Ensemble of Rule Learner and Sequential Minimum Optimization Algorithm for Intrusion Detection System

D. P. Gaikwad, M. M. Swami, S. S. Kolte

***Abstract:** An intrusion detection system is a process which automates analyzing activities in network or a computer system. It is used to detect nasty code, hateful activities, intruders and uninvited communications over the Internet. The general intrusion detection system is struggling with some problems like false positive rate, false negative rate, low classification accuracy and slow speed. Now-a-days, this has turned an attention of many researchers to handle these issues. Recently, ensemble of different base classifier is widely used to implement intrusion detection system. In ensemble method of machine learning, the proper selection of base classifier is a challenging task.*

In this paper, machine learning ensemble have designed and implemented for the intrusion detection system. The ensemble of Partial Decision Tree and Sequential Minimum optimization algorithm to train support vector machine have used for intrusion detection system. Partial Decision Tree rule learner is simplicity and it generates rules fast. Sequential Minimum optimization algorithm is easy to use and is better scaling with training set size with less computational time. Due to these advantages of both classifiers, they jointly used with different methods of ensemble. We make use of all types of methods of ensemble. The performances of base classifiers have evaluated in term of false positive, accuracy and true positive. Performance results display that proposed majority voting method of ensemble using Partial Decision Tree rule learner and Sequential Minimum optimization algorithm based Support Vector Machine offers highest classification among different ensemble classifiers on training dataset. This method of ensemble exhibits highest true positive and lowest false positive rates. It is also observed that stacking of both PART and SMO exhibits lowest and same classification accuracy on test dataset.

***Keywords:** AdaBoost, Bagging, Combination rule, PART, SMO, True positive and False positive*

I. INTRODUCTION

Intrusion detection system is powerful tool which play vital role in protecting the computers and networks. It is used to analyse activities in network or computer for signs of possible results, which are abuse or incomplete threats of abuse of computer security policies, standard security practices or acceptable user policies. It detects malicious code, malicious activities, intruders and unwanted communications over the Internet. Thus, intrusion detection systems have state-of-the-art detection approaches. They are used exclusively in monitoring, analysing, alerting, archiving and reporting. It plays a vigorous role in protecting the modern networks and computers. However; an intrusion detection technology is still immature. Despite the advancements and substantial research efforts, the general intrusion detection system is struggling with some problems like false positive rate, false negative rate, low classification accuracy, slow speed and volumes.

Now-a-days, soft computing techniques, data mining and machine learning algorithms are mostly used in intrusion detection field. This technique has the capability of adaptable information processing for conduct real-life vague circumstances [1]. Specifically, Fuzzy Set and Fuzzy Logic, Artificial Neural Network, Evolutionary Programming and Particle Swarm Optimization techniques are being used to implement intrusion detection system. Researchers have used Support Vector Machines, Radial Basis Function, Linear Discriminant Analysis, Classification and Regression Tree (CART) and Iterative Dichotomise 3 (ID3) for intrusion detection. Rule learner are used to such as RIDOR (Ripple down Rule learner), PART and association rule learning have also used in intrusion detection. For reduction of bias and variance on different training dataset, ensemble of base classifiers is used. This method is also called as hybrid classification. The combination of multiple weak learning algorithms or weak learners is called ensemble [2] [3]. In ensemble, multiple weak classifiers are independently trained and then their predictions are combined in some way to make the overall prediction. This method of combination of base classifiers is a very great and very popular. The ensemble classifiers can be centered on either supervised or unsupervised learning techniques [4] [5]. The ensemble of analogous or dissimilar classifiers can reduce the bias and variance on the different training data set. Lastly, ensemble can also be used to combine two different machine learning classifier using Bagging, Boosting, AdaBoost, Stacking (blending) and voting techniques of ensemble. Providing the strong security mechanism is a great challenge in the field of computer and network security. Intrusion detection system is a very important security mechanism to protect computers and networks. To design and implement a successful mechanism for intrusion

Revised Manuscript Received on December 15, 2019.

* Correspondence Author

Dr. D. P. Gaikwad*, Assistant Professor, Computer Science and Engineering, AISSMS College of Engineering, SPPU Pune, India. E-mail: dp.g@rediffmail.com

M. M. Swami, Assistant Professor, Computer Engineering, AISSMS College of Engineering, SPPU Pune, India. E-mail: mmswami@aissmscoe.com.

S. S. Kolte, Assistant Professor, Computer Engineering, AISSMS College of Engineering, SPPU Pune, India. E-mail: sskolte@aissmscoe.com.

detection system, there is a need of selection of appropriate technique, method of intrusion detection system, and relevant features in training data set.

The irrelevant features in training dataset do not help in increasing the accuracy and unnecessary increase the model building time. Due to high model building time, most of the existing systems cannot deploy on line. To overcome these problems, we have implemented a novel intrusion detection system using Genetic algorithm and ensemble classifiers.

In this paper, the ensemble of PART rule learner and SMO based Support Vector Machine base classifiers have used for intrusion detection system. The Genetic algorithm has used for selection of relevant features from training dataset, which helped to reduce the training time. The rest of the paper is ordered as follows. In Section 2, the literature survey papers are described. Section 3 describes the ensemble classifier. Section 4 discusses the experimental results. Finally, Section 5 is devoted to conclude the paper.

II. LITERATURE SURVEY

Number of attempts has been made to implement intrusion detection systems. In this section, we present some important proposals made by researchers.

Heba Ezzat Ibrahim et.al, [6] have used Naïve Bayes C4.5 and multilayer perceptron to implement intrusion detection system. The proposed intrusion detection system is multilayer. Juvonen and Sipola [7] have proposed online anomaly detection system using un-supervised learning method and combination rule extraction algorithm. The rules are generated by using Conjunctive rule extraction algorithm. Muameret.al, [8] have used data mining and expert system to implement intrusion detection system. The system have implemented in WEKA. Efficiency of detection, overall performance and false positive rate are better than the existing systems. Pandaa et.al, [9] have implemented intrusion detection system unsupervised and supervised learning methods. The system is hybrid intelligent approach for intrusion detection system. Marchetti et.al, [10] have proposed framework for intrusion detection system. It is based on two unsupervised classifier. Pseudo-Bayesian probability correlation and Self-Organizing maps are used to identify the different kinds of multistep attacks. Shrinivasu et.al, [11] have used Genetic Algorithm weight extraction algorithm to extract and improve weights between the neurons of artificial neural network. This GA-NN based intrusion detection is effectively used to identify the intrusions in network. Kumar [12] have implemented ensemble based intrusion detection system. He used boosting method to implement NFBoost ensemble algorithm. The adaptive hybrid Neuro-fuzzy system has used for classification DDoS attacks.

Krawczyk et.al, [13] have used clustering method for intrusion detection system. The clustering method is used to partition training data set. The clusters are used to train a one-class classifier. These classifiers are combined together to implement OCClustE architecture. This proposed OCClustE is used to the formation of a pool of M classifiers for each of the target classes. Chebrolu et.al, [14] have implement system to select significant features from training dataset. He has used Bayesian networks and CART for selection of features and classification. Mukkamalaa et.al, [15] have implemented ensemble method of machine learning using Artificial neural network, SVM and Multivariate Adaptive Regression Splines.

Authors have studied the performances of artificial neural network, Support Vector Machine and Multivariate Adaptive Regression Splines. They observed that the performance of ensemble classifier is superior in the individual's performance. He also studied and addressed different ensemble methods using hard and soft computing techniques. Menahem et.al, [16] have used five base classifier for intrusion detection system. The combination of these base classifiers have suggested for detecting the malware in the network. The five base classifiers from different families of classifiers have used to form ensemble classifier. Liu et.al, [17] have used SVM as a base classifier for implementing ensemble classifier. This new ensemble chaffier is used for learning from imbalanced datasets. It is used with a combination of over-sampling and under-sampling technique. It is used to integrate the classification results of weak base classifiers constructed individually on the processed data. Obimbo [18] have used SOFM based intrusion detection system. This system is ranking system based on SOFM. This system trains many SOFMs separately instead of one for improving precision on classification rate. It also used for increasing classification accuracy by reducing false positive rate on each type of attacks. D P Gaikwad [19] [20] have implemented Ripple down Rule learner for intrusion detection system. The ensemble methods have been used and analyzed to study the performances of individuals.

III. ENSEMBLE AND BASE CLASSIFIERS

In this section, the introduction of base classifiers has given in short. The detail ensemble of these classifier have described in detail.

A. Partial Decision Tree as Base Classifier

There exists many rule learner algorithms of soft computing and machine learning to generate rules from decision trees. The C4.5 and RIPPER are two main schemes for rule learning. Both the schemes operate in two stages. The C4.5 first induces an initial rule set and then refines the rule set using complex optimization stage by discarding the individual rule. RIPPER does the same thing by adjusting individual rules. These two schemes can be combined to produce optimal rule sets. This combination of two schemes of rule learning is called as a Partial Decision Tree (PART). This combined scheme does not require any complex optimization stage. The algorithm to combine C4.5 and RIPPER is very simple, effective and straightforward. This scheme, initially builds decision tree which is pruned to reduce size of tree. This pruned tree is build using current set of instances. The best leaf which gives largest coverage is then transformed in the rule. Then decision tree is castoff by removing cover instances from the training dataset. This process is repeated for all set of instances of the training dataset.

This process is called separate-and–conquer strategy. PART algorithm produces rule sets which are more accurate than RIPPER's rule set.

PART's rule sets are as accurate as C4.5's rule set and the size of rule sets of PART is about of the same size of the C4.5 rule set. The performance of PART is fast because it does not need any post processing [21]. These features of Partial decision tree enable us to select as a base classifier for ensemble

B. Sequential Minimum Optimization algorithm to train Support Vector Machine

The SMO algorithm is row action method which is closely related to Bregman's optimization algorithms [22] [23]. These optimization algorithms are used to solve convex programming problems. The convex problems are solved with linear constraints. In this algorithm, each step plans the present primal point onto each constraint. Algorithms are iterative in nature.

Bregman's algorithm can solve the QP problem without modification. Support vector machine QP problem is solved by using Sequential Minimal Optimization algorithm. It is very simple algorithm that can train Support vector machine problem without any extra matrix storage. It is used to decay the total QP problem into QP sub-problems. Sequential Minimal Optimization is used to solve the smallest possible optimization problem at all steps. To obey a linear equality constraint, Sequential Minimal Optimization algorithm uses two Lagrange multipliers. The benefit of Sequential Minimal Optimization algorithm lies in the fact that solving for two Lagrange multipliers can be done. Using Sequential Minimal Optimization algorithm, very large Support vector machine training problems can fit in memory of computer. Sequential Minimal Optimization algorithm is also used to improve scaling and computation time of Support vector machine [24]. It acts very well on Support vector machines where many of the Lagrange multipliers are at certain. Sequential Minimal Optimization plays well for linear Support vector machines with sparse inputs, even for non-linear Support vector machines. The computation time of kernel can be decreased by directly speeding up Sequential Minimal Optimization algorithm. Chunking Support vector machine learning algorithm applies a majority of its time in the QP code. Chunking Support vector machine learning algorithm cannot take advantages of either the sparseness of the input data or linearity of the Support vector machine. On large problems, the Sequential Minimal Optimization perform well since its scaling with training set size is improved than chunking algorithm. Sequential Minimal Optimization algorithm can be 15 times faster than nonlinear SVM and 1200 times faster than linear SVMs.

C. Proposed Ensemble of base classifiers

In ensemble, initially different base classifiers are constructed using different training datasets. Then, trained base classifiers are combined together using different methods of combination. AdaBoost and Bagging methods work on single base classifier which uses sunsets of training dataset. AdaBoost and Bagging uses different subsets of training datasets for various training. The selection of subsets of training datasets is done using different methods of sampling theorems. In voting method, base classifiers from different family are combined together to take advantages of different classifiers. Different base classifiers are combined in different ways using combination rules. The key condition for an ensemble classifier is that the base classifiers should autonomous to perform better than a single base classifier. For precise classification, choice of base classifier is very vital step in voting ensemble technique.

In this paper, PART rule learner and SMO algorithm have combined together for voting based ensemble using different combination rules. Rule Learners and function based base classifier offer low generalization error and show higher classification accuracy. This was reason for selecting these classifiers as base classifiers. In this paper, NSL_KDD training dataset have used for training ensemble and base classifiers. In ensemble, training datasets D_1 and D_2 are sampled from NSL_KDD dataset D. The size of each dataset is equal in number but distributions of samples are not identical. Each base classifier is constructed using training set D_1 and D_2. The ensemble classifier can be obtained by using unlike combining rules. The equation 1 is used to combine predictions of base classifiers. Base classifiers are combined using different combination rule to predict the class of test sample. The combined voting will result in an ensemble decision for class Ꞷ.

$$C^*(x) = (\text{Combination Rule})\ (C_1(x), C_2(x)). \qquad (1)$$

Following algorithm describes the procedure for combination of base classifiers. This clue is inspired by the general technique of ensemble of multi classifier. The algorithm leads with the division method of the pre-processed NSL_KDD dataset. Base classifiers are trained in parallel using sub training datasets. For finalizing class of test sample, all classifiers are combined using different combination.

Algorithm. Building ensemble classifier.

Input: NSL_KDD training D and testing T datasets.

```
 Begin:
1. Sampling of D1 and $D_2$ datasets
2. Build PART and SMO using $D_1$ and $D_2$.
3. For each t $\epsilon$ T Do
4. C* (t) = Voting Combination Rule ((C1 (t), C2 (t)).
   End. (Where Vote= combination rule (E.g. Majority vote)
```

Output: Ensemble Classifier C*.

IV. EXPERIMENTAL RESULTS

This section describes the performance analysis of intrusion detection system using a rule learner and a function based classifier. In specific, the combination of PART Rule leaner and SMO based SVM have investigated and applied. Initially, the performances of base classifiers have been described in detail. Secondly, ensembles classifier's performances are evaluated in term of false, true positives and classification accuracy. For training and testing, the Intel (R) CORE™ i5-3210M CPU @ 2.50GHz with 8 GB RAM with 64 bit operating is used.

Initially, the intrusion detection systems have implemented using two base classifiers. The performance of base and ensemble classifiers have studied and analyzed on cross validation, training and test datasets. The performance of classifiers have assessed in terms of false positive, classification accuracy and true positive. The classification accuracy on unseen dataset or test dataset is important for classifiers.

Table I shows the performance analysis of each classifier and ensemble classifiers. According to Table I and Fig.1, ensemble of PART and SMO algorithm based SVM using majority voting combination rule exhibits higher accuracy as compared with individual base classifiers. Table II shows the true and false positive values of different base classifiers. According to Table II ensemble using majority voting combination of PART and SMO Algorithm based SVM shows higher true positive rate than individual base classifier on test dataset.

Table- I: Performance analysis of base classifier and ensemble classifiers

Classifier	Training	Cross Validation	Testing
SMO	93.73%	93.73%	72.21%
PART	99.81%	99.66%	77.79%
Majority Voting (Part and SMO)	99.69%	99.50%	78.76%

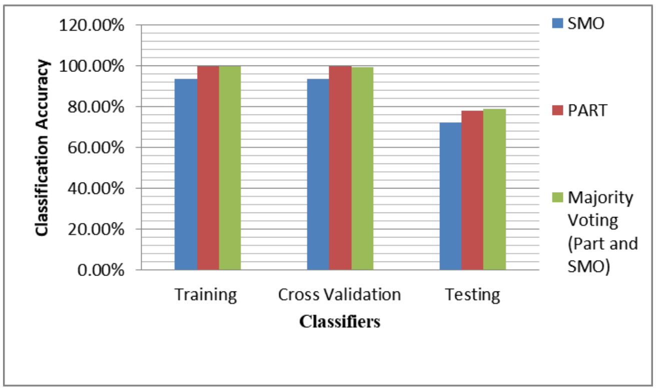

Fig.1. Classification Accuracies of base and ensemble classifiers.

Table- II: Performance analysis of base classifier and ensemble classifiers

Ensemble Classifiers	Training	Cross Validation	Testing
AdaBoost (PART)	99.91%	99.70%	77.79%
Bagging(PART)	99.85%	99.73%	78.67%
Stacking(PART)	53.46%	53.46%	43.08%
AdaBoost(SMO)	93.73%	93.73%	72.14%
Bagging (SMO)	93.73%	93.73%	72.14%
Stacking (SMO)	53.46%	53.46%	43.08%
Random Forest	99.91%	99.59%	77.32%

Secondly, the intrusion detection systems have implemented using different ensemble methods using base classifiers. AdaBoost, Bagging and Voting methods of ensemble using base classifiers have used for intrusion detection system. The Random forest ensemble also have used for the same. The performance of base and ensemble classifiers have studied and analyzed on cross validation, training and test datasets. The performance of classifiers have assessed in terms of true positive, classification accuracy and false positive rates. The classification accuracy on unseen dataset or test dataset is important for classifiers. Table III shows the performance analysis of each ensemble using base classifier and Random forest. According to Table III and Fig. 2, Bagging of PART rule learner offers higher classification accuracy as compared to other ensemble classifiers on test dataset. It shows that Bagging of PART exhibits higher accuracy than other ensemble of SMO based SVM and Random forest on test dataset.

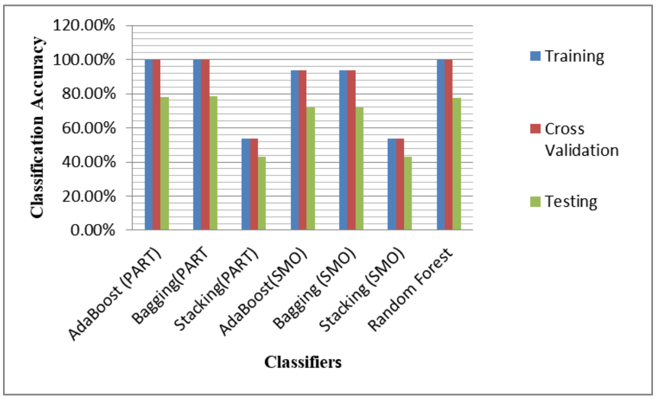

Fig.2. Classification Accuracies of base and ensemble classifiers.

According to Table IV, Bagging of PART rule learner offers higher true positive rate than other ensemble classifier with SMO algorithm based SVM and Random Forest on test dataset.

It is observed that bagging of PART rule learner offers 78.6684 % classification accuracy with 0.787 true positive rates. The majority voting method of ensemble using PART and SMO algorithm based SVM offers classification accuracy 78.7571 % with 0.788 true positive and 0.168 false positive rates. Finally, majority voting method of ensemble using PART rule learner and SMO algorithm based SVM offers highest classification and true positive rates with lowest false positive rate among different ensemble classifiers. It is also can observe that stacking of both PART and SMO exhibits same accuracy on test dataset.

V. CONCLUSIONS

In this paper, PART rule leaner and SMO algorithm based Support Vector Machine classifiers have used for intrusion detection system. Initially, two base classifiers have studied and implemented for intrusion detection system. Ensemble method is very effective way to reduce the false positives in classification. In second phase, ensemble classifiers are used for intrusion detection. PART Rule Learner and Support Vector machine using SMO have used as base classifier because they provide low training and generalization error. The performances of these base classifiers and ensemble classifier have evaluated in terms of classification accuracy, true and false positives. Genetic search algorithm have used to reduce the dimensionally of training dataset which decreased computational and model biding time. Ensemble method uses unstable classifiers for increasing classification accuracy.

The experimental results show that bagging of PART rule learner offers 78.6684 % classification accuracy with 0.787 true positive rates. The majority voting method of ensemble using PART and SMO algorithm based SVM offers classification accuracy 78.7571 % with 0.788 true positive and 0.168 false positive rates.

Finally, majority voting method of ensemble using PART rule learner and SMO algorithm based SVM offers highest classification and true positive rates with lowest false positive rate among different ensemble classifiers. It is also can observe that stacking of both PART and SMO exhibits same accuracy on test dataset.

Table- III: True positives and false positives of base and ensemble classifiers

Classifier	True positive on Training	False Positive on Training	True positive on Cross Validation	False Positive on Cross Validation	True positive on Testing	False Positive on Testing
SMO	0.937	0.067	0.937	0.067	0.722	0.227
PART	0.998	0.002	0.997	0.003	0.778	0.176
Majority Voting (Part and SMO)	0.997	0.003	0.995	0.005	0.788	0.168

Table- IV: True positive and False positives of AdaBoost, Bagging and Random forest

Ensemble Classifier	True positive on Training	False Positive on Training	True positive on Cross Validation	False Positive on Cross Validation	True positive on Testing	False Positive on Testing
AdaBoost (PART)	0.999	0.001	0.997	0.003	0.778	0.176
Bagging (PART)	0.999	0.001	0.997	0.003	0.787	0.170
Stacking (PART)	0.535	0.535	0.535	0.535	0.431	0.431
AdaBoost (SMO)	0.937	0.067	0.937	0.067	0.721	0.227
Bagging (SMO)	0.937	0.067	0.937	0.067	0.721	0.227
Stacking(SMO)	0.535	0.535	0.535	0.535	0.431	0.431
Random Forest	0.999	0.001	0.996	0.004	0.773	0.179

REFERENCES

1. Imson Garfinkel and Gene Spafford, "Practical UNIX and Internet Security: Morris Street, Sebastopol CA," O'Reilly and Associates Inc., ISBN 1-56592-148-8, 2nd edition, April 1996.
2. Ethem Alpaydın. Introduction to Machine Learning, Massachusetts London England: MIT Press Cambridge, 2nd edition, ISBN 978-0-262-01243-0, 2010.
3. Alex and Vishwanathan. Introduction to Machine Learning. Cambridge. United Kingdom: Cambridge University Press, 2008.
4. Tom T. Mitchell. Machine Learning. Portland: McGraw Hill, ISBN: 0070428077 March 1, 1997.
5. Jason Brownlee, "Machine Learning Mastery: Machine Learning Resource Guide," http://MachineLearningMastery.com.
6. Heber Ezra, Sheriff Bard and Mohamed Shaheen, "Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems," In International Journal of Computer Applications., vol. 56, no.7, October 2012, pp. 10-16.
7. Juvonen et.al. , "Combining Conjunctive Rule Extraction with Diffusion Maps for Network Intrusion Detection," In proc. Eighteenth IEEE Symposium on Computers and Communications (ISCC 2013), 2013, pp. 411-416.

8. Muamer N. Mohammada et.al., “A Novel Intrusion Detection System by using Intelligent Data Mining in WEKA Environment,” Procedia Computer Science., vol.3, no.3, 2011, pp.1237–1242.
9. Mrutyunjaya, Ajith and Manas, “A Hybrid Intelligent Approach for Network Intrusion Detection,” in Proc. International Conference on Communication Technology and System Design, Procedia Engineering, vol. no. 36, 2011, pp.1-9.
10. Mirco Marchetti, Michele and Fabio “Framework and Models for Multistep Attack Detection,” Journal of Security and Its Applications, vol. 5, no. 4, October 2011, pp. 73-82.
11. P. Shrinivasu and Avadhani, “Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection,” Procedia Engineering, Elsevier Ltd., vol. 38, ,2012 pp. 144-53.
12. Arun Kumar and Selvakumar, “Detection of Distributed Denial of Service attacks using an Ensemble of adaptive and Hybrid Neuro-Fuzzy Systems,” In Computer Communications, vol. 36, no. 3, February 2013, pp. 303–319.
13. Bartosz, and Bogusław, “Clustering-based Ensembles for one-class classification”, In Information Sciences, vol. 264, 2014, pp.182–195.
14. Srilatha Chebrolu, Ajith Abraham and Johnson P. Thomas, “A Feature deduction and Ensemble design of Intrusion detection systems,” In Computers & Security.vol. no. 24, 2005, pp. 295-307.
15. Srinivas Mukkamalaa, Andrew Sunga and Ajith Abrahamb, “Intrusion Detection uses an Ensemble of Intelligent paradigms,” In Journal of Network and Computer Applications, vol. 28, 2005, pp.167–182.
16. 16 Eitan Menahem, at.el. “Improving malware detection by applying Multi-inducer Ensemble,” In Computational Statistics and Data Analysis, vol. 53, 2009, pp. 1483–1494
17. Yang Liu, Xiaohui Yu, Jimmy and Aijun, “Combining Integrated sampling with SVM Ensembles for Learning from Imbalanced Datasets,” In Information Processing and Management, vol. 47, 2011, pp. 617–631.
18. Charlie Obimbo, Haochen Zhou and Ryan Wilson, “Multiple SOFMs Working Cooperatively In a Vote-based Ranking System For Network Intrusion detection,” In Procedia Computer Science, vol. 6, 2011, pp. 219–224.
19. Gaikwad and Thool, “Intrusion Detection System using Ripple down rule learner and Genetic Algorithm,” In International Journal of Computer Science and Information Technologies, Vol. 5 issue. 6, 2014, PP. 6976-6980.
20. Gaikwad and Ravindra C. Thool, “Intrusion Detection System Using Bagging Ensemble Method of Machine Learning,” In proceeding of International Conference on Computing Communication Control and Automation, 2015.
21. Elbe Frank and Ian Witten, “Generating Accurate Rules Sets without Global Optimization,” Department of Computer Science Technical report, University of Waikato, Hamilton, New Zealand, January 1990.
22. Bregman, L. M., "The Relaxation Method of Finding the Common Point of Convex Sets and its Application to the Solution of Problems in Convex Programming," In USSR Computational Mathematics and Mathematical Physics, 1967, 7:200-217,
23. Censor, Y., "Row-Action Methods for Huge and Sparse Systems and Their Applications," SIAM Review, 23(4), 1981, pp. 444-467
24. John C. Platt, “Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Machines,” In Technical Report MSR-TR-98-14, Microsoft Research, April 21, 1998.

AUTHORS PROFILE

Dr. D. P. Gaikwad is working as an Associate Professor in the Department of Computer Engineering, AISSMS College of Engineering, Pune. He received his M. Tech (CSE) from College of Engineering, Pune and Ph.D. degree from SGGSIOET, Nanded. His area of interests is Machine Learning, Microprocessor, Network Security and Soft Computing. He published more than 30 Research Papers in various International Journals and Conferences.

Mrs. M. M. Swami is an Assistant Professor in the Department of Computer Engineering, AISSMS College of Engineering. She received her M. Tech. (Computer Science and Technology) Department Of Technology, Kolhapur and B. E(Computer Science and Engineering) Bharati Vidhyapith College of Engineering, Kolhapur.

Mrs. S. S. Kolte an Assistant Professor in the Department of Computer Engineering, AISSMS College of Engineering. She received her M.E (Computer Science and Engineering) D.Y.Patil Institute, Pune and B. E(Computer Science and Engineering) Sinhgad Institute of Technology, Lonavala.