Building an Effective Intrusion Detection System using combined Signature and Anomaly Detection Techniques

Prakash N Kalavadekar, Shirish S. Sane

Abstract: ***Intrusion Detection Systems (IDS) are providing better solution to the current issues and thus became an important element of any security infrastructure to detect various threats so as to prevent widespread harm. The basic aim of IDS is to detect attacks and their nature and prevent damage to the computer systems. Several different approaches for intrusion detection have been reported in the literature. These approaches are broadly categorized into three approaches: I) Signature-based approach II) Anomaly based approach and III) Hybrid approach that combines signature and anomaly detection approaches. Hybrid approach has been found to be superior to either signature based or anomaly based approaches. Several different algorithms are available for hybrid approach. This paper suggests the combined approach using signature and anomaly detection techniques. The signature based is build using genetic algorithm as filter based feature selection and J48 as classifier and data mining approach is used to build anomaly based IDS. The performance of combined IDS is evaluated on well known datasets such as KDD Cup 99, UGR 16 and Kyoto 2006+ etc. The experimental results presented here are encouraging and show superiority of combined IDS to detect network anomalies with respect to time required building the model, detection rate, accuracy and false positive rate.***

Index Terms: Anomaly, Data Mining, Intrusion Detection, Anomaly, Signature.

I. INTRODUCTION

Network attacks from the different networks and types can be detected using Intrusion Detection System (IDS). To capture and protect network packets IDS can be used efficiently. The captured packets are analyzed to detect malicious network activities with the help of IDS, so it can be informed to take action on malicious connection and further prevention can be applied to the network. Network security can be provided by combining IDS with the firewall. Intrusion detection systems are further classified as signature based detection and anomaly based detection [1]. Signature based detection techniques detect attacks based on the known attack signatures. They are effective in detecting known attacks with low errors. However, they cannot detect newly created attacks that do not have similarity to the known attacks. Anomaly based detection system generate profiles of normal traffic pattern by analyzing normal traffic in the network. Generally behaviour of attacker and normal user is used to find deviation in anomaly detection method to detect attacker. So it is useful to detect new attack patterns, but detection rate and false positive rate is not good compare to signature based detection models for known attacks.

In 2005 a new method was proposed as hybrid intrusion detection which will combine both methods as signature based and anomaly based to solve the limitation of individual methods. The performance of the combined method is measured with the performance of combination of two different methods. Most combined detection systems independently train a signature based detection model and an anomaly based detection model, and then simply aggregate the results of the both models. If one of the methods declares attack then combined intrusion detection system declares an attack. So detection rate will be improved but problem of high false positive rate will remain [7].

A new combined intrusion detection method which integrates two models as signature based detection model and an anomaly based detection model. To build normal behaviour profiles in the anomaly based detection model known normal traffic information is used. The proposed combined technique used the normal training data as of different services. Different types of services and connections are used to prepare normal traffic data which will improve the performance of the system. A filter based feature selection using genetic algorithm and J48 (C4.5) decision tree (DT) is used to build signature based detection model and the frequent association rule mining is used to develop anomaly based detection model. The combined system is implemented using genetic algorithm to select important features and then model is trained using J48 and multi class SVM on different standard datasets, and frequent association rule mining is applied on normal traffic patterns. The combined intrusion detection system was evaluated by conducting different experiments in which the KDD Cup 99, NSLKDD, Kyoto 2006+, DARAPA MIT/LL 99 and UGR 16 datasets are used. By observing experiment results, we can say that the proposed method gives better performance in terms of detection rate for unknown and known attacks than the conventional methods.

II. RELATED WORK

The various researchers have done their research on hybrid intrusion detection methods in which they have proposed different techniques to overcome the disadvantages of the anomaly based detection and signature based detection methods. The three different methods have used by various researcher to combine the anomaly based detection model and signature based detection model: anomaly

Revised Manuscript Received on August 05, 2019.

Mr. Prakash N. Kalavadekar, K.K Wagh Institute of Engineering Education & Research, Nashik, Savitribai Phule Pune University, India.

Dr. Shirish S. Sane, K.K Wagh Institute of Engineering Education & Research, Nashik, Savitribai Phule Pune University, India.

based detection followed by signature based detection, parallel use of anomaly based detection and signature based detection, and signature based detection followed by anomaly based detection.

Koutsoutos, Christou, and Efremidisto gives solution using classifier as artificial neural network and they have implemented IDS where a combination of more than one neural network is used which is capable of detecting network attacks on web servers. Their system is useful to detect unseen attacks and make categorization.

Prema Rajeswari and Kannan [2008] have proposed a rule based approach using enhanced C4.5 algorithm for intrusion detection. It is used to detect abnormal behaviors of internal attackers in the networks using classification and decision making.

D. Barbara [2008] proposes how attack characteristics, system training history, services provided, and underlying network conditions will impact on sensitivity of both signature based and anomaly based detection models. They also suggested that data mining techniques can be used to construct classification models from labeled attacks.

Lee et al. [1998] had proposed that how to generate rules for anomaly detection method using normal traffic. Fan extended Lee's method to find accurate boundaries between known attacks and unknown anomalies.

Kai Hwang, Fellow, IEEE, Min Cai, Member, IEEE, Ying Chen, Student Member, IEEE, and Min Qin [2007] suggest data mining techniques where association rules were used to build IDS. They have suggested how single connection attacks will be detected as well as multi connection attacks. They also give information of systems based on misuse model like SNORT and Bro.

Gisung Kim, Seungmin Lee, Sehun Kim (2014) done the analysis on a brand new hybrid intrusion detection technique that hierarchically integrates a misuse detection model and an anomaly detection model. First, the C4.5 decision tree (DT) is used to produce the misuse detection model which decomposes the traditional training information into different small clusters. And to produce associate anomaly detection model used the one class support vector machine (1-class SVM).

The experiments were conducted with a modified version of well known KDD Cup 99 dataset as the NSL-KDD data set. Their method gives better detection rate than the conventional methods for both unknown and known attacks. It also maintains a low false positive rate compare to other methods. And significantly reduces the high time complexity of the training and testing for the system. The one class SVM does not require the labeled information. However, there is disadvantage due to its high false positive rate so it is difficult to use the one class SVM in the real world.

In the paper [24] Wenying and his colleague (2014) uses combination of SVM method and CSOACNs (Clustering based on Self-Organized Ant Colony Network) for getting advantages of each method and avoiding their weaknesses. They have implemented algorithm and for evaluation used KDDCup 99 standard dataset as a benchmark. As per their experiments it is observed that CSVAC (Combining Support Vectors with Ant Colony) gives better performance in terms of both classification rate and run-time efficiency than SVM alone or CSOACN alone. The CSVAC algorithm have shown higher average detection rate, less training time, and lower rates of both false negative and false positive than pure SVM alone as per their experimental results. Even it gives better performance of less training time with comparable detection rate and false alarm rates than pure CSOACN. But still effectiveness and the flexibility of IDS system is less & required to improve.

Ghun Guo,Yuan Ping, Nian Liu and Shou-Shan Luo [2016] proposes two level hybrid approach for intrusion detection using combine misuse and anomaly detection. They used a misuse detection component and two anomaly detection components to build two level hybrid solutions. The first level as anomaly detection based on the change of cluster centers using K-means or CURE method. The second level two detection components using K-nearest neighbors algorithm to reduce the false positive rate and false negative rate generated by first level. The experimental results are tested on KDDCup 99 and Kyoto University Benchmark dataset. The IDS detect network anomalies effectively and having a low false positive rate.

So it can be observed that there is scope for research by combining advantages of both signature & anomaly detection model to improve the detection rate & time efficiency with real time traffic & multi connection in network. Following sections gives the details of the proposed method with experimental setup and result analysis.

III. IMPLEMENTATION METHODOLOGY

Effective combined signature based and anomaly based IDS framework is shown in Fig. 1 which will be used for detection of known & unknown attacks. Signature based IDS is trained by using previously known attack patterns. Whenever new record comes to system it compares that pattern with previously known attack pattern and based on comparison decision will be given as known & unknown attacks.

Signature based IDS uses genetic algorithm as filter approach for selecting number of features from given dataset. The selected features are used to train model using J48 classifier from Weka 3.8. Below Fig. 1 the algorithmic steps used in feature selection as genetic algorithm are given [1]-[3].

Fig. 2 shows the anomaly detection system in which normal traffic records are used to generate rule database. The important attributes are selected which includes service as one of the attribute and frequent service is calculated using selected support value. Then association rule mining is applied to generate rules with selected confidence value. In generated rules there is possibility of redundant and long rules, so pruning is applied to remove redundant rules and left hand side with only two attributes from which one will be service. The rule matching technique is used to detect anomaly and normal packets.

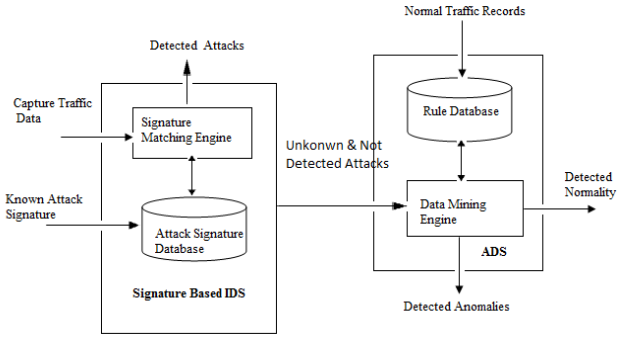

Fig. 1 Framework for Combined Signature and Anomaly Intrusion Detection System

Input- Binary encoded string which is having length n (where n is the number of features), population size, Uniform Crossover Probability (Pc), Mutation Probability (Pm), Empty solution (All bits value '0').
Output- Selected important features.

1. Initialize the population with chromosome which has size n and each gene value can be '0' or '1'. (0-means feature value zero and 1- means feature value other than zero)
2. Initialize Maximum Fitness = Solution length (n), previous fitness = 0 & calculate current fitness (initial value is zero) of chromosome by incrementing fitness value by one if solution bits match with gene bits.
3. While ((current fitness – previous fitness)>0.001) {
    a. With the specified probability Pc & Pm do uniform crossover and mutation operations.
    b. Increment fitness value if solution bits match with gene bits.
    c. Make previous fitness = current fitness.
4. Using tournament selections find the best of chromosomes into new population. }
5. Display the solution with selected features.

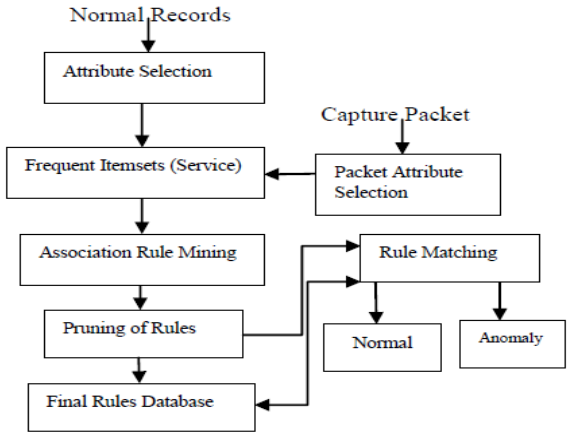

Fig. 2 Framework for Anomaly Detection System

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental Setup

Feature selection algorithms aim at selecting optimum features from the given set of features. The selected features are then used by a classifier to build a trained model without compromising the detection rate and/or accuracy of the model. Basically anomaly IDS implemented for services which are running on the server and can be accessed through network by number of clients. So it is required to prepare normal profile of the server with respect to traffic log which generated by communication between server and number of clients. The frequent itemsets and association rule mining algorithm is applied to generate frequent episode rules on normal traffic data. After the generation of rules few pruning techniques are applied to generate new rules. The pruning techniques used as 1] Removing redundant rules. 2] LHS was maintained with maximum two attributes and one attribute service is compulsory. The IDS is evaluated using following datasets for rule generation and testing the system.

1] 1999 DARPA Lincoln Lab IDS evaluation dataset which consist of 11 attributes with score value which is defined as if 1 then attack else normal packet.

It consists of intra traffic and inter traffic data as day wise. Here we have used intra traffic data of date 06/02/1998 with 33856 records and 7 services are considered.

The following six attributes are used for training the system as duration, service, srcport, destport, srcIP, destIP. For normal rule generation 255 normal records are used from dataset with support= 0.7 and confidence = 0.5. The Table I shows the number of rules with respect to different services.

I: Number of Rules for Intra traffic

Service	#Rules	#Pruned Rules	Time (ms)
http	25	8	60
Auth	105	27	59
Finger	22	7	11
ftp	0	0	5
Ftpdata	3	1	6
Smtp	0	0	5
telnet	0	0	7
Total	**155**	**43**	**183**

2] We have used inter traffic data of date 06/02/1998 with 33519 normal records and 7 services are considered.

The following six attributes are used for training the system as duration, service, srcport, destport, srcIP, destIP. For normal rule generation 33519 normal records are used from dataset with support= 0.5 and confidence = 0.3.The Table II shows the number of rules with respect to different services.

II: Number of Rules for Inter traffic

Service	#Records	#Rules	#Pruned Rules	Time (ms)
http	32155	03	01	8
Auth	75	22	07	11
Finger	109	03	01	7
ftp	118	03	01	8
smtp	896	03	01	9
telnet	35	0	0	10
Eco/i	131	416	81	38
Total	**33519**	**450**	**92**	**91**

3] KDD Cup 99 dataset which consist of 41 attributes with label as normal or attack name. We have used 2673 normal records and 12 services are considered.

The following six attributes are used for training the system as duration, protocol, service, flag, src_bytes, dest_bytes. For normal rule generation 2673 normal records are used from dataset with support= 0.5 and confidence = 0.3.The Table III shows the number of rules with respect to different services.

III: Number of Rules for KDD Cup 99

Service	#Records	#Rules	#Pruned Rules	Time (ms)
http	223	22	07	8
Auth	04	22	07	8
Finger	10	22	07	11
ftp	227	105	27	22
smtp	118	22	07	10
telnet	38	03	01	6
Private	834	22	07	54
Other	59	22	07	7
Domain_u	1096	22	07	11
Pop 3	04	124	33	27
Ecr/i	35	105	27	18
Eco/i	25	105	27	23
Total	**2673**	**596**	**164**	**205**

4] Kyoto 2006+ August 2009 dataset which consist of 24 attributes with label as normal or attack. We have used 74458 normal records and 2 services are considered.

The following six attributes are used for training the system as duration, service, src_ip, src_port, dest_ip, dest_port. For normal rule generation 74458 normal records are used from dataset with support= 0.5 and confidence = 0.3.The Table IV shows the number of rules with respect to different services.

IV: Number of Rules for Kyoto 2006+ (August 2009)

Service	#Records	#Rules	#Pruned Rules	Time (ms)
smtp	63018	03	01	8
Other	11440	10	07	10
Total	**74458**	**13**	**08**	**18**

5] UGR16 dataset built with real traffic and up to date attacks using cyclostationary based network IDS. It consists of 4 month (18/03/2016-26/06/2016) data with 16,900 Million records and 10 attributes. The following seven attributes and eight services are used for training the system as duration, Src_IP, Dest_IP, Src_port, Dest_port, protocol, service. For normal rule generation normal records are used from dataset with support= 0.5 and confidence = 0.3.The Table 5 shows the number of rules with respect to different services.

Table 5: Number of Rules for UGR16

Service	#Records	#Rules	#Pruned Rules	Time (ms)
Service 1	31	22	07	11
Service 2	02	2979	425	172
Service 3	249	03	01	08
Service 4	270	03	01	07
Service 5	06	03	01	05
Service 9	60	03	01	07
Service 10	43	2979	413	164
Service 12	25	22	07	12
Total	**686**	**6014**	**856**	**386**

B. Performance Evaluation

Performance of implemented system has been evaluated using accuracy, detection rate, false positive rate and are defined by

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FN+FP} \quad (1)$$

$$\text{Detection Rate} = \frac{TP}{TP+FN} \quad (2)$$

$$\text{False Positive Rate} = \frac{FP}{FP+TN} \quad (3)$$

where, True Positive (TP) is the number of anomaly records are identified as anomaly, True Negative (TN) is the number of normal records are identified as normal, False Positive (FP) is the number of actual normal records are identified as anomaly, False Negative (FN) is the anomaly records are identified as normal.

C. Results and Discussion

The detection performance of the anomaly intrusion detection system using rule matching for four datasets with randomly selecting attack and normal records are shown in Table VI. The Table VII shows performance using randomly generated attacks for two datasets.

The combined performance of the intrusion detection system using J48 with GA as signature based IDS and anomaly based system on the five datasets are shown in Table VIII. The results clearly demonstrate that the performance of IDS is enhanced by the combined effect of both signature and anomaly based system. It shows clearly that the detection model combined with the both systems has achieved an accuracy rate of 99.96%, 99.81%, 99.89% ,99.94%and 99.32% for DARPA Lincoln Lab, KDD Cup 99, NSL-KDD, Kyoto 2006+ (August 2009) and UGR16, respectively, and significantly up to the mark with all other methods. The table shows that the combined IDS performance is better than only signature based IDS or anomaly based IDS.

VI: Detection for all services based on the four dataset

Dataset	# Rules	# Records	Accuracy	DR	FPR
DARPA Lincoln Lab dataset	135	200	100	100	0.00
KDD Cup 99	164	60	68.33	50	13.33
Kyoto 2006 + August 2009	08	200	100	100	0.00
UGR16	856	100	100	100	0.00
Average			92.08	87.50	3.33

VII: Detection for all services based on the randomly generated attacks

Dataset	# Rules	# Records	Accuracy	DR	FPR
DARPA Lincoln Lab dataset	135	100	100	100	0.00
KDD Cup 99	164	30	80	80	0.00
Average			90.00	90.00	0.00

VIII: IDS combined performance with signature and anomaly detection

Dataset	#Train	#Test	SDS			ADS			SDS+ADS		
			Accuracy	DR	FPR	Accuracy	DR	FPR	Accuracy	DR	FPR
DARPA Lincoln Lab	20347	13564	99.80	99.80	0.00	81.48	81.48	0.00	99.96	99.96	0.00
KDD Cup 99	48852	32568	99.48	99.48	0.3	59.44	73.00	5.55	99.81	99.78	0.23
NSLKDD	75584	50389	99.47	99.50	0.3	78.87	76.76	0.00	99.89	99.88	0.00
UGR16	6203	4135	96.03	96.00	4.7	82.92	82.92	0.00	99.32	99.32	0.00
Kyoto August 2009	86045	57363	99.77	99.80	0.2	75	100	0.2	99.94	100	0.2

Fig. 3 illustrates a comparison between detection rates and false positive rates of all datasets on which testing was done using proposed system. By observing the figure we can comment that the proposed system gives satisfied performance over all tested datasets.

D. Comparative Study

Table IX shows a comparative results achieved by two level hybrid, DT +1Class SVM, CSOACN and CSVAC proposed in [7],[10] that have been tested on Kyoto 2006+ dataset and KDD Cup 99 dataset.

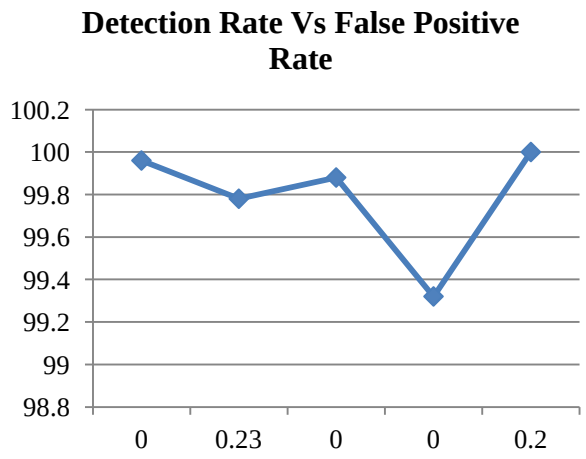

Fig. 3 Comparison results of Detection rate Vs False positive rate of all datasets

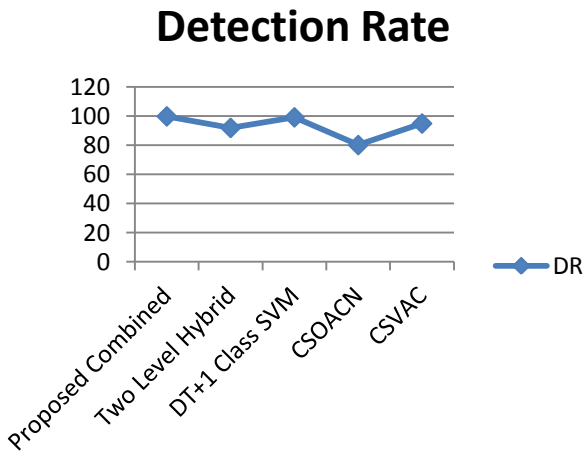

Fig. 4 Comparison results of Detection rate on the KDD Cup 99 dataset

Through the results, proposed system shows improvement in detection rate and reduction in false positive rate. However, the obtained results of the proposed system are better, compared to other methods as shown in Table IX. The final results achieved by proposed system show 99.78%, 0.23% and DT + 1 Class SVM show 99.10%, 1.2% of the final detection and false positive rates respectively.

Fig. 4 illustrates a comparison between proposed system and other existing systems in terms of detection rates.

IX: Comparative Performance of Proposed System

Dataset	Method	Accuracy (%)	DR (%)	FPR (%)
KDD Cup 99	Proposed Combined	99.81	99.78	0.23
	Two Level Hybrid	93.29	91.86	0.78
	DT+1 Class SVM	na	99.10	1.2
	CSOACN	na	80.10	2.84
	CSVAC	na	94.86	6.01
Kyoto 2006+	Proposed Combined	99.94	100	0.2
	Two Level Hybrid	95.76	93.25	1.05
	DT+1 Class SVM	na	na	na
	CSOACN	na	na	na
	CSVAC	na	na	na

V. CONCLUSION & FUTURE SCOPE

In this paper, a new effective intrusion detection method that combined signature based detection and anomaly based detection was proposed. With genetic algorithm as feature selection and C4.5 decision tree (J48) as classifier was used to generate signature based model and then frequent itemsets with association rule mining was used to build normal traffic rule database for anomaly based detection model. The anomaly detection model use service as main part of rule to build normal behavior of system. The experiments demonstrated that the proposed an effective combined intrusion detection method improves the IDS in terms of accuracy, detection rate and false positive rate for network anomalies as compare to existing hybrid approaches. The overall accuracy of proposed IDS is 99.87 and detection rate is 99.89. The performance of effective combined IDS can be enhanced in future research work and investigation.

REFERENCES

1. Prakash Kalavadekar, Dr. Shirish Sane "Building an Effective Intrusion Detection Systems using Genetic Algorithm based Feature Selection", INTERNATIONAL Journal of Computer Science and Information SECURITY (IJCSIS) , Volume 16, No.7, July 2018, ISSN 1947-5500, pp.97-110.
2. Prakash Kalavadekar, Dr. Shirish Sane "Effective Intrusion Detection Systems using Genetic Algorithm", International Journal ON EMERGING Trends in Technology, Volume 4, Special Issue July-2017, pp.8315-8319.
3. Prakash Kalavadekar, Dr. Shirish Sane "Effect of Mutation and Crossover Probabilities on Genetic Algorithm and Signature Based Intrusion Detection System", To be published in International Journal of Engineering & Technology (UAE), ISSN-2227-524X.
4. Prakash Kalavadekar, Dr. Shirish Sane "Effective Intrusion Detection Systems using Hybrid Approach"International Journal of Exploring Emerging Trends in Engineering, Volume 3 Issue 2 Mar-Apr-2016
5. MIN CAI, KAI HWANG AND MIN QIN "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes", IEEE Transactions on Dependable And Secure Computing, Vol.4 No.1, Jan-March 2007.
6. MOHAMMED A. AMBUSAIDI, PRIYADARSHI NANDA "Building an intrusion detection system using a filter-based feature selection algorithm", IEEE Transactions on computers, November 2014.
7. GISUNG KIM, SEUNGMIN LEE, SEHUN KIM "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection", Expert Systems with Applications, Elsevier Ltd, 2014.
8. S. JAJODIA L., POPYACK D. BARBARA, J. COUTO AND N. WUY. ADAM "Detecting Intrusions by data mining ", Technical report, Workshop Information Assurance and Security, USA, 2001.
9. BHARATHI M. SAHANA DEVI K. J. "Hybrid intrusion detection with weighted signature generation", Technical report, Dept of CSE, CHICKBALLAPUR, 2011.
10. SIVA S. SIVATHA SINDHU, S. GEETHA, A. KANNAN "DECISION TREE BASED LIGHT WEIGHT INTRUSION DETECTION USING A WRAPPER APPROACH", EXPERT SYSTEMS WITH APPLICATIONS 39 129-141, 2012.
11. KAPIL KUMAR GUPTA, BAIKUNTH NATH, RAMAMOHANARAO KOTAGIRI " Layered Approach Using Conditional Random Fields for Intrusion Detection" IEEE Transactions on Dependable and Secure Computing, Vol.4 No.1, Jan-March 2010
12. DR. SAURABH MUKHERJEEA, NEELAM SHARMA "INTRUSION Detection using Naive Bayes Classifier with Feature Reduction", Procedia Technology, 119 – 128, 2012.
13. BERTRAND PORTIER, FROMENT-CURTIL " Data Mining Techniques for Intrusion Detection", The University of Texas at Austin, Dr. Ghosh - EE380L Data Mining Term Paper, Spring 2000.
14. L PREMA RAJESWARI, KANNAN ARPUTHARAJ " An Active Rule Approach for Network Intrusion Detection with Enhanced C4.5 Algorithm", I. J. Communications, Network and System Sciences, 4, 284-359 Published Online, November 2008.
15. NAHLA BEN AMOR, SALEM BENFERHAT " Naive Bayes vs Decision Trees in Intrusion Detection Systems" , SAC'04, March 14-17, Nicosia, Cyprus,2004.
16. AHMED H. FARES AND MOHAMED I. SHARAWY " Intrusion Detection: Supervised Machine Learning", Journal of Computing Science and Engineering, Vol. 5, No. 4, PP. 305-313, December 2011.
17. ADETUNMBI A.OLUSOLA., ADEOLA S.OLADELE AND DARAMOLA O. ABOSEDE "Analysis of KDD 99 Intrusion Detection Dataset for Selection of Relevance Features", Proceedings of the World Congress on Engineering and Computer Science 2010,Vol I WCECS 2010, San Francisco, USA, October 20-22 2010.
18. MAHBOD TAVALLAEE, EBRAHIM BAGHERI, WEI LU AND ALI A., GHORBANI "A Detailed Analysis of the KDD CUP 99 Data Set", Proceedings of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009).
19. TAISIR ELDOS, MOHAMMAD KHUBEB SIDDIQUI AND KANAN, "The KDD99 Dataset: Statistical Analysis for Feature Selection", Journal of Data Mining and Knowledge Discovery ISSN: 2229-6662 & ISSN: 2229-6670, Volume 3, Issue 3, pp.-88-90, 2012.
20. YISEHAC YOHANNES, JOHN HODDINOTT " Classification and Regression Trees: An Introduction", International Food Policy Research Institute, 2033 K Street, N.W.Washington, D.C., U.S.A, 2006
21. PEYMAN KABIRI AND ALI A. GHORBANI "Research on Intrusion Detection and Response: A Survey", International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005.
22. WENKE LEE AND SALVATORE J. STOLFO "Data Mining Approaches for Intrusion Detection", 7th USENIX Security Symposium, 1998.
23. ISMAIL BUTUN, SALVATORE D. MORGERA, AND RAVI SANKAR "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2013.
24. WENYING FENG, QUINGLEI, GONGZHU HU, JIMMY XIANGI HUANG "Mining Network data for intrusion detection through combining SVMs with ant colony networks", Future Generation Computer Systems, Elsevier, 2013.
25. SEYED MOJTABA, HOSSEINI BAMAKAN, HUADONGWANG, TIANYINGJIE, YONGSHI "An effective intrusion

detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization", Nerocomputing, Elsevier Ltd, 2016.
26. S. MUKKAMALA, A. H. SUNG "Significant feature selection using computational intelligent techniques for intrusion detection", Advanced Methods for Knowledge Discovery from Complex Data, Springer, 2005, pp. 285–306.
27. S. CHEBROLU, A. ABRAHAM, J. P. THOMAS "Feature deduction and ensemble design of intrusion detection systems", Computers & Security 24 (4) (2005) 295–307.
28. Y. CHEN, A. ABRAHAM, B. YANG "Feature selection and classification flexible neural tree", Neurocomputing 70 (1) (2006) 305–313.
29. KAPIL KUMAR GUPTA, BAIKUNTH NATH, SENIOR MEMBER, IEEE, AND RAMAMOHANARAO KOTAGIRI, MEMBER, IEEE "Layered Approach Using Conditional Random Fields for Intrusion Detection", IEEE Transactions on DEPENDABLE AND Secure Computing, Vol. 7, No. 1, January-March 2010.

AUTHORS PROFILE

Mr.Prakash N.Kalavadekar, received Bachelors Degree in Computer Science & Engineering and Masters Degree ME in Computer Science & Engineering from Walchand College of Engineering, Sangli in the year 1997 and 2007 respectively, pursuing PhD in Computer Engineering from Savitribai Phule Pune University,Pune.His areas of interests include Data Mining, Databases, Computer Network & Security, Cloud Computing and Image Processing.

Dr. Shirish S.Sane, obtained his Bachelors' Degree in Computer Engineering from the Pune Institute of Computer Technology (PICT), Pune, Masters Degree M. Tech (CSE) from IIT Bombay and Ph. D. in Computer Engineering from Savitribai Phule Pune University, formerly known as University of Pune. Dr. Shirish is working as the Head of the Computer Engineering Department and Vice Principal at K K Wagh Institute of Engineering Education & Research, Nashik. He has published more than 60 research papers at the National and International Conferences and Journals. He has also authored books on the subjects "Data Structures" and "Theory of Computer Science". His areas of interests include Data Mining, Databases, Compilers and Cloud Computing.