Indian Journal of Science and Technology, *Vol 8(34), DOI: 10.17485/ijst/2015/v8i34/86123, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Integrated Approach for Intrusion Detection using Computational Methods

B. Ben Sujitha[1]* and V. Kavitha[2]

[1]Department of CSE, Ponjesly College of Engineering, Nagercoil – 629003, Tamil Nadu, India; bensujitha@gmail.com
[2]Department of CSE, University College of Engineering, Kanchipuram, Kanchipuram – 631552, Tamil Nadu, India; kavinayav@gmail.com

Abstract

Today's network world is facing lot of challenging task; Intrusion Detection is the method adopted to identify the unauthorised activities in the network. The type of malicious activities grows on increasing. There is very much essential to develop a new Intrusion Detection System, which can detect the malicious activities. The main purpose of our newly hybrid system is developed to identify both known and unknown attack. The proposed system is tested with the benchmark KDD '99 intrusion data set. The proposed work also focuses on the detection rate and false alarm rate. The new system is developed with an optimized algorithm for feature to produce the reduced set of features. The attack detection rate is comparatively good; can be achieved by using layered approach with enhanced fuzzy multi-objective particle swarm optimization which does the feature selection effectively. The fuzzy based support vector machine algorithm is effectively applicable to detect anomaly attack. The newly described system is must more efficient in detection U2R attack, when compared with the existing methods takes long time for training to detect the unknown attack. Also our system is working with very less time for detection. The proposed system with the advantage of detection rate up to 99.1% and the false alarm rate is very much reduced.

Keywords: Attack, Computation, Fuzzy, Goodfit, Intrusion Detection, Objective Function, Optimization, Support Vector Machine

1. Introduction

Internet is the collection of computers connected together. Day by day; there is a steady increase in the number of internet users. The malicious activities are increasing at a high rate day by day. The attack can be spread throughout the world from one device to another device is high rate. So it is very essential to design a system to fight with the malicious activities and determination of those activities. To face the challenge new type of intrusion detection system has been designed.

But the attackers evolve with increased way of doing to overcome the put in safety systems[1]. The types of go into discovery models are and anomaly and misuse[2,3]. A misuse-based have the comparison with the information stored in a knowledge-base. Both within one's knowledge and unknown thing being force into are taken to be using something not regular, not normal careful way. Attacks can be put in order into four groups[4].

1.1 Denial of Service (DoS)

Attacker keeps from taking place given authority from using a public organization, computer or useable thing. The features are Ping of Death, SYN Flood, Smurf, Back, Apache2, Tear drop Land.

1.2 Remote to User (R2L)

Intruder profit way in to the one attacked person host.the features Dictionary, Imap, Named, Sendmail, Ftp_write, Guest.

*Author for correspondence

1.3 User to Root (U2R)

Intruder undesired one going in has nearby way in to the one attacked person machine and gains to profit higher degree user rights. The attributes are Xterm, Perl, Eject, Fdformat Load module, **1.4 Probing (Probe)**.

The host information is gathered by the intruder. The features are Nmap, Mscan, Saint, Ipsweep Satan.

It is very much most important to keep safe the networks from within one's knowledge and unknown attack and also to discover new and unseen attack. There is a most important to build a hybrid system can be used to mark unseen or new attribute as they give to one of the certain classes to every test example. This system can also learn features from all the classes while training is done. In this paper, a new intelligent intrusion detection system has been proposed using hybrid feature selection technique and modified layered approach with generation of new rule which can effectively discover new sort of attack.

In Section 2, discuss about the associated work with highlighting on different methods and frameworks used for intrusion detection. Section 3 covers feature selection technique adopted to improve the efficiency of the system. The Layered architecture[5] in Section 4. In Section 5 deals with fuzzy based Support Vector Machine. The integration of layered approach with fuzzy based SVM is described in Section 6. The results and comparison of the proposed method with other approaches is given in Section 7. It is made observation that the proposed system, layered fuzzy based support vector machine with multi objective particle swarm optimization, acts importantly better than other systems.

2. Related Work

Intrusion Detection System (IDS) are security management system is used to identify anomalous activities and incomplete signatures within computers or networks. The various existing techniques and frameworks are discussed as follows.

Data mining approaches are used for detecting intrusions given by Lee et al. in[6–8]. Data mining approaches are based on construction of classifiers by discovering pertinent patterns of program and user behaviour. Association rules[9] and frequent episodes are used to be train the record patterns. However, mining of features is limited to place to come and go through level of the packet and requires the number of records to be large and meagrely populated; otherwise, they tend to produce a bulky number of rules that increase the complexity of the system[10]. Data clustering methods such as the k-means and the fuzzy c-means have also been applied broadly for intrusion detection[11,12]. Clustering method is based on the calculation of numeric distance between the observations.

Intelligent IDS[13,14] achieve higher detection accuracy done with the intelligent computer programs. It can analyse the environment and acts flexibly. These programs compute the actions and generate the rule by self learning[15]. These systems has the capability for taking self decision. Some method achieves the processing by using uncertain information[16,17].

ANN[18] has the feasibility in learning about the new attack. This approach takes too much of time for training and no provision to give the description of the attack details.

Support Vector Machines[19] map true valued input point vector to a higher to do with measures point space through nonlinear mapping and can make ready at the same time discovery power to do, amount with greatly sized size of facts and used for both type of class such as binary-class and multiclass order. SVM is an oversaw learning careful way used for getting answer to, way out of order and regression questions. More numbers of patterns can be trained using SVM. SVM has high speed, so it has been decided as a best system for intrusion detection. The new system is designed to have good doing work well and high having no error for discovery.

3. Feature Selection

Feature Selection (FS) is the knowledge for computers pre-processing techniques used making out the important features and removing the without relations ones. The importance of feature selection is data perceptive, acquirement of knowledge about the process, data reduction thus there is a reduction in the computation time. The importance of feature selection is knowledge for computers able to see quickly, got by learning of knowledge about the process, facts copies of smaller size thus there is a copies of smaller size in the computation time. The types of feature selection are filter methods[20] and wrapper methods[21]. Filter method can work efficiently with large number of traffic records. The wrapper method identifies the features and evaluate them having highest assessment.

Our proposed system use the Multi Objective Particle Swarm Optimization[22] feature selection method increases

the exactness and speeds up the detection time. This technique encompasses the filter and wrapper approach. The multi-objective PSO has the capability to continue the diversity of swarms, has its flexibility. PSO was originally proposed for solving continuous problems[23].

Multi-objective optimisation involves at the same time optimising two or more contradictory objective functions. In mathematical terms, the formulae for a minimisation problem with multiple objective functions can be written as:

The conditions used to select the optimum features with highest classification accuracy are as follows:

- If Goodfit (xi) = Goodfit (xb) and |xi| < |xb| then xb = xi ; // report the xb of particle i.
- If any Goodfit (xb) = Goodfit (gb) and |xb| < |gb| then gb = xb ; // report the gb of particle i.

3.1 Modified PSO Feature Selection Algorithm

Input: Training data set and Test data set
Output: subset of features

(i) start
(ii) make ready the very small bits position and rate of motion;
(iii) While greatest point iterations is not got to do
(iv) Calculate the goodfit of each particle on the Training set;
(v) For x=1 to XPopulation Size do
(vi) If Goodfit(xi) < Goodfit(xb) then
(vii) xb = xi ; 8. Else if Goodfit (xi) = Goodfit (xb) and |xi| < |xb| then
(viii) xb = Yi ; // Update the xb of particle i
(ix) If any Goodfit (xb) < Goodfit (gb) then
(x) gb = xb ; // Update the gb of particle i
(xi) Else if any Goodfit (xb) = Goodfit (gb) and |xb| < |gb| then
(xii) gb = xb ; // Update the gb of particle i
(xiii) For i=1 to Population Size do
(xiv) Bring to the current state the rate of motion and the position of particle i;
(xv) Determine the classification accuracy of the selected feature subset on the Test set;
(xvi) The position of gb (the selected feature subset) is determined.Based on the iterative search and evaluation procedure as given in our previous work 11 set of important features are selected in the selection process.

4. Layered Approach

The Layer-based Intrusion Detection System (LIDS) proposed by Gupta et al.[24] has the better chances of making certain accessibility, isolation and persons of representative of knowledge for computers. The system is put in an orderly way as level as go into level, which takes to be the same the go into attack with the related point. In that way in each level being like attack are taken to be by training each level not dependently and detailed to the making observation system and also the attack is in the way in the one level. The system has the better chances of copies of smaller size of verification time in the coming after level. Levels act as an apparatus for making liquid clean, which solid mass any anomalous connection and make ready quick move to go into. It is gave effect to with a small group of features for every level rather than using all the 41 points. So the system is being with doing a play getting better during both the training and the testing of the system.

5. Fuzzy based SVM

Support Vector Machines (SVM) is used with a supervised manner[25] to solve the classification problem. The large number of patterns is trained using SVM. Fuzzy Support Vector Machine[26] reduces the training time and improves the efficiency. The scaling process is done in the final step i.e. normalizing all features so that they have zero mean and a standard deviation of 1. This avoids numerical instabilities during the SVM calculation[27]. After the important features are extracted in terms of the values of the parameters Pj, the parsimonious fuzzy rules are applied based on the support vectors $S\{X_s^1\}$, which lies as l = 1 and N_s discovered by the SVM. Figure 1 illustrates the membership function.
The training process is performed as follows:

- Each support vector corresponds to a fuzzy rule. The number of fuzzy rules equals to the number of support vectors;
- Given the i[th] support vector x_s^1; i=1,…,L
  (i) The i[th] fuzzy rule is determined as follows: the MF of fuzzy set for the j[th] input variable in the i[th] rule is:

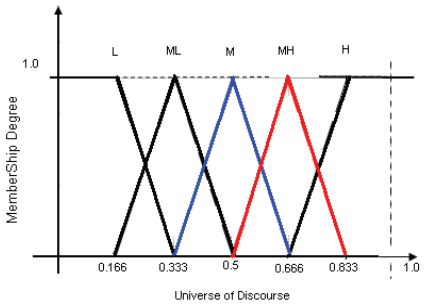

Figure 1. Membership degree.

$$A_i^j(x_j) = a^j(x_j - m_i^j) \quad (1)$$

Where m_i^j is the jth element of the ith support vector x_5^1.

(ii) The i[th] fuzzy rule is induced from α_0 and class labels, i.e., the consequent value of the ith rule is

$$bi = \alpha_0^{(i)} y_s^{(i)} \quad (2)$$

The class I membership of x is given using the minimum operator for:

$$m_i(x) = \min_{j=1.n.} m_{ij}(x) \quad (3)$$

If x is satisfied

$$nD_k(x)\begin{cases} > 0 \ for \ k = i \\ \leq 0 \ for \ k \neq i, k = 1,..n \end{cases} \quad (4)$$

The rule of fuzzy can be selected by the following steps:

- Make out the misclassification rates (MRs) of the rules.
- Initialize s=1 and assume a small value to threshold.i.e. $h_s(h_s > 0)$
- Identify the suitable fuzzy rule by

$$\left\{ Rulei \,|\, \alpha_0^{(i)} \ or \ w_i > h_s \right\} \quad (5)$$

4) Build a fuzzy classifier (FC).
5) Put to use FC for certain dataset 'v' and the test dataset't' to obtain new MRs:Ev (s) .
6) while Ev (s) = Ev (0), end the selection and use FC (s-1) as the final compact classifier and Et(s-1)as the measure of generalization performance for FC (s-1) ; else, s will be incremented by 1, assign a higher value to threshold Th_s, and go to Step 3.

Fuzzy Logic subsequently applying a Support Vector Machine on intrusion and normal rule pool, all possible combinations of rules will be simulated. As in the Figure 2, more number of rules should be generated when there is more generations. On a huge dataset, apply fuzzy logic to avoid the sharp boundary problem. In this module, kinds of attributes i.e. continuous and discrete are used. For continuous attributes like source bytes, duration, destination bytes, find the maximum values for each attributes and then divide these values into Low, Medium and High series and find the fuzzy membership value for each attribute. For discrete attributes, numbers of columns are stable on the basis of types of values for that attribute that is protocol attribute is divided into ICMP, TCP and UDP. The following algorithm displays fuzzy logic implementation for the rule pool.

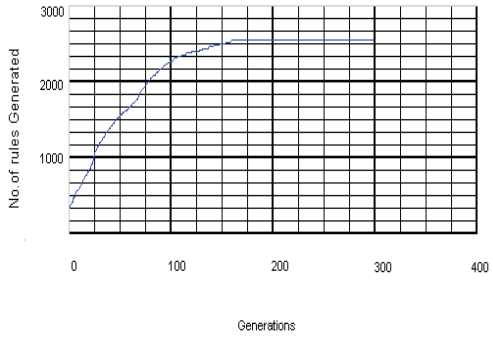

Figure 2. No. of rules generation.

5.1 Algorithm: Fuzzy Rule Extraction

Input: Attack or Normal rule pool.
Output: rule pool contains fuzzy rules

(i) β=the mean value of attribute Ai; γ = the highest value of attribute Ai in the dataset.
(ii) Select features from rule pool.
(iii) Check for missing record for all records.
(iv) Select record from the rule pool.
(v) Process all selected attribute.
(vi) Divide each continuous attribute into HIGH, MEDIUM and LOW.
(vii) Set fuzzy membership value to the continuous feature.
(viii) Estimate membership of fuzzy value for each continuous attribute.
(ix) Divide each discrete attribute into a number of types.
(x) Set binary value for each discrete attribute.

(xi) Store all fuzzy rules in fuzzy rule pool.
(xii) Repeat step 5 until all selected columns are covered.
(xiii) Repeat step 2 until all records in the rule pool is considered.

6. Integrating Layered Approach with Fuzzy based SVM

The Integrated proposed system is given in the Figure 3.

The proposed system is organised as four layers which can be specially designed to identify respective class of attack. Each layer is composed with training phase to identify the attack. The training of the data is done using fuzzy based SVM approach, discussed in Section 5. Support Vector Machine[28] using rule based. The system can work with less number of attributes. Our proposed system can label the attack as well as system is trained with the new data set regularly. The important advantage of our proposed work is challenged by identifying new attacks without any difficulty by generating fuzzy rule automatically based on the decision function and firing strength [29]. Fuzzy rules are ranked based on the importance of induced fuzzy rules, which leads to generate a more parsimonious fuzzy classifier based on R values of fuzzy rules. Also SVM does not need all the attributes of the network packet.

$$f(x) = sig\left(\sum_{i=1}^{m} y_i \alpha_i^n \langle x_i, x \rangle +_x g^* \right) \quad (6)$$

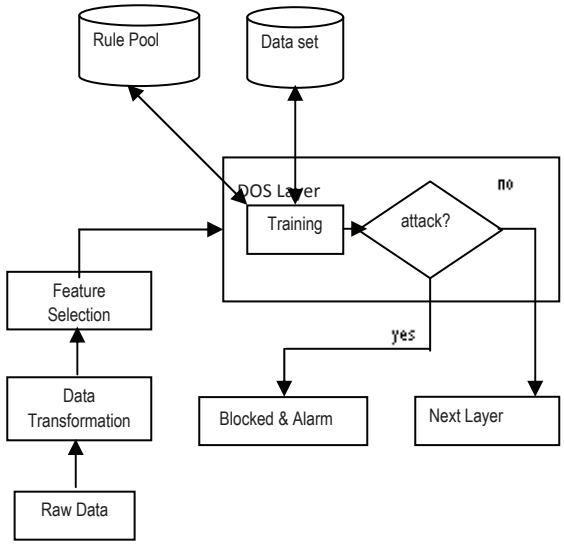

Figure 3. Architecture of proposed model.

This module classifies the attribute as attack or not, based on the vector and the decision is taken by the rules from the rule pool. If the system could not able to identify exactly the parameter is set. Thus the new fuzzy rules are generated. Once the training process is repeated and identification is performed. This approach has the great advantage of reducing false alarm and increase the detection rate. Another advantage of this approach is the process of blocking the identified attack.

7. Experiments

The some of the input features are continuous and discrete stored in the text file. The next process is conversion of continuous attribute to discrete. The normalized features are taken as input for the selection process the features are identified using the F Score measure. The next important step is applying the objective function of the selected feature in the previous step. Finally, the algorithm gives the output of less number of selected features by evaluating the good fit function and the swarm rule. Feature selection is done automatically by MSPSO algorithm. As the result of feature selection only important 11 features have been selected and fed in to the integrated layered approach in which each layer is independently trained to identify a specific type of attack. The benefit of this approach is the system can detect any type of attack. Some of the sample rules are taken from[30]. When the classification takes place if the system finds difficulty to identify the label to mark, then the rule generation process is executed. Once the new rule is generated, which is automatically updated in the rule pool. Also the prescribed data set used for labelling is automatically updated for the next time training. Because of the updating capability, the new proposed system can identify any new type of attack without risk. For the successive classification process, the computation time is so much reduced. The experiment is repeated for 125 times, it is observed the time taken to detect and report is gradually decreased. The first layer is designed to identify DoS attack, which is the stopping the service. The connection level features such as the "duration of connection" and "source bytes" are used in the second layer. The third layer is identifier of R2L attacks are the network level and the host level features. "Duration of connection" and "service requested" is the network level features and the host level features such as the "number of failed login attempts" are selected. The U2R attacks are the content based and target an application. The features such as "number of file

creations" and "number of shell prompts invoked" are chosen for the fourth layer. The most significant benefit of this layered approach is reduced time taken for training. In each layer the features are identified and labelled. If the feature is identified as attack it is blocked and discarded then by prevented to pass to the next layer. The features available as the output of the fourth layer are not attack. As soon as attack is detected, the system raises the alarm or gives alert about the attack.

The classes namely Normal, DoS, Probe, R2L, U2R are used in the test. The testing task is repeated for 125 cycles. It is analysed from the Table 2 and Table 3 the new proposed system has remarkable detection result and reduced rate of false alarm, comparing with other existing system. The Figure 4 and Figure 5 shows the advantage of the proposed method.

Table 2. Detection rate

	DoS	Probe	U2R	R2L
Layered F -SVM	98.9	99.0	96	58
Multi-SVM	96.8	75	5.3	4.2
PN rule	96.9	73.2	6.6	10.7
Layered CRF	97.4	98.6	86.3	29.6
PSO with SVM	97.9	98.6	68.9	19.5

Table 3. False alarm rate

	DoS	Probe	U2R	R2L
Layered F -SVM	0.04	2.75	0.032	0.2
Multi-SVM	0.1	11.7	47.8	35.4
PN rule	0.05	7.5	89.5	12.0
Layered CRF	0.07	0.91	0.05	0.35
PSO with SVM	0.07	3.1	0.05	0.35

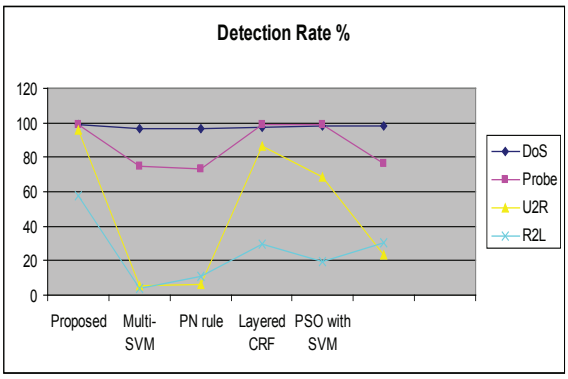

Figure 4. Detection rate.

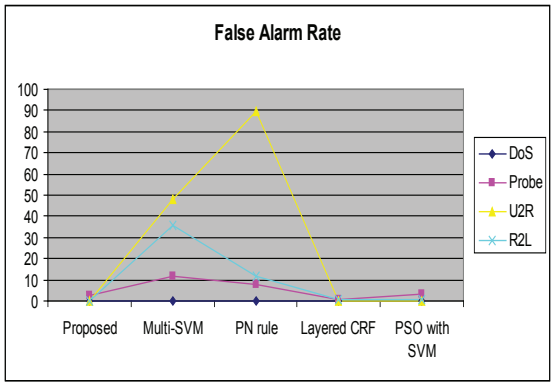

Figure 5. False alarm rate.

8. Conclusion

In this study, MPSO algorithm with discretization is proposed can work with continuous and discrete type of attribute. An efficient objective function with F Score provide classification accuracy rate. This new system can work dynamically to identify the new type of attack. Fuzzy based SVM approach does the classification method using the best selection parameter values and the features in the subset. The new hybrid method has produced good classification and accuracy values. Based on the experiment results the proposed method provides high detection rate and low positive false rate. The important advantage of the new system is the number of features is reduced from 41 to 11, which leads to high detection accuracy (99.1%) and speed up the time to 0.15 sec.

9. References

1. Anderson J. Overview of Attack Trends. An introduction to neural networks. Cambridge: MIT; 2002. Available from: attack_trends.pdf
2. Vokorokos L, Balaz A, Chovanec M. IDS using self organizing map. Acta Electrotechnica et Informatica. 2006; 1(6):1–6.
3. Sung A, Mukkamala S. Identifying important features for intrusion detection using support vector machines and neural networks. Symposium on Applications and the Internet; 2003 Jan 27-31. p. 209–16.
4. Gupta KK, Nath B, Kotagiri R. Network security framework. Int'l J Computer Science and Network Security. 2006 Jul; 6(7B):151–7.
5. Lee W, Stolfo S. Data mining approaches for intrusion detection. Proc Seventh USENIX Security Symp: (Security '98); 1998 Jan. p. 79–94.

6. Johri S. Novel method for intrusion detection using data mining. International Journal of Advanced Research in Computer Science and Software Engineering. 2012 Apr; 2(4):93–6.
7. Lee W, Stolfo S, Mok KI. A data mining framework for building intrusion detection model. Proc IEEE Symp Security and Privacy (SP '99); Oakland, CA. 1999. p. 120–32.
8. Agrawal R, Imielinski T, Swami A. Mining association rules between sets of items in large databases. Proc ACM SIGMOD. 1993 Jun; 22(2):207–16.
9. Tiwari KK, Tiwari S, Yadav S. Intrusion detection using data mining techniques. International Journal of Advanced Computer Technology. 2013; 2(4):21–5.
10. Portnoy L, Eskin E, Stolfo S. Intrusion detection with unlabeled data using clustering. Proc ACM Workshop Data Mining Applied to Security (DMSA): 2001. p. 1–14.
11. Shah H, Undercoffer J, Joshi A. Fuzzy clustering for intrusion detection. Proc 12th IEEE Int'l Conf Fuzzy Systems (FUZZ-IEEE '03): 2003 May 25-28. p. 1274–8.
12. Jaisankar N, Kannan A. A hybrid intelligent agent based intrusion detection system. Journal of Computational Information Systems. 2011; 8:2608–15.
13. Chaudhary A, Tiwari VN, Kumar A. Neuro-fuzzy based intrusion detection systems for network security. Journal of Global Research in Computer Science. 2014 Jan; 5(1):1–2.
14. Aburomman AA, Reaz MBI. Evolution of intrusion detection systems based on machine learning methods. Australian Journal of Basic and Applied Sciences. 2013.
15. Zhang W, Teng S, Zhu H, Du H, Li X. Fuzzy multi-class support vector machines for cooperative network intrusion detection. Proc 9th IEEE Int Conference on Cognitive Informatics (IEEE, Piscataway): Beijing; 2010 Jul 7-9. p. 811–8.
16. Sharma R, Balkishan, Sikka S. Soft computing based intrusion detection system. International Journal of Computer Science and Mobile Computing. 2014; 3.
17. Moradi M, Zulkernine M. A neural network based system for intrusion detection and classification of attacks. Proceedings of IEEE International Conference on Advances in Intelligent Systems – Theory and Applications: (IEEE, Amsterdam), Luxembourg; 2004.
18. Golmah V. An efficient hybrid intrusion detection system based on C5.0 and SVM. International Journal of Database Theory and Application. 2014; 7(2):59–70.
19. Gupta KK, Nath B, Kotagiri R. Conditional random fields for intrusion detection. Proc 21st Int'l Conf Advanced Information Networking and Applications Workshops (AINAW '07): Niagara Falls Ont; 2007. p. 203–8.
20. Chou TS, Yen KK, Network JL. Intrusion detection design using feature selection of soft computing paradigms. International Journal of Computational Intelligence. 2007; 4(3):196–208.
21. Elloumi W, Baklouti N, Abraham A. The multi-objective hybridization of particle swarm optimization and fuzzy ant colony optimization. IOS Press. 2014; 27(1):515–25.
22. Kennedy J, Eberhart R. Particle swarm optimization. IEEE International Conference on Neural Networks; 1995; 4: p. 1942–8.
23. Gupta KK, Nath B, Kotagiri R. Layered approach using conditional random fields for intrusion detection. IEEE Trans Dependable Secure Computing. 2010 Jan-Mar; 7(1):35–49.
24. Begg RK, Palaniswami M, Owen B. Support vector machines for automated gait classification. IEEE Transactions on Biomedical Engineering. 2005 May; 52(5):828–38.
25. Jinbiao Z. Research on intrusion detection system based on clustering fuzzy support vector machine. International Journal of Security and its Applications . 2014; 8(3):249–60.
26. Hasan AM, Nasser M, Pal B, Ahmad S. Support vector machine and random forest modeling for Intrusion Detection System (IDS). Journal of Intelligent Learning Systems and Applications. 2014 Feb; 6(1):45–52.
27. Koshal J, Bag M. Cascading of C4.5 decision tree and support vector machine for rule based intrusion detection system. I J Computer Network and Information Security. 2012 Aug; 4(8):8–20.
28. Pitiranggon P, Benjathepanun N, Banditvilai S, Boonjing V. Fuzzy rules generation and extraction from support vector machine based on kernel function firing signals. World Academy of Science, Engineering and Technology. 2010; 4(8):1209–16.
29. Kadam PU, Jadhav PP. An effective rule generation for intrusion detection system using genetics algorithm. International Journal of Science, Engineering and Technology Research. 2013 Oct; 2(10):2014–8.