classified.

$$\text{Detection Rate}=\frac{\text{True Positive}}{\text{True Positive}+\text{False Negative}}$$

f) False Positive Rate: This indicates number of incorrectly classified number of attacks.

$$\text{False Positive Rate}=\frac{\text{False Positive}}{\text{True Negative}+\text{False Positive}}$$

g) Kappa statistic: It indicates the maximum accuracy that reaches to the 1. The values which near to 1 have higher accuracy like .9, .8 etc.

4.4 A graphical representation of various parameters is listed below:

(i) <u>Accuracy:</u>

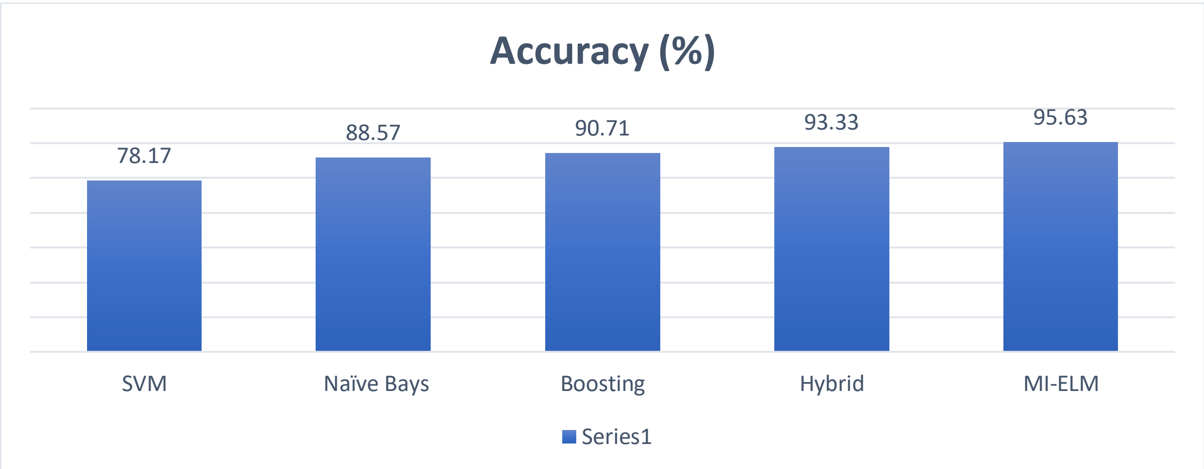


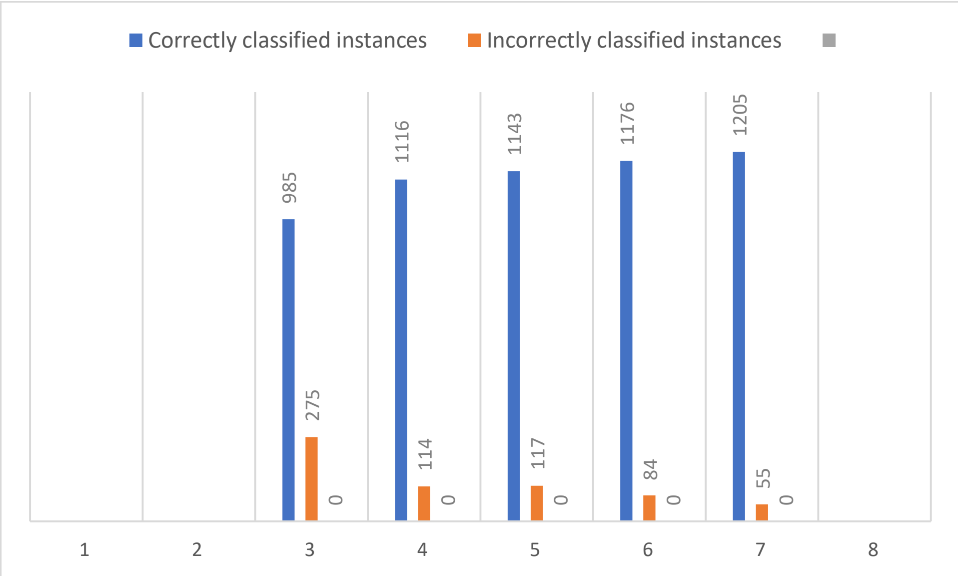
Fig.2

The graph shows a comparative study of results of various classifiers and technique with respect to the accuracy.

Observation:

It was found that the proposed technique (MI-ELM) showed the highest accuracy, 95.63% among the selected classifiers.

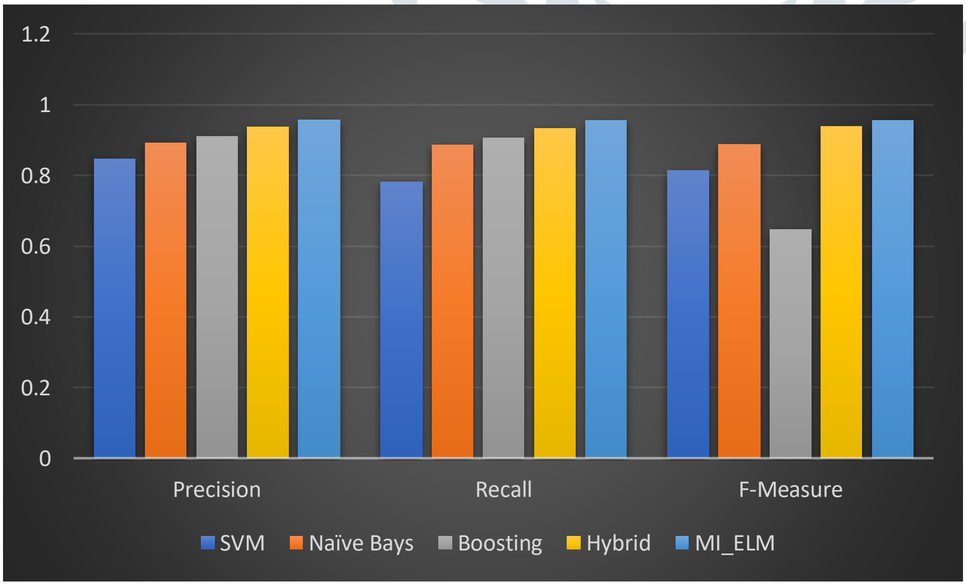
(ii) Correctly classified instances and Incorrectly classified instances:



(Fig.3)

The figure shows that the both correctly classified and the Unclassified instances values are obtained through the sum of the diagonal elements in the confusion matrix.

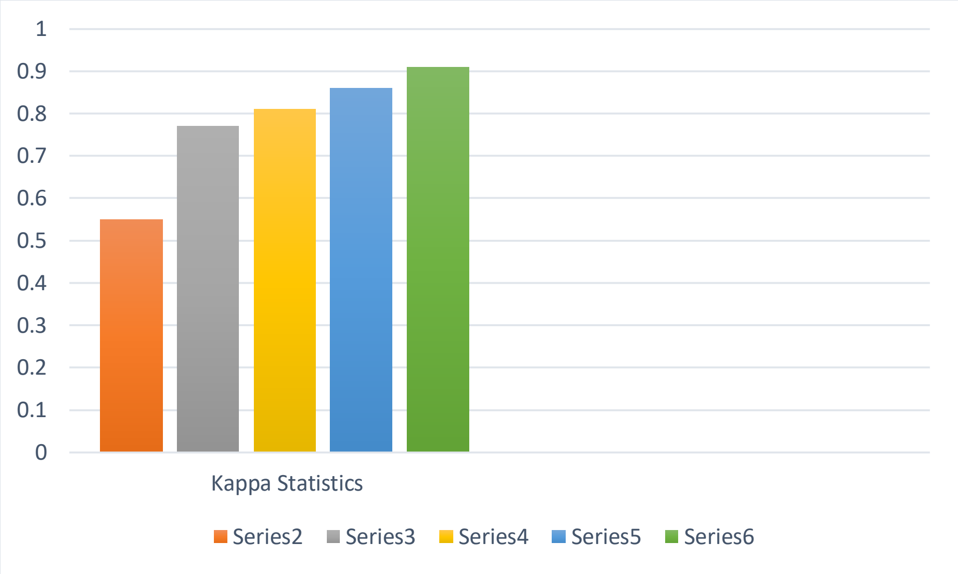
(iii) Precision, Recall and F-Measure:



(Fig.4)

The parameters have taken in fig.4 Precision, Recall and the F-Measure of the classifiers of SVM, Naïve Bayes, boosting, Hybrid and MI-ELM. In all cases, MI-ELM shows maximum and nearly approaches to 1.

(iv)Kappa Statistic:



(Fig.5)

In series6 the graph shown nearly reaches more in MI-ELM. The values .55, .77, .81, .86 and .91 in this .91 among these comes near to 1. So, it means .91 has maximum accuracy.

5. Conclusion

Intrusions are attacks that enters into the systems without any kind of permissions to destroys the systems. Intrusion detection are used for analyzing the systems for something intruders to diagnosis and provides proper reports to a third party. There is a KDD data set and in this data set network traffic analysis is its normal traffic as well as abnormal. In this we are using Extreme Learning Machine technique with grouping of some classifiers. Our experimental results have shown maximising accuracy when we have made a comparison of existing classifiers with proposed techniques. In our research we have integrating separate classifiers like MNB, LP Boosting and the Support vector machine (SVM) model for Intrusion detection. The performance of Nsl-Kdd dataset has analyzed Intrusion dataset through DARPA benchmark. The proposed model has merits of showing much increased accuracy and best truism when combining with many of the classifiers.

REFERENCES

[1] S. T. Sobh, "Anomaly detection based on hybrid artificial immune principles," Information Management & Computer Security, vol. 21, no. 14, pp. 1-25, 2013.

[2] R. M. Rimiru, T. Guanzheng, and S. N. Njuki, "Towards automated intrusion response: A PAMP - based approach," International Journal of Artificial Intelligence and Expert Systems, vol. 2, no. 2, pp. 23-35, 2011.

[3] M. Mehdi, S. Zair, A. Anou, and M. Bensebti, "A bayesian networks in intrusion detection systems," Journal of Computer Science, vol. 3, no. 5, pp. 259-265, 2007.

[4] Carl Endorf, Eugene Schultz, and Jim Mellander, "Intrusion Detection & Pre-vention", McGrawHill/Osborne, 2004.

[5] J. Zhang and M. Zulkernine, "Network Intrusion Detection Using Random Forests", Proc. of the Third Annual Conference on Privacy, Security and Trust, pp. 53-61, St. Andrews, New Brunswick, Canada, October 2005.

[6] Elvis Tombini, Herve Debar, Ludovic Me, and Mireille Ducasse, "A Serial Combination of Anomaly and Misuse IDSes Applied to HTTP Traffic", 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, December 2004.

[7] Wenke Lee and Salvatore J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems", ACM Transactions on Information and System Security (TISSEC), Volume 3, Issue 4, November 2000.

[8] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data", Applications of Data Mining in Computer Security, Kluwer, 2002.

[9] J. Zhang and M. Zulkernine, "Anomaly based network intrusion detection with unsupervised outlier detection", The 2006 IEEE International Conference on Communications, Istanbul, Turkey, June 2006.

[10] Kingsly Leung and Christopher Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters", Australasian Computer Science Conference, Newcastle, NSW, Australia, 2005.

[11] Daniel Barbarra, Julia Couto, Sushil Jajodia, Leonard Popyack, and Ningning Wu, "ADAM: Detecting Intrusions by Data Mining", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security T1A3 1100 United States Military Academy, West Point, NY, June 2001.

[12] Elvis Tombini, Herve Debar, Ludovic Me, and Mireille Ducasse, "A Serial Combination of Anomaly and Misuse IDSes Applied to HTTP Traffic", 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, December 2004.

[13] Debra Anderson, Thane Frivold, and Alfonso Valdes, Next-Generation Intrusion Detection Expert System (NIDES) - A Summary, Technical Report SRICSL-95-07, SRI, May 1995.

[14] Khan, L.; Awad, M.; Thruaisingham, B.: A new intrusion detection system using support vector machines and hierarchical clustering. VLDB J. 16, 507–521 (2007)

[15] Peddabachigiri, S.; Abraham, A.; Grosan, C.; Thomas, J.: Modeling intrusion detection system using hybrid intelligent system. J. Netw. Comput. Appl. 30, 114–132 (2007)

[16] Lee, W.; Stolfo, S.; Mok, K.:A data mining frame work for building intrusion detection mode. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 120–132 (1999).

[17] Wang, G.; Hao, J.; Ma, J.; Huang, L.: A new approach to intrusiondetectionusingartificialneuralnetworksandfuzzyclustering. Expert Syst. Appl. 37, 6225–6232 (2010).

[18] G. B. Huang, H. Zhou, X. Ding and R. Zhang, "Extreme Learning Machine for Regression and Multiclass Classification," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 42, no. 2, pp. 513-529, April 2012.

[19] Thaseen S *et* al. Integrated Intrusion Detection Model Using Chi-Square Feature Selection and Ensemble of Classifiers. Arabian Journal for Science and Engineering 2018, 44(4); 3357-3368

[20] Shafi, K.; Abbass, H.A.: An adaptive genetic-based signature learning system for intrusion detection. Expert Syst. Appl. 36(10), 12036–12043 (2009)

[21] Amor, N.B.; Benferhat, S.; Elouedi, Z.: Naive Bayes vs decision trees in intrusion detection systems. In: SAC'04: Proceedings of the 2004 ACM Symposium on Applied Computing, New York. ACM Press (2004)

[22] Li, Y.; Guo, L.: An active learning based TCM-KNN algorithm for supervised network intrusion detection. Comput. Secur. 26, 459– 467 (2007)

[23] Tsang, C.H.; Kwong, S.; Wang, H.: Genetic fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. Pattern Recognit. 40, 2373–2391 (2007)

[24] Xiang, C.; Yong, P.C.; Meng, L.S.: Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees. Pattern Recognit. Lett. 29(7), 918–924 (2008)

[25] Kausar N *et al*. An Approach towards Intrusion Detection using PCA Feature Subsets and SVM. International Conference on Computer & Information Science (ICCIS) lEEE 2012; 978-1-4673-1938-6/12

[26] Akashdeep et al. A feature reduced intrusion detection system using ANN classifier Expert Systems with Applications (2017); 88: S249–257

[27] Zainal A et al. Ensemble of One-class Classifiers for Network Intrusion Detection System. IEEE (2008); 978-0-7695-3324-7/08

[28] Zhang J et al. A Hybrid Network Intrusion Detection Technique Using Random Forests. Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) IEEE 2006; 0-7695-2567-9/06

[29] Pietraszek T, Tanner A. Data mining and machine learning Towards reducing false positives in intrusion detection. Information Security Technical Report (2005) 10, 169-183

[30] Shrinivasu, P.; Avadhani, P.S.A.: Genetic algorithm-based weight extractionalgorithmforartificialneuralnetworkclassifierinintrusion detection. Procedia Eng. 38, 144–153 (2012)

[31] Balon-Perin, A.: Ensemble-based methods for intrusion detection (2011–2012)

[32] F. Benjamin, K. Ammar, H. C. Nabil, C. Chieh, and P. Greg, "Feature selection based on mutual information for human activity recognition," in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, 2012, pp. 1729-1732.

[33] S. Y. Lee, Y. T. Park, D. Auriol, and J. Brian, "A novel feature selection method based on normalized mutual information," Applied Intelligence, vol. 37, no. 1, pp. 100-120, 2012

[34] A. Fred and A. K. Jain, "Combining multiple clusterings using evidence accumulation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 6, pp. 835-850, 2005.

[35] S. Mukkamala and A. H. Sung, "Feature ranking and selection for intrusion detection systems using support vector machines," in Proc. International Conference on Information and Knowledge Engineering, 2002, pp.503–509

[36] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," Journal of Computers and Security, vol. 24, no. 4, pp. 295–307, 2005.