# A REVIEW OF MACHINE LEARNING METHODOLOGY FOR NETWORK INTRUSION DETECTION

**S. Lingeswari**

*PG Scholar, Department of Computer science Engineering, Pandian Saraswathi Yadav Engineering College, Arasanoor, Tamilnadu, India.*

***Abstract***

*Security is a key issue to both computer and computer networks. Intrusion detection System (IDS) is one of the major research problems in network security. IDSs are developed to detect both known and unknown attacks. There are many techniques used in IDS for protecting computers and networks from network based and host based attacks. Various Machine learning techniques are used in IDS. This study analyzes machine learning techniques in IDS. It also reviews many related studies done in the period from 2000 to 2012 and it focuses on machine learning techniques. Related studies include single, hybrid, ensemble classifiers, baseline and datasets used.*

***Index Terms:*** *Security, Intrusion detection, Machine learning techniques, Classification.*

## Introduction

Internet has become very popular. It is used almost everywhere including all types of business. Data and information are sent and received through internet. Therefore, information security needs to be safeguarded against any intrusion; detection of which has been one of the main problems in this field. Intrusion detection Systems (IDSs) is a software or device that helps to resist network attacks. The goal of IDS is to have defense wall which does not allow such types of attacks. It detects unauthorized activities of a computer system or a network, firstly introduced by Anderson in 1980 [1]. IDS is an active and secure technology which insures confidentiality, integrity, availability and doesn't allow the intruders to bypass the security mechanisms of a network or host [2]. There are two categories of intrusion detection system (IDS) [3]: Anomaly and misuse detection. Anomaly tries normal usage as intrusion, where as misuse uses well-known attacks. All previous techniques of machine learning techniques for IDS from 2000 to 2012 are going to be explained and analyzed for conclusive results and future direction. This paper has been organized as follow. Section 2 has an overview of different machine learning techniques used in IDS. Section 3 analyses related work. Section 4 concludes for future direction.

## Machine Learning Techniques

While analyzing the previous work done on Intrusion Detection System related to machine learning techniques, it comes to fore that there are three main classifiers; Single classifiers, Hybrid classifiers and ensemble classifiers.

Type of classifiers such as single, hybrid and ensemble and their references of publications from 2000 to 2012, are depicted in table1.

## Single Classifiers

The single classifiers are given as under.

**Fuzzy Logic**

It is also known as fuzzy set theory, used for reasoning. Its value ranges from 0 to 1. e.g, raining is a natural event and it can be from slight to violent [4]. It is effective and very potential technique. It deals with human decision making and reasoning. It uses if then else rules. It is used in many engineering applications [5], but mainly in anomaly IDS. It is more effective in port scans and probes involving high resource consumption [6].

**Genetic Algorithms**

It enables computer to have natural evolution and selection [7], and can work with huge population and can pick the superior items. Its choosing capability is based on some performance criteria [8]. It is inspired biologically heuristic search. IDS collects information on traffic then applies the GA and obtains the information which is normal or attack [9].

**Self-Organizing Maps**

Self Organizing Maps (SOM) is unsupervised learning technique and a type of neural network. SOM algorithm can map a high dimension data in two dimension array. It is used for dimension reduction with one input layer and one Kohonen's layer and it maps n-dimensions into two-dimensions. It can self categorize all the inputs providing straight forward methods for data clustering [10].

**K-Nearest Neighbor**

K-nearest Neighbor (k-NN) is very old and simple method to classify samples [11][12]. The K is a very important parameter in creating a K-NN classifier. Changing k value gives different performances. K-NN calculates a rough distance between two different points, being different from inductive approach and it is instance base learning. It searches some input vectors and classifies new instance and by this way finds a k-nearest neighbor [13].

**Support Vector Machine**

Support Vector Machine (SVM) is proposed in [14]. Through support Vector Machine, the efficiency of classification can be enhanced by constructing a hyper plan, the SVM classifies the data into different groups, divides data into two groups; supports vectors and quadratic programming problem [15].

**Artificial Neural Networks**

Artificial Neural Network (ANN) is an information processing unit. It mimics the neurons of a human brain [16]. Multilayer Perception is mostly used in neural network architecture. It is often used in pattern recognition problems. ANN is a classification technique. It is flexible and fast and can analyze the non linear data set with multi-variable [17].

**Decision Trees**

Decision tree (DT) is a simple "if then else rules" but very powerful. It is an important classification algorithm. First we select the attributes and then it is capable of classifying the data. It classifies a sample going through a number of decisions. The first decision helps the second one and it becomes like a tree structure. The classification of sample starts with root node and ends with end node which is also called leaf.

**Table 1 Articles Written for Types of Classifiers.**

| Types of Classifier | Articles Written |
|---|---|
| Single | The references of articles written for single classifiers are as follows. [15, 23, 26, 27,28, 29, 30, 31, 32, 33, 34,35, 36,37,38,39,40,41,42,43,44,45,46,47, 48,49,50,51,52,53,54,55,56,57,58,59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72,73,74,75,76,77,78,79,80,81,82,83, 84, 85, 86, 87, 88, 89, 90, 91, 92] |
| Hybrid | The references of articles written for Hybrid classifiers are as follows. [8,18,30,31,93,94,95,96,97,98,99,100, 101,102,103,104,105,106,107,108,109, 110,111,112,113,114,115,116,117,118, 119,120,121,122,123,124,125,126,127, 128,129,130,131,132,133,134,135,136, 137,138,139,140,141,142,143,144,145, 146, 147, 148, 149, 150] |
| Ensemble | The references of articles written for Ensemble classifiers are as follows. [18, 20, 92, 97, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161] |

Year-wise work done for single, hybrid and ensemble classifiers from 2000 to 2012 is shown in Figure1.

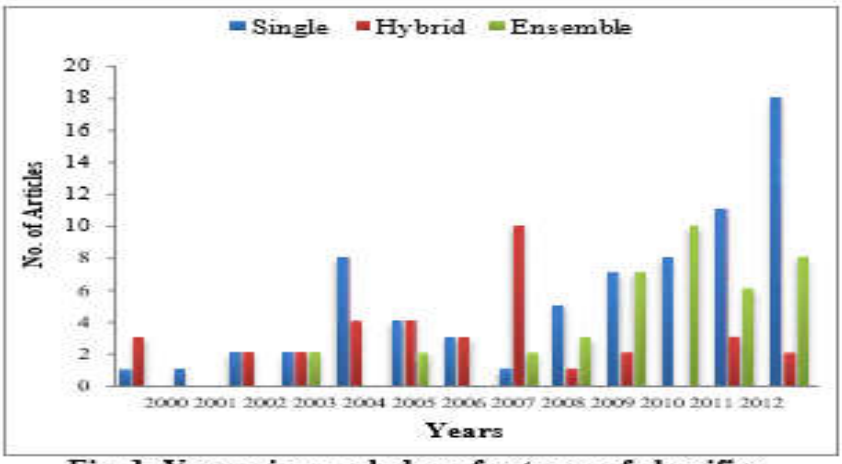


**Fig. 1. Year-wise work done for types of classifier.**

**Table 2 Articles Written for Types of Single Classifiers with Different Categories.**

| Category | Articles Written |
|---|---|
| K-NN | The references of articles written for K-NN are as follows. [31, 34, 35, 43, 45, 82, 162] |
| DT | The references of articles written for DT are as follows. [30, 32, 37, 76, 80, 162] |
| GA | The references of articles written for GA are as follows. [26, 36, 163, 164] |
| Fuzzy Logic | The references of articles written for Fuzzy logic are as follows. [29, 58] |
| SVM | The references of articles written for SVM are as follows. [15,23,28,31,33,37,42,44,47,52,54, 55, 57, 59, 62, 65, 66, 67, 69, 72, 73, 77,79, 84, 85, 86, 89, 90, 91, 117, 158] |
| Bayesian | The references of articles written for Bayesian are as follows. [39, 40, 49, 61] |

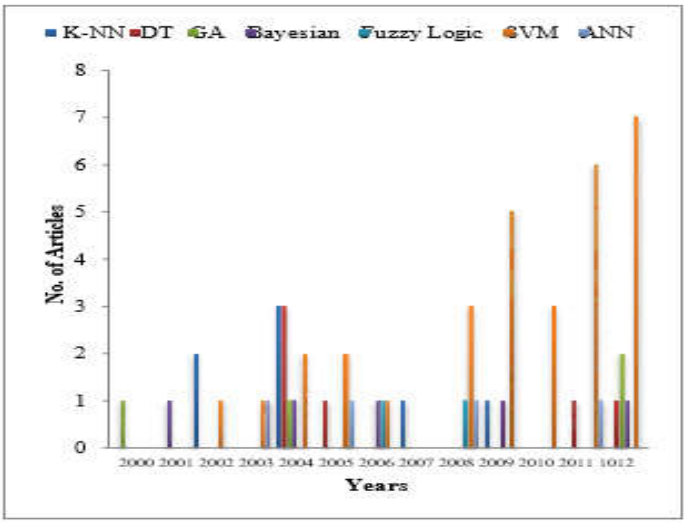


**Fig. 2. Year-wise work done for single classifiers**

**Hybrid Classifiers**

Mostly the work is done to build a better system and therefore, leads to the development of hybrid classifiers for Intrusion Detection System. Hybrid classifiers combine few Machine Learning Techniques to improve system performance for example, DT and GA or K-NN and SVM. This hybrid approach had two sides. The first one takes raw data and produces immediate results and the second one takes this immediate results and produce final results [19].

Hybrid architecture is designed and proved that it can improve the performance [20]. Hybrid approach can help both anomalies and misuse detection [20] to combine Host based Intrusion Detection System (HIDS) and Network Based Intrusion Detection System (NIDS).

Articles written for types of hybrid classifier are shown in table 1 while year-wise work done for hybrid classifier is shown in figure 1 from years 2000 to 2012 is shown in figure3.

**Table 3 Articles Written for Types of Hybrid Classifiers with Different Categories.**

| Category | Articles Written |
|---|---|
| DT, SVM | [18, 133, 143] |
| SOM, DT | [30] |
| Neural network Model (NNM), Asymmetric Cost | [92] |
| Fussy logic (FL), traditional rule based expert system (TRBES) | [93] |
| SVM, linear genetic programmed (LGP), Bees Algorithm(BA) | [94] |
| Evolutionary Algorithm (EA), Swarm Optimizing Algorithm (SOA) | [95] |
| Five different fusion rules | [97] |
| NNM, SOM | [99] |

| | |
|---|---|
| SVM, Clustering Method, Ant Colony Algorithm | [100] |
| SOM, Principle Component Analysis (PCA) | [103] |
| GA, Clustering | [104] |
| PCA, NN | [105] |
| Mining Fuzzy Association Rules, Fuzzy Frequency Episodes | [106] |
| Three layer NN & offline analysis | [107] |
| Classification, Association | [108] |
| FL, Artificial Intelligent (AI) | [109] |
| GA, DT | [111] |
| GA, FL | [112, 150] |
| Three Classifier, Clustering Algorithm | [114] |
| Two Hierarchical Based Framework, Radial Basis Function (RBF) | [115] |
| UCSM | [8] |
| Genetic Fuzzy Systems (GFSs), Pittsburg Approach | [48] |
| Bayesian Network, HMM | [118] |
| PLS, CVM | [119] |
| Immune Genetic Algorithm (IGA) | [120] |
| Noise Reduced Payload Based Fuzzy Support Vector, FSVM | [121] |
| FL, HMM | [122] |
| SVM, Fuzzy Algorithm (FA) | [123] |
| SVM, GA | [124] |
| SOM, K-Means | [125] |
| FSVM, RS | [126] |
| Fuzzy Support Vector Machine | [127] |
| SA, SVM, DT | [128] |
| SVM, RS | [129] |
| SVM, RBFNN | [130] |
| SVM, HM, TSM | [131] |
| KNN, NB | [132] |
| PCA, DT | [134] |
| TASVM | [135] |
| SOM, Artificial Immune System (AIS) | [136] |
| SVM, MLP | [137] |
| GA, NN | [138] |
| GA, KNN | [139] |
| SOM, NN, K-Means | [140] |

| | |
|---|---|
| RBF, Elman Neural Network | [141] |
| K-NN, TAAN | [142] |
| ANN, FC | [144] |
| SVM, DT, Kernel Fisher discriminant Analysis (KFDA) | [145] |
| SVM, FL | [146] |
| DT, Bayesian Clustering | [147] |
| SVM, FCM, PSO | [148] |
| SVM, Artificial Immunization Algorithm | [149] |

**Ensemble Classifiers**

It is used to improve the performance of single classification [21]. Ensemble classifiers combine weak single classifiers and collectively produce a better result [22]. It provides a new and accepted solution for many applications. Table 3 and figure 1 show year-wise work done on Ensemble classification of IDS. Articles written for types of Ensemble classifier are shown in Table 4, while year-wise work done for Ensemble classifier is shown in figure 1 from years 2000 to 2012 is shown in Figure 1.

**Table 4 Articles Written for Types of Ensemble Classifiers with Different Categories.**

| Category | Articles Written |
|---|---|
| SVM, DT | [18, 158] |
| MLP, RBF | [20] |
| Multiple Classifier System (MCS) | [97, 161] |
| GA, FL | [150] |
| HMM, Statistical Rule Based Method (SRBM) | [151] |
| Standard Machine Learning, Clustering Technique | [152] |
| SVM, MARs, ANN | [153] |
| DT | [154] |
| SVC, K-means, Density Estimation | [155] |
| SVM, MK | [156] |
| Improvised GA, Neutrosophic Logic Classifier | [103] |
| Neuro tree | [160] |

**Baselines**

There are different baselines used for validation and are good for evaluation of performance. It also shows how much the capacity of machine is to identify attacks and how many incorrect classifications can occur [23]. Figure 3 shows year

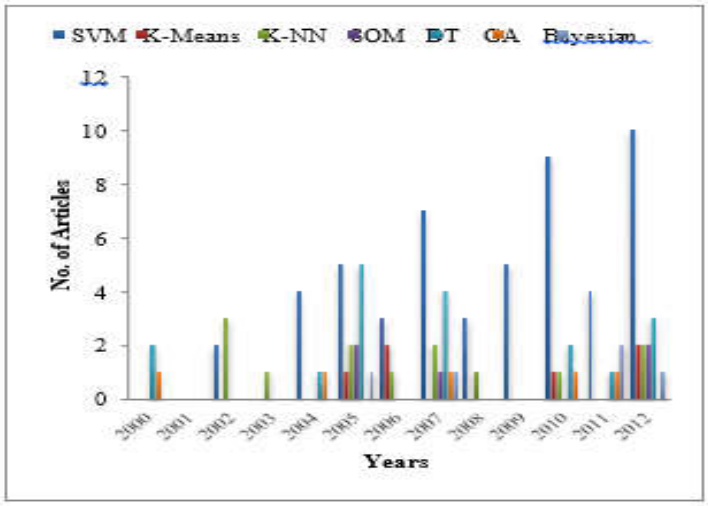


**Fig. 3. Year-wise work done for Baseline classifiers**

**Data Sets**

DARPA1998, DARPA1999 and KDD99 are the data sets, used for classification tasks. KDD99 is the mostly used data set. There are many draw backs of DARPA [24] such as normal attack is not realistic; false alarm behavior cannot be validated. KDD99 dataset is inherited from DARPA and has got the same limitations. These are also validated again [25]. Many people have worked on different datasets used for classifiers. Figure 4 show year-wise work done on datasets from 2000 to 2012. These datasets are publically used and recognized as a standard datasets for IDS. Year-wise work done dataset used from years 2000 to 2012 is shown in figure 4.

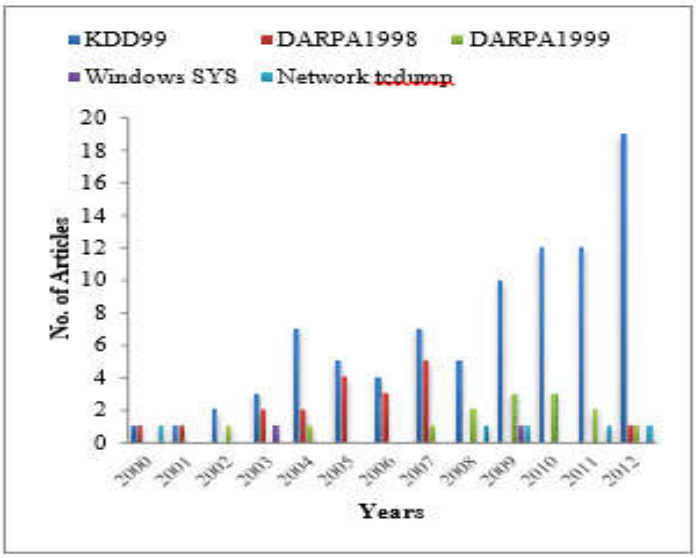


**Fig. 4. Year-wise work done for Datasets used**

**Analysis and Comparison**

The analysis of different articles written on Machine Learning Techniques for IDS with respect to time is discussed as under.

**Table 5: Articles written for types Classifiers.**

| Classifiers/ years | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Single Classifier | 1 | 1 | 2 | 2 | 8 | 4 | 3 | 1 | 5 | 7 | 8 | 11 | 18 |
| Hybrid Classifier | 3 | 0 | 2 | 2 | 4 | 4 | 3 | 10 | 1 | 2 | 0 | 3 | 2 |
| Ensemble Classifier | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 3 | 7 | 10 | 6 | 8 |

**Single Classifiers**

There are many single classifiers but we have selected seven of them. SVM is the most popular single classifier. No of articles written on SVM are 31. It is the maximum number of articles written as compared to other types of articles. Highest numbers of articles are written on SVM in 2009, 20011 and 2012 which is 5, 6 and 7 respectively. Fuzzy logic has a very low focus. Average numbers of articles written for single classifiers are 9.

**Table 6 Articles Written for Types Classifiers.**

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K-NN | | | | | | | | | | | | | |
| DT | | | | | | | | | | | | | |
| GA | | | | | | | | | | | | | |
| Bayesian | | | | | | | | | | | | | |
| Fuzzy Logic | | | | | | | | | | | | | |
| SVM | | | | | | | | | | | | | |
| ANN | | | | | | | | | | | | | |

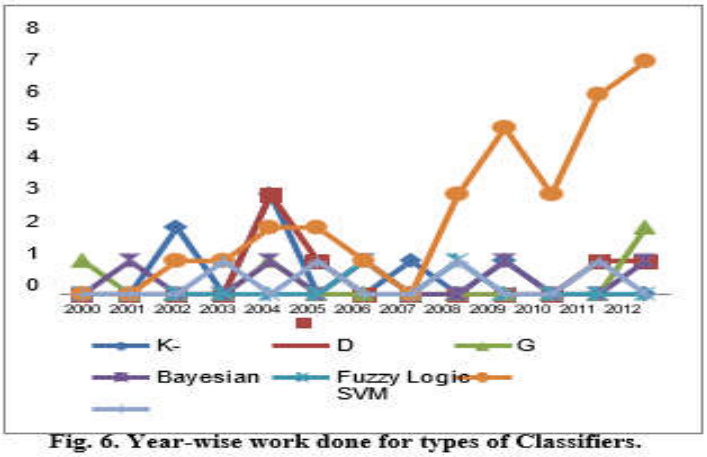


**Fig. 6. Year-wise work done for types of Classifiers.**

**Hybrid Classifier**

E learning techniques used in hybrid classification from year 2000 to 2012 are evaluated here. SVM, GA and DT for hybrid classification are used in 17, 8 and 7 articles respectively. These are also very popular techniques for hybrid classification. Other techniques are normally used.

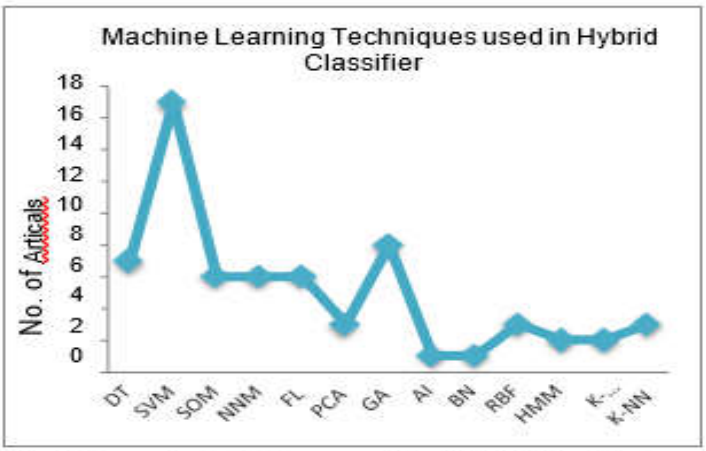


**Fig. 7. Important techniques used in Hybrid Classification.**

**Ensemble Classifier**

SVM is also a popular technique for ensemble classifier. It is mostly used. SVM is used in 4 articles while DT and GA are used in 2 and 2 articles respectively. RBF, FL, HMM, K- means, ANN and SVC are used just once

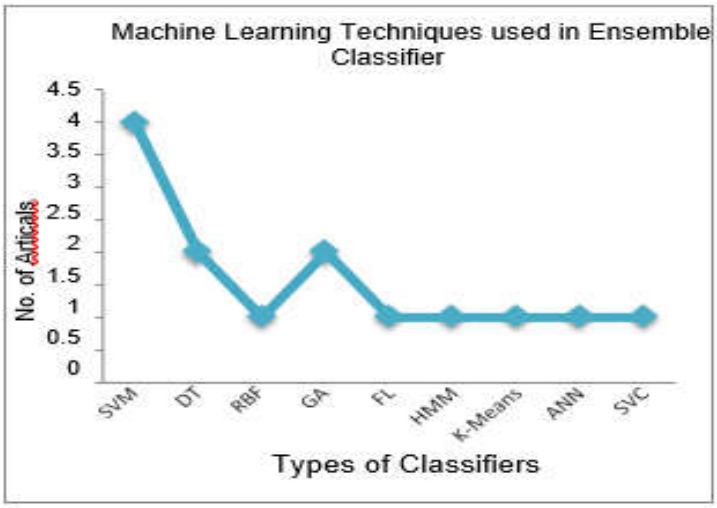


**Fig. 8. Important techniques used in Ensemble Classification**

There are many machine learning techniques used in single, hybrid and ensemble classifiers. SVM is mostly used technique in single, hybrid and ensemble classifiers. After SVM the most popular techniques are GA and DT. SVM is used in 31 articles in single classifier, in 17 articles in hybrid classifiers and in 4 articles in ensemble classifiers. SVM is also combined with other techniques in hybrid and ensemble classifications.

## Conclusion

A lot of work has been done to detect and prevent the Intrusions. There are many machine learning techniques used in Intrusion Detection System and they comprised single, hybrid and ensemble classifiers. Many resources have been used on various machine learning techniques. These techniques work very well for IDS but it is known that there is not even a single technique that can identify all types of attacks. Therefore it still needs more efforts to improve the performance of machine learning techniques to identify all types of attacks and false alarms should be reduced.

There are many classifications but none of them is complete. Hybrid classification is closer one. If we take two or three best single classifiers and improve them a little more and combine them and used it as a single hybrid classifier. False alarm alerts must be reduced and feature selection algorithm should also be improved.

## References

1. J. P. Anderson, “Computer security threat monitoring and surveillance,” technical Report 98-17, James P. Anderson Co., Fort Washing ton, Pennsylvania, USA, April 1980.
2. Mohd. J. Haque, K. W. Magld and N. Hundewale, “An Intelligent Approach for Intrusion Detection Based on Data Mining Techniques,” 2012 International Conference on Multimedia and Systems (ICMCS).

3. C. -F. Tsai, Y. -F. Hsu, C. -Y. Lin and W. -Y. Lin, "IntrusionDetectionby Machine Learning: A Review,"ExpertSystemswithApplication36,2009.
4. H. Zimmermann, Fuzzy set theory and its applications. Kluwer Academic Publishers.2001.
5. A. A. Aburomman and M. B -I. Reaz, "Evolution of Intrusion Detection System Based on Machine Learning Methods", Australian Journal of Basic and Applied Sciences, 7(7): 799-8 13,2013.
6. H. Kaur, G. Singh and J. Minhas, "A Review of Machine Learning Based Anomaly Detection Techniques" International Journal of Computer Applications Technology an d Research volume 2- issue 2, 185-187,2013.
7. J. R. Koza, Genetic p rogramming: On the programming of computers by means of natural selection.Massachusetts:MIT,1992.
8. K. Shafi and H. A. Abbass , "An adaptive genetic- based signature learning system for intrusion detection." Expert Systems w ith Applications, 36(10): 12036-12043,2009.
9. R. Borgohain, "FuGeIDS : Fu zzy Genetic paradigms in Intrusion Detection Systems," International Journal of Advanced Networking and Ap plications, vol. 3, no. 6, pp. 1409-1415,2012.
10. T. Kohonen, "Self-organized formation of topologically correct feature maps," Biological Cybernetics, 43, 59-69, 1982.
11. C. M. Bishop, Neural network for pattern recognition, England, 1995, Oxford University.
12. S. Manocha, and M. A. G irolami, "An empirical analysis of the probabilist c K-nearest neighbor classifier," Pattern Recognition Letters, 28, 1818- 1824.2007.
13. T. M. Mitchell, Machine learning. McGraw Hill, New York, USA, 1997.
14. V. Vapnik, Statistical learning theory, John Wiley, New York, USA, 1998.
15. S. J. Horng, M. Y. Su, Y. H. Chen, T. W. Kao, R. J. Chen, J. L. Lai and C. D. Kara, "A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert Systems with Applications, 38(1): 306-313.2011.
16. S. Haykin, Neural networks: A comprehensive foundation (2nd ed.), Prentice Hall, New Jersey, U.S.A, 1999.
17. H. C. Wu and S. H. S. Huang "Neural networks-based detection of stepping-stone in trusion." Expert Systems with Applications, 37(2): 1431 -1437, 2010.
18. S. Peddabachigari, A. Abraham, C. Gransen and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems." Journal of Network and Computer Applications, 30(1):114-132,2007.
19. M. Govindarajan and R.M. Chandrasekaran, "Intrusion detection using neural based hybrid classification methods," Computer Networks, 55(8): 1662-1671, 2011.
20. J. Kittler, M. Hatef, R. P. W. Duin and J. Matas, "On combining classifiers," IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), 226-239, 1998.
21. F. Majidi, H. Mirzaei, T. Irnapour and F. Faroughi, "A diversity creation method for ensemble based classification: Application in intrusion detection," 2008 7th IEEE International

Conference on Cybernetic Intelligent Systems, CIS'2008.

22. P. Somwang, and W. Lilakiatsakun, "Computer network security based on Support Vector Machine approach," 2011 11th International Conference on Control, Automation and Systems, (ICCAS2011).
23. 2000. "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory." ACM Trans. Inf. Syst. Secur., 3(4): 262- 294.
24. M. Mahoney and P. Chan, 2003. "An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection." Recent Advances in Intrusion Detection. Editor G. Vigna, C. Kruegeland E. Jonsson, Springer Berlin Heidelberg, 2820: 220- 237.
25. B. Balajinathand S. V. Raghavan, "Intrusion detection through behavior model." Computer Communication, 24, 1202-1212.2000.
26. Y. Bouzida, F. Cuppens, N. Cuppens-Boulahia and S. Gombault, "Efficient intrusion detection using principal component analysis," In Paper presented at the proceedings of the 3eme conference surlasecurite et architectures reseaux (SAR). Orlando, FL, USA,2004.
27. W.-H. Chen, S. -H. Hsu, and H. -P. Shen, "Application of SVM and ANN for intrusion detection," Computer and Operations Research, 32, 2617-2634,2005.
28. W. Chimphlee, A. H. Addullah, M. N. M. Sap, S.Srinoy and S. Chimphlee, "Anomaly-based intrusiondetection using fuzzy rough clustering." In Paper presented at the international conference on hybrid information technology (ICHIT'06),2006.
29. O. Depren, M. Topallar, E. Anarim and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, 29, 713-722.2005.
30. E. Eskin, A. Arnold, M. Prerau, L. Portnoy and S. Stolfo, A geometric frame work for unsupervised anomaly detection: Detecting intrusions in unlabeled data. Kluwer,2002.
31. W. Fan, W. Lee, M. Miller, S. J. Stolfo and P. K. Chan, "Using artificial anomalies to detect unknown and known network intrusions," Knowledge and Information Systems, 507-527.2004.
32. W. Fan, W. Lee, M. Miller, S. J. Stolfo and P. K. Chan, "Using artificial anomalies to detect unknown and known network intrusions," Knowledge and Information Systems, 507-527.2004.
33. K. A. Heller, K. M. Svore, A. D. Keromytisand S. J. Stolfo, "One class support vector machines for detecting anomalous window registry accesses," In Paper presented at the 3rd IEEE conference data mining workshop on data mining for computer security. Florida,2003.
34. Y. Liao and V. R. Vemuri, "Use of K-nearest neighbor classifier for intrusion detection," Computer and Security, 21(5), 439-448,2002.
35. Y. Li and L. Guo, "An active learning based TCM- KNN algorithm for supervised network intrusion detection,"ComputerandSecurity,26,459-467,2007.

36. S. Mukkamala, A. H. Sung and A. Abraham, "Modeling intrusion detection systems using linear genetic programming approach," In Paper presented at the proceedings of innovations in applied artificial intelligence, 17th international conference on industrial and engineering applications of artificial intelligence and expert systems (IEA/AIE), Lecture notes in computer science (Vol.3029) , Springer, 2004.
37. Peddabachigari, S., Abraham, A., & Thomas, J. (2004), Intrusion detection System using decision trees and support vector machines. International Journal of Applied Science and Computations.
38. V. Ramos and A. Abraham, "ANTIDS: Self organized ant based clustering model for intrusion detection system," In Paper presented at the proceedings of the fourth IEEE international workshop on soft computing as trans disciplinary science and technology (WSTST'05), Berlin, Springer-Verlag, 2005.
39. M. G. Schultz, E. Eskin, E., Zadok and S. J. Stolfo, "Data mining methods for detection of new malicious executables," In Paper presented at the proceedings of the 2001 IEEE symposium on security and privacy (SP'01),2001.
40. S. L. Scott, "A Bayesian paradigm for designing intrusion detection systems," Computational Statistics and Data Analysis, 45, 69-83,2004.
41. M. Shyu, S. Chen, K. Sarinnapakornand L. Chang, "A novel anomaly detection scheme based on principal component classifier," In Paper presented at the proceedings of ICDM'03,2003.
42. M. Tian, S. -C. Chen, Y. Zhuang and J. Liu, "Using statistical analysis and support vector machine classification to detect complicated attacks," In Paper presented at the proceedings of the third international conference on machine learning and cybernetics. Shanghai,2004.
43. K. Wang and S. J. Stolfo, "Anomalous Payload-based network intrusion detection," In Paper presented at the proceedings of recent advance in intrusion detection (RAID), Sophia Antipolis, France, 2004.
44. W. Wang and R. Battiti, "Identifying intrusions in computer networks with principal component analysis," In Paper presented at the proceedings of the first international conference on availability, reliability and security (ARES'06),2006.
45. W. Wang, X. Guan and X. Zhang, A novel intrusion detection method based on principle component analysis in computer security," In Paper presented at the proceedings of the international symposium on neural networks, Dalian, China,2004.
46. Y. Wang, I. Kim, G. Mbateng and S.-Y. Ho, "A latent class modeling approach to detect network intrusion. Computer Communications, 30, 93-100, 2006.
47. Z. Zhang and H. Shen, "Application of online-training SVMs for real-time intrusion detection with different considerations," Computer Communications, 28, 1428- 1442, 2005.
48. M. S. Abadeh, H. Mohamadi and J. Habibi, "Design and analysis of genetic fuzzy systems for intrusion detection in computer networks," Expert Systems with Applications, 38(6): 7067-7075, 2011.

49. H. Altwaijry and S. Algarny, "Bayesian based intrusion detection system." Journal of King Saud University - Computer and Information Sciences, 24(1): 1-6,2012.
50. F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," Journal of Network andComputerApplications,34(4):1184-1199.2011.
51. X. Arau, R. de-Oliveira, E. -W. Ferreira, A. A. Shinode and B. Bhargara, "Identifying important characteristics in the KDD99 intrusion detection dataset by feature selection using a hybrid approach," 2010 IEEE 17th International Conference on Telecommunications (ICT),2010.
52. R. Ashok, A. J. Lakshmi, G. D. V. Rani, M. N. Kumar, "Optimized feature selection with k-means clustered triangle SVM for Intrusion Detection," 2011 Third International Conference on. Advanced Computing (ICoAC),2011.
53. V. Bolón-Canedo, N. Sánchez-Maroño, A. Alonso- Belanzos, "Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset," Expert Systems with Applications 38(5): 5947-5957.2011.
54. C. A. Catania, F. Bromberg and C. G. Garino, "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection." Expert Systems with Applications, 39(2): 1822-1829,2012.
55. R. C. Chen, K. F. Cheng C. F. Hsieh, "Using Rough Setand Support Vector Machine for Network Intrusion Detection System," Proceedings of the 2009 First Asian Conference on Intelligent Information and Database Systems, IEEE Computer Society, 465-470, 2009.
56. C. Chi, T. Wee-Peng H. Guang-Bin, "Extreme learning machines for intrusion detection," The 2012 International Joint Conference on Neural Networks (IJCNN),2012.
57. G. Chunhua, and Z. Xueqin, "A Rough Set and SVM Based Intrusion Detection Classifier," Second International Workshop on Computer Science and Engineering (WCSE '09),2009.
58. H.F. Eid, A. Darwish A. H. Ella and A. Abraham, "Principle components analysis and Support Vector Machine based Intrusion Detection System," 2010, 10th International Conference on Intelligent Systems Design and Applications (ISDA),2010.
59. D. M. Farid, and M. Z. Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm,"2010.
60. L. Feng, W. Wang, L. Zhu and Y. Zhang, "Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation." Journal of Network and Computer Applications, 32(3): 721-732,2009.
61. Z. Gengming and L. Junguo, "Research of Intrusion Detection Based on Support Vector Machine," International Conference on Advanced Computer Theory and Engineering 2008 (ICACTE '08),2008.
62. S.J. Horng, P. Fan, Y. P. Chou, Y. C. Chang Y. Pan, "A feasible intrusion detector for recognizing IIS attacks based on neural networks." Computers & Security, 27(3-4): 84-100,2008.

63. J. Jiaqi, L. Ru, Z. Tianhangand S. Feigin, “A New Intrusion Detection System Using Class and Sample Weighted C-support Vector Machine,” 2011 Third International Conference on Communications and Mobile Computing (CMC),2011.
64. Y. Jingbo, L. Haixiao D. Shunliand C.Limin, Intrusion Detection Model Based on Improved Support Vector Machine. 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI),2010.
65. Z. Kai-mei, Q. Xu Z. Vu and J. Li-juan, “Intrusion Detection Using Isomap and Support Vector Machine,” AICI '09, 2009 International Conference on Artificial Intelligence and Computational Intelligence, 2009.
66. N.Kausar,B.B.SamirS.B.Sulaiman,I.Ahmadand M. Hussain, “An approach towards intrusion detection using PCA feature subsets and SVM,” 2012 International Conference on Computer & Information Science (ICCIS),2012.
67. L. Koc, T.A. Mazzuchi and S. Sarkani, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier." Expert Systems with Applications, 39(18): 13492-13500, 2012.
68. W. Li, and Z. Liu, "A method of SVM with Normalization in Intrusion Detection." Procedia EnvironmentalSciences11, PartA(0):256-262,2011.
69. Y. Li, J. Xia, S. Zhang, J. Yan, X. Xi and K. Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method." Expert Systems with Applications, 39(1): 424-430, 2012.
70. M. N. Mohammad, N. Sulaiman and E. T. Khalaf, "A novel local network intrusion detection system based on support vector machine." Journal of Computer Science, 7(10): 1560-1564,2011.
71. M.N. Mohammed and N. Sulaiman, "Intrusion Detection System Based on SVM for WLAN," Procedia Technology, 1(0): 313-317,2012.
72. M. S. Mok, S. Y. Sohn and Y. H. Ju, "Random effects logistic regression model for anomaly detection," Expert Systems with Applications, 37(10): 7162-7166, 2010.
73. S. Mukherjee and N. Sharma, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction," Procedia Technology, 4(0): 119-128, 2012.
74. A.P. Muniyandi, R. Rajeswari and R. Rajaram, "Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm,"Procedia Engineering, 30(0): 174-182, 2012.
75. M. Muntean, H. Valean, L. Miclea and A. Incze, “A novel intrusion detection method based on support vector machines,” 2010 11th International Symposium on Computational Intelligence and Informatics (CINTI), 2010.
76. C.R. Pereira, R.Y.M. Nakamura, K.A.P Costa, J.P. Papa, "An Optimum-Path Forest framework for intrusion detectionin computer networks." Engineering Applications of Artificial Intelligence, 25(6): 1226-1234, 2012.

77. S. Saha, A.S. Sairam, A. Yadav and A. Ekbal, “Genetic algorithm combined with support vector machine for building an intrusion detection system,” Proceedings of the International Conference on Advances in Computing, Communications and Informatics. Chennai, India, ACM: 566-572, 2012.
78. P. Sangkatsanee, N. Wattanapongsakorn and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," Computer Communications, 34(18): 2227-2235.2011.
79. N. Sharma and S. Mukherjee, "A Novel Multi- Classifier Layered Approach to Improve Minority Attack Detection in IDS." Procedia Technology, 6(0): 913-921.2012.
80. H. M. Shirazi, "Anomaly Intrusion Detection System Using Information Theory, K-NN and KMC algorithms." Australian Journal of Basic & Applied Sciences, 3(3): 251-2597,2009.
81. S. Suthaharan and T. Panchagnula, “Relevance feature selection with data cleaning for intrusion detection system,” 2012 Proceedings of IEEE Southeastcon, 2012.
82. P. Winter, E. Hermann and M. Zeilinger, “Inductive Intrusion Detection in Flow-Based Network Data Using One-Class Support Vector Machines,” 2011 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2011.
83. Y. Xieand Y. Zhang, “An intelligent anomaly analysis for intrusion detection based on SVM,” 2012 International Conference on Computer Science and Information Processing (CSIP),2012.
84. P. Winter, E. Hermann and M. Zeilinger, “Inductive Intrusion Detection in Flow-Based Network Data Using One-Class Support Vector Machines,” 2011 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2011.
85. Y. Xieand Y. Zhang, “An intelligent anomaly analysis for intrusion detection based on SVM,” 2012 International Conference on Computer Science and Information Processing (CSIP), 2012.
86. D. Xuejun, Z. Guiling, Y. Ke, B. Ma and Z. LI, “High Efficient Intrusion Detection Methodology with Twin Support Vector Machines,” International Symposium on Information Science and Engineering 2008 (ISISE '08), 2008.
87. Y. Yi, J. Wu and W. Xu, "Incremental SVM based on reserved set for network intrusion detection," Expert Systems with Applications, 38(6): 7698-7707, 2011.
88. Z. Yongli, and Z. Yanwei, “Application of Improved Support Vector Machines in Intrusion Detection,” 2010 2nd International Conference on e-Business and Information System Security (EBISS), 2010.
89. J. Yu, H. Lee, M. Kim and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, 31(17): 4212-4219, 2008.
90. S. Zaman, and F. Karray, “Features Selection for Intrusion Detection Systems Based on Support Vector Machines,” 6th IEEE Consumer Communications and Networking Conference 2009 (CCNC 2009), 2009.

91. R. Zhao, Y. Yu and M. Cheng, "An Intrusion Detection Algorithm Model Based on Extension Clustering Support Vector Machine," International Conference on Artificial Intelligence and Computational Intelligence 2009 (AICI'09).
92. D. Joo, T. Hong and I. Han, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors," Expert System with Applications, 25, 69-75.2003.
93. S. M. Bridges and R. B. Vaughn, "Intrusion detection via fuzzy data mining," In Paper presented at the twelfth annual Canadian information technology security symposium. Ottawa, USA, 2000.
94. S. Chavan, K. D. N. Shah and S. Mukherjee, "Adaptive neuro-fuzzy intrusion detection systems," In Paper presented at the in proceedings of the international conference on information technology: Coding and computing(ITCC'04), 2004.
95. Y. Chen, A. Abraham and B. Yang, "Hybrid flexible neural-tree-based intrusion detection systems," International Journal of Intelligent Systems, 22, 337- 352, 2007.
96. G. Florez, S. M. Bridges and R. B. Vaughn, "An improved algorithm for fuzzy data mining for intrusion detection," In Paper presented at the proceedings of the North American fuzzy information processing society conference (NAFIPS 2002). New Orleans, LA, USA, 2002.
97. G. Giacinto and F. Roli, "Intrusion detection in computer networks by multiple classifier systems," In Paper presented at the proceeding of ICPR 2002, 16$^{th}$international conference on pattern recognition, Quebec City, Canada, 2003.
98. S. Y. Jiang, X. Song, H. Wang, J. -J. Han and Q. -H. Li, "A clustering-based method for unsupervised intrusion detections," Pattern Recognition Letters, 27, 802-810, 2006.
99. H. G. Kayacik, Z. -H. Nur and M. I. Heywood, "A hierarchical SOM-based intrusion detection system," Engineering Applications of Artificial Intelligence,20,
100. L. Khan, M. Awad and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," The VLDB Journal, 16, 507-521,2007.
101. W. Lee and S. Stolfo, "Data mining approaches for intrusion detection," In Paper presented at the proceedings of the seventh USENIX security symposium (SECURITY'98), SanAntonio, TX.1998.
102. W. Lee and S. Stolfo, "A framework for constructing features and models for intrusion detection systems," ACM Transactions on Information and System Security (TISSEC), 3(4), 227-261, 2000.
103. G. Liu and Z. Yi, "Intrusion detection using PCASOM neural networks," In Paper presented at the proceeding of ISNN2006. Lecture notes in computer science. Berlin, Heidelberg, 2006.
104. Y. Liu, K. Chen, X. Liao and W. Zhang, "A genetic clustering method for intrusion detection," Pattern Recognition, 37, 927-942.2004.
105. G. Liu, Z. Yi and S. Yang, "A hierarchical intrusion detection model based on the PCA neural networks," Neuro computing, 70, 1561-1568, 2007.

106. J. Luo and S. M. Bridgest, “Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection,” International Journal of Intelligent Systems, 15, 687-703, 2000.
107. M. Moradi and M. Zulkernine, “A neural network based system for intrusion detection and classification of attacks,” In Paper presented at the proceeding of the 2004 IEEE international conference on advances in intelligent systems - Theory and applications, Luxembourg, 2004.
108. T. Ozyer, R. Alhajjand K. Barker, “Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening,” Journal of Network and Computer Applications, 30, 99-113, 2007.
109. T. Shon, X. Kovah and J. Moon, “Applying genetic algorithm for classifying anomalous TCP/IP packets,” Neuro computing, 69, 2429-2433.2006.
110. T. Shon and J. Moon, “A hybrid machine learning approach to network anomaly detection,” Information Sciences, 177, 3799-3821.2007.
111. G. Stein, B. Chen, A. S. Wu and K. A. Hua, “Decision tree classifier for network intrusion detection with GA- based feature selection,” In Paper presented at the proceedings of the 43rd annual Southeast regional conference. Kennesaw, Georgia,2005.
112. A.N. Toosi and M.A. Kahani, “New approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers,” Computer Communication, 30, 2201-2212.2007.
113. C. -H. Tsang, S. Kwong and H. Wang, “Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection,” Pattern Recognition, 40, 2373-2391, 2007.
114. C. Xiang and S.M. Lim, “Design of multiple-level hybrid classifier for intrusion detection system” In Paper presented at the proceeding of the IEEE workshop machine learning for signal processing, 2005.
115. C. Zhang, J. Jiang and M. Kamel, “Intrusion detection using hierarchical neural network,” Pattern Recognition Letters, 26, 779-791,2005.
116. L. -H. Zhang, G. -H. Zhang, L. Yu, J. Zhang and Y.-C. Bai, “Intrusion detection using rough set classification,” Journal of Zhejiang University Science, 5(9), 1076-1086, 2004.
117. B. Agarwal and N. Mittal, "Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques." Procedia Technology, 6(0): 996- 1003, 2012.
118. N. Devarakonda, S. Pamidi, V. V. Kumari and A. Govardhan, "Intrusion Detection System using Bayesian Network and Hidden Markov Model." Procedia Technology, 4(0): 506-514, 2012.
119. X. S. Gan, J. S. Duanmu, J. F. Wang and W. Cong, "Anomaly intrusion detection based on PLS feature extraction and core vector machine." Knowledge- Based Systems, 40(0): 1-6, 2013.
120. S. Ganapathy, K. Kulothungan, P. Vogesh and A. Kannan, "A Novel Weighted Fuzzy C – Means Clustering Based on Immune Genetic Algorithm for Intrusion Detection." Procedia Engineering, 38(0):

121. Z. Guiling, K. Yongzhen, S. Liankun and L. Weixin, "An Improvement of Payload-Based Intrusion Detection Using Fuzzy Support Vector Machine," 2010 2nd International Workshop on Intelligent Systems and Applications (ISA), 2010.
122. X. D. Hoang, J. Hu, and P. Bertok, "A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference." Journal of Network and Computer Applications 32(6): 1219- 1228, 2009.
123. L. Huike and G. Daquan, "A Novel Intrusion Detection Scheme Using Support Vector Machine Fuzzy Network for Mobile Ad Hoc Networks," Second Pacific-Asia Conference on Web Mining and Web- based Application, 2009. (WMWA'09).
124. F. Kuang, W. Xu, S. Zhang, Y. Wang and K Liu, "A novel approach of KPCA and SVM for intrusion detection," Journal of Computational Information Systems, 8(8): 3237-3244, 2012.
125. S. Lee, G. Kim and S. Kim, "Self-adaptive and dynamic clustering for online anomaly detection." Expert Systems with Applications, 38(12): 14891- 14898, 2011.
126. L. Lei, and Z. Ke-nan, "A New Intrusion Detection System Based on Rough Set Theory and Fuzzy Support Vector Machine," 3rd International Workshop on Intelligent Systems and Applications (ISA), 2011.
127. L. Lei, G. Zhi-ping, D. Wen-Yan, "Fuzzy Multi-class Support Vector Machine Based on Binary Tree in Network Intrusion Detection," International Conference on Electrical and Control Engineering (ICECE), 2010.
128. S.W. Lin, K.C. Ying C. Y. Lee and Z. J. Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection." Applied Soft Computing, 12(10): 3285-3290, 2012.
129. Z. Liu, J. Kang and Y. Li, "A hybrid method of rough set and support vector machine in network intrusion detection," 2nd International Conference on Signal Processing Systems (ICSPS), 2010.
130. G. Meijuan, T. Jingwen and X. Mingping, "Intrusion Detection Method Based on Classify Support Vector Machine," Second International Conference on Intelligent Computation Technology and Automation, 2009. ICICTA'09.
131. S.A. Mulay, P.R. Devale and G.V. Garje, "Decision tree based Support Vector Machine for Intrusion Detection," International Conference on Networking and Information Technology (ICNIT),2010.
132. H. Om and A. Kundu, "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system," 1st International Conference on Recent Advances in Information Technology (RAIT), 2012.
133. V.K. Pachghare and P. Kulkarni, "Pattern based network security using decision trees and support vector machine," 3rd International Conference on Electronics Computer Technology (ICECT),2011.
134. M. Panda, A. Abraham and M. R. Patra, "A Hybrid Intelligent Approach for Network Intrusion Detection," Procedia Engineering, 30(0): 1-9,2012.

135. T. Pingjie, J. Rong-an and Z. Mingwei, “Feature Selection and Design of Intrusion Detection System Based on k-Means and Triangle Area Support Vector Machine,” Second International Conference on Future Networks, 2010, ICFN'10.
136. S.T. Powers and J. He, "A hybrid artificial immune system and Self Organising Map for network intrusion detection." Information Sciences, 178(15): 3024-3042, 2008.
137. K. Qazanfari, M. S. Mirpouryan and H. Gharaee, “A novel hybrid anomaly based intrusion detection method,” Sixth International Symposium on Telecommunications (IST),2012.
138. P. Srinivasu and P. S. Avadhani, "Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection." Procedia Engineering, 38(0): 144-153,2012.
139. M.Y. Su, "Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest- neighbor classifiers." Expert Systems with Applications, 38(4): 3492-3498,2011.
140. G. C. Tjhai, S. M. Furnell, M. Papadaki and N. L. Clarke, "A preliminary two-stage alarm correlation and filtering system using SOM neural network and K- means algorithm," Computers & Amp; Security, 29(6): 712-723.2010.
141. X. Tong, Z. Wang and H. Yu, "A research using hybrid RBF/Elman neural networks for intrusion detection system secure model." Computer Physics Communications, 180(10): 1795-1801, 2009.
142. C. F. Tsai, and C. Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection," Pattern Recognition, 43(1): 222-229.2010.
143. J. Visumathi and K. L. Shunmuganathan, "An Effective IDS for MANET Using Forward Feature Selection and Classification Algorithms,"Procedia Engineering, 38(0): 2816-2823, 2012.
144. G. Wang, J. Hao, J. Hao and L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering." Expert Systems with Applications, 37(9): 6225-6232, 2010.
145. Z. Wei, T. Shaohua, Z. Haibin, H. Du and X. Li, “Fuzzy Multi-Class Support Vector Machines for cooperative network intrusion detection,” 9th IEEE International Conference on Cognitive Informatics (ICCI), 2010.
146. C. Xiang, P. C. Yong and L. S. Meng, "Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees." Pattern Recognition Letters, 29(7): 918-924, 2008.
147. F. Xiaozhao, Z. Wei, T. Shaohua and H. Na, “A Research on Intrusion Detection Based on Support Vector Machines,” International Conference on Communications and Intelligence Information Security (ICCIIS), 2010.
148. C. Zhenguo and Z. Guanghua, “Support Vector Machines Improved by Artificial Immunisation Algorithm for Intrusion Detection,” International Conference on Information Engineering and Computer Science, 2009, ICIECS2009.

149. M. S. Abadeh, J. Habibi, Z. Barzegarand M. Sergi, “A parallel genetic local search algorithm for intrusion detection in computer networks,” Engineering Applications of Artificial Intelligence, 20, 1058-1069, 2007.
150. S. -J. Han and S. -B. Cho, “Detecting intrusion with ruled-based integration of multiple models,” Computers and Security, 22(7), 613-623.2003.
151. D. K. Kang, D. Fuller and V. Honavar, “Learning classifiers for misuse and anomaly detection using a bag of system calls representation,” In Paper presented at the proceeding of the 2005IEEE.
152. C. Dartigue, J. Hyun Ik and W. Zeng, A New Data- Mining Based Approach for Network Intrusion Detection,” Communication Networks and Services Research Conference, 2009. CNSR '09. Seventh Annual.2009.
153. G. Giacinto, R. Perdisci, M. D. Rio and F. Roli, "Intrusion detection in computer networks by a modular ensemble of one-class classifiers," InformationFusion,9(1):69-82,2008.
154. S. Guanghui, G. Jiankang, N. Yan, “An Intrusion Detection Method Based on Multiple Kernel Support Vector Machine,” International Conference on Network Computing and Information Security (NCIS), 2011.
155. B. Kavitha, D.S. Karthikeyan and P. S. Maybell, "An ensemble design of intrusion detection system for handling uncertainty using Neutrosophic Logic Classifier," Knowledge-Based Systems, 28(0): 88-96, 2012.
156. Y. Li, J.L. Wang, Z. H. Tian, T. B. Lu and C. Young, "Building lightweight intrusion detection system using wrapper-based feature selection mechanisms." Computers & Security, 28(6): 466-475, 2009.
157. P. A. Rajkumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," Computer Communications, 34(11): 1328- 1341.2011.
158. S. S. S. Sindhu, S. Geetha, A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach." Expert Systems with Applications, 39(1): 129-141, 2012.
159. G. Giacinto, R. Perdisci, M. D. Rio and F. Roli, “Intrusion detection in computer networks by a modular ensemble of one-class classifiers,” Information Fusion, 9, 69-82.2006.
160. L. Breiman, J. H. Friedman, R. A. Olshen and P. J. Stone, “Classification and regressing trees,” California:WadsworthInternationalGroup,1984.