Genetic Algorithm based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Networks

Anand Kannan and Gerald Q. Maguire, Jr.
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden
e-mail: {anandk,maguire}@kth.se

Ayush Sharma and Peter Schoo
Fraunhofer Research Institution for
Applied and Integrated Security
Munich, Germany
e-mail: firstname.lastname@aisec.fraunhofer.de

***Abstract*— Cloud computing is expected to provide on-demand, agile, and elastic services. Cloud networking extends cloud computing by providing virtualized networking functionalities and allows various optimizations, for example to reduce latency while increasing flexibility in the placement, movement, and interconnection of these virtual resources. However, this approach introduces new security challenges. In this paper, we propose a new intrusion detection model in which we combine a newly proposed genetic based feature selection algorithm and an existing Fuzzy Support Vector Machines (SVM) for effective classification as a solution. The feature selection reduces the number of features by removing unimportant features, hence reducing runtime. Moreover, when the Fuzzy SVM classifier is used with the reduced feature set, it improves the detection accuracy. Experimental results of the proposed combination of feature selection and classification model detects anomalies with a low false alarm rate and a high detection rate when tested with the KDD Cup 99 data set.**

Keywords- Intrusion Detection System (IDS), Genetic Algorithm (GA), Fuzzy Support Vector Machine (FSVM), tenfold cross validation

I. INTRODUCTION *(HEADING 1)*

Cloud computing has drastically modified the operating models of organizations reducing both capital and operational expenditures. Moreover, cloud computing virtualizes the physical resources and provides these virtualized resources through provisioning models devised for the cloud ecosystem, such as Software as a service, Platform as a Service, and Infrastructure as a service provisioning models.

Some, cloud service providers provide services to their customers without owning the underlying physical resources, by leasing the physical resources from a cloud vendor, thus reducing their capital and operational expenditures as well as the risks attached with owning and managing the resources. At the same time, the cloud vendor can amortize their already low per-head costs by provisioning their virtualized resource set to more service providers.

The capabilities of cloud computing are enhanced by integrating networking functions with it, which allows the cloud vendor to provision network resources along with other resources. This enables on-demand, dynamic, isolated, and elastic provisioning of virtualized network resources to the end user. In addition, it allows the cloud vendor to optimize various parameters such as network load, network latency, and resource usage. The European Seventh Frame work Programme based project Scalable and Adaptive Internet Solutions (SAIL) introduces a new provisioning model, namely Network-as-a-service, which enables the provisioning of virtualized network resources. The project also describes a Cloud Network (CloNe) architecture as the backbone of a service provisioning infrastructure.

The introduction of network resources into the existing cloud computing service provisioning models introduces network-related security challenges. Some of these security challenges were described by Schoo et al., in [12], specifically information security, virtualization environment threats, and communication security. Fusenig et al. in [13] proposed a security architecture for strengthening the CloNe architecture by adding a security goal translation function, identity management function, access control policy function, and an auditing and assurance function. This paper describes the design and deployment of a Genetic Algorithm based Feature Selection Algorithm for effective feature selection as part of an Intrusion Detection System (IDS) using a Fuzzy SVM classifier to support the auditing and assurance function of the CloNe security architecture. Conventional intrusion detection and prevention strategies, firewalls, access control schemes, and cryptographic methods used in the past for providing security to the data communicated through the cloud networks have failed to prove themselves effective for protecting networks and systems from increasingly sophisticated attacks. The proposed IDS turns out to be a suitable solution to these issues. An IDS has become an essential component in security systems since it can be used to detect threats *before* they cause widespread damage. The design and construction of an IDS has many challenges including data collection, data pre-processing, identification of malicious nodes, reporting, and response. Among these activities, identification of malicious nodes is an important and essential activity.

The IDS proposed in this paper can be used to examine collected audit data. Intrusion detection paradigms are based upon models of intrusive or innocent behaviour, so that both internal and external intrusion attempts may be identified efficiently. Moreover, an intelligent IDS should be an

effective defensive system that is capable of adapting dynamically to the changing traffic patterns and must be deployed throughout the network, rather than only at servers. This deployment is essential to detect attackers both at the individual nodes and also based on the traffic patterns in the network. The main factor that complicates constructing such an IDS is the necessity for an autonomously evolving system. Complicating this evolution are the huge amounts of network traffic, highly imbalanced data distribution, and the difficulty in recognizing normal versus abnormal behaviour of a user or application. As the audit database grows, even more data has to be considered when forming patterns, otherwise there is increased risk for a high false positive rate. Too high a rate of false positives defeats the purpose of an IDS as either too many alerts are generated that have to be handled manually or there are too many authorized actions which are prevented from occurring. This audit database is frequently augmented with additional real time traffic data. In most IDSs, the IDS is trained on the whole audit database. Our observations reveal that this database contains irrelevant and redundant features impeding the training and testing process, consuming unnecessary resources and leading to poor detection rate.

In order to improve the performance of an IDS, it is necessary to identify and remove the insignificant and duplicate information from the underlying dataset. Therefore, an effective IDS must have a pre-processing component that selects only the necessary features and a classification component for making efficient decisions. These components must work together to optimize the performance with respect to the detection time and to enhance the detection accuracy.

In this paper, we propose an intrusion detection system which uses a new genetic based feature selection algorithm and combine it with a Fuzzy SVM based classifier proposed by Lin [11] in order to create IDS that is effective in identifying intrusions present at the network layer. For this purpose, we propose a new architecture for host based intrusion detection system which will analyse the data present in the network. In order to validate this system, we use the KDD Cup dataset records split in the ratio of 9:1 to provide a tenfold cross validation of the effectiveness of the classifier. The main contribution of the proposed system is that it provides an architectural framework for integrating the feature selection system with the decision making system.

The remainder of this paper is organized as follows: Section 2 surveys related works and compares them with this proposed solution. Section 3 describes a Cloud Network Security Architecture. Section 4 describes the proposed IDS system architecture. Section 5 offers details of the proposed IDS. Section 6 discusses the results obtained with the proposed IDS and a tenfold cross validation performed to test of the system. Section 7 concludes and suggests some possible future enhancements.

II. RELATED WORK

There are many works in the literature concerning feature selection and classification. Among them, a heuristic genetic neural network was proposed by Zhang [1] to improve the performance of intrusion detection, in which input features, network structure, and connection weights were considered jointly. Li et al. [2] combined a fuzzy SVM and a multi-class SVM based on a binary tree to develop a network IDS that increases the classification accuracy. Chen et al. [3] discussed the application of fuzzy transitive kernels as fuzzy similarity relations for developing a fuzzy roughest based classifier. They used the lower approximation in fuzzy transitive kernel based fuzzy rough set and assigned memberships to each object. Finally, they used this for classification, thus enhancing the performance of SVM for their application.

Jiang et al. [4] introduced class and sample weighted factors, thus to solve the problem of classification biases caused by uneven training sets. Furthermore, they constructed a decision model based on these samples to improve the classification accuracy. Zaman et al. [5] improved the Support Vector Decision Function approach by integrating it with a fuzzy inferencing model. They used the fuzzy inferencing model to improve the performance of learning approximation used for decision making.

El-Khatib [6] proposed a novel hybrid model that efficiently selects the optimal set of features in order to detect intrusions which are specific to 802.11. Their model for feature selection uses the information gain ratio which is used to compute the relevancy of each feature. Moreover, this system uses the existing k-means classifier to classify and select the required and relevant features of MAC layer which will help to improve the accuracy of intrusion detection systems and at the same time it will reduce learning time of its learning algorithm. Farid et al. [7] enhanced the performance of IDS by proposing a weight based decision tree. Guo et al. [8] proposed a new feature selection algorithm by combining rough sets and genetic algorithm to form a new clustering technique. Stein et al. [9] proposed a decision tree classifier for network intrusion detection with GA-based feature selection. The main advantage of their work is reduction in classification time.

Cao Li-ying et al. [10] combined SVM algorithm and LVQ neural network algorithm and applied it in network intrusion detection systems. They concluded as follows: (1) In contrast with BP neural networks, the convergence speed of SVM-LVQ model is faster and the method is easy to perform. Furthermore, its detection rate of attacks is significantly higher and error rate is lower. (2) The combined model method to obtain the recognition rate has improved significantly than the ordinary method. Krzysztof Cpałka [6] proposed a new class of neuro-fuzzy systems. Moreover, he developed a novel method for reduction of such systems without the deterioration of their accuracy. The reduction algorithm gradually eliminates inputs, rules, antecedents, and the number of discretization points of integrals in the “centre of area” defuzzification method. It then automatically detects and merges similar input and output fuzzy sets. Computer simulations have shown that the accuracy of the system after reduction and merging has not deteriorated, despite the fact that in some cases up to 54% of various parameters and 74% of inputs were eliminated. The reduction algorithm has been tested using well-known classification benchmarks.

The basic requirements of the IDS proposed in this paper are its seamless integration with the overall CloNe (security) architecture and the individual security functions. Moreover, the proposed IDS shall aim to detect the plausible attacks on the CloNe architecture with an acceptable success rate. In this paper, a new intrusion detection system is proposed which differs from existing work in many ways. First, this is a host based IDS and hence is more efficient than the existing network based IDSs. Second, we consider intrusions at the network layer and hence all the important attacks, including Denial of Service attacks, are captured effectively. Third, it uses a pre-processing technique based on genetic algorithms which intelligently performs attribute selection. Fourth, it uses a new classification algorithm for effectively identifying the intruders. Finally, we use tenfold cross validation for validating the decisions made in this system.

III. CLOUD NETWORK SECURITY ARCHITECTURE

Figure 1 describes CloNe architecture, its supporting security functions and their interaction mechanisms. This CloNe security architecture aims to strengthen the CloNe architecture against the security challenges and vulnerabilities described in Schoo et al [12]. Fusenig et al [13] described holistic security architecture to address some of the security challenges of CloNe architecture.

The security architecture comprises of a security goal translation function as its backbone, which translates the security requirements given by the different entities in the provisioning infrastructure. The security goal translation translates the security requirements into concrete resource configurations and sends them to the resource administration interface for deployment on the underlying resource set. The security functions include the backbone security goal translation function, auditing and assurance function, access control policy function, and identity management function.

The auditing and assurance function ensures that the security goal translation function and its supporting security functions are functioning in accordance with the operating policies specified by the different participating entities of the provisioning infrastructure. The auditing and assurance function devised for the CloNe architecture builds upon the Cloud Audit specifications, and integrates seamlessly with the supporting functions of the CloNe security architecture. An important addition to the auditing and assurance function can be the integration of an intrusion detection system which provides an acceptable success rate defined and measured using a metric-based approach. The backbone intrusion detection algorithm shall be described in detail in Section 5.

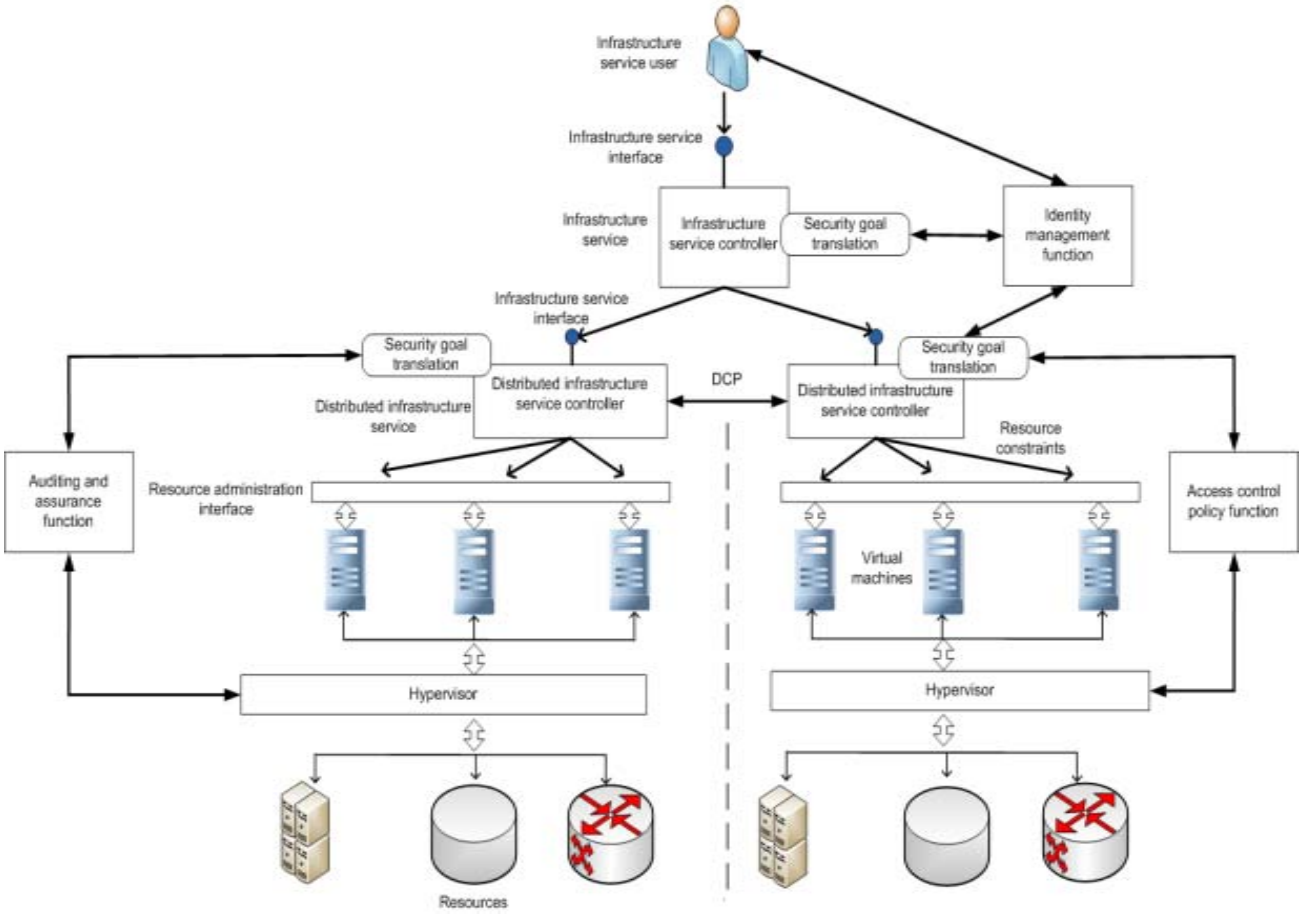

Figure 1: CloNe security architecture

IV. IDS ARCHITECTURE

The architecture of the IDS proposed in this paper is shown in Figure 2. This IDS consists of four modules: User Interface Module, Feature Selection Module, Classification Module, and Prevention module.

The user interface module collects the networks data from the KDD'99 cup data set. The feature selection module selects the necessary features based on genetic algorithms. The Classification module is used to classify the data by using the Fuzzy SVM [11]. The prevention module decides whether the decision made by the classification module on the first set of records is valid and prevents the attacks.

V. DETAILS OF THE PROPOSED IDS

In this paper, we propose a new intrusion detection system in which we have developed a new genetic algorithm based feature selection algorithm. Moreover, an effective classification algorithm called Fuzzy Support Vector Machines [11] has been used in this work for effective classification of network trace data. From the approaches used in this work, it was possible to find the intruders effectively.

A. Proposed Feature Selection Technique Using GA

Genetic based feature selection algorithm has been used in this work in order to select suitable subset of features so that they are potentially useful in classification. Another advantage of GA based feature selection in this work is that it finds and eliminates the redundant features if any because these redundant features may misguide in clustering or classification. The reduction in number of features reduces the training time and ambiguousness, thus a weighted sum genetic feature selection algorithm has been proposed which has increased global search capability and is better in attribute interaction when compared to other algorithms such as the greedy method.

B. Proposed Framework for Genetic Feature Selection

Subset generation use a method of heuristic search by Lasarczyk et al. [14], in which each instance in the search space specifies a candidate solution for subset evaluation. The decision process is determined by some basic issues. Initially, the search starting point is decided since it controls the direction of search. Feature selection search starts either with a null set with features added one by one or it starts with a full set of features and eliminates them one by one. Both these methods have the drawback of being trapped into local optima. In order to avoid this we employ a random search. Figure 3 shows the framework for our proposed genetic based feature selection approach. This framework uses genetic operations to identify & select the most relevant features of the 41 features present in the KDD cup data set.

Next, a search strategy is decided. A dataset with N features has 2N candidate subsets. This value is very large for moderate and large value of N. In our test case, there are 41 candidate subsets which are quite large. There are three different types of search strategies. They are complete, sequential, and random. Complete searches like branch and bound are exhaustive searches. Sequential search such as greedy hill climbing add or remove features one at a time and find optimal features.

Random search generates the subset in a completely random manner, i.e., it does not follow any deterministic rule. When compared to above two approaches, the utilization of randomness helps to avoid the local optima problem occurring in the heuristic search space to obtain an optimal subset.

1) Evaluation of Subset

After the subset is generated, it is evaluated using an evaluation criterion. The best or optimal subset of features obtained using one criterion may not be optimal according to another criterion. Based on the dependency of evaluation of a subset using the classification or clustering algorithm applied at the end, feature subset evaluation criterion can be classified into independent or dependent criterion. Commonly used independent criteria are distance, information, dependency, and consistency measures. If a feature incurs greater difference computed using the above criteria than other features, then the feature that incurs greater difference is considered. This evaluation criterion uses the intrinsic characteristics of the dataset without applying any classification or clustering algorithms.

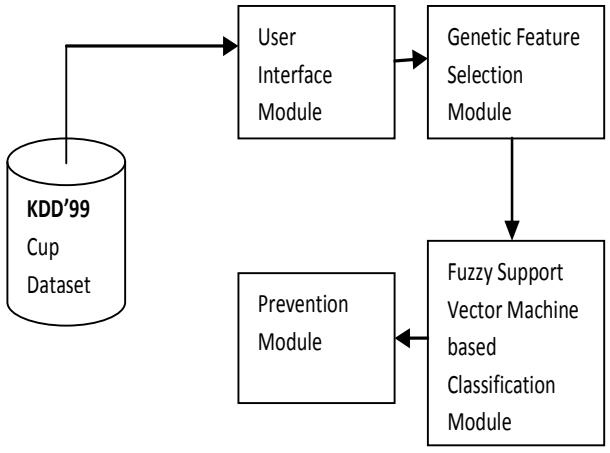

Figure 2: Proposed IDS architecture

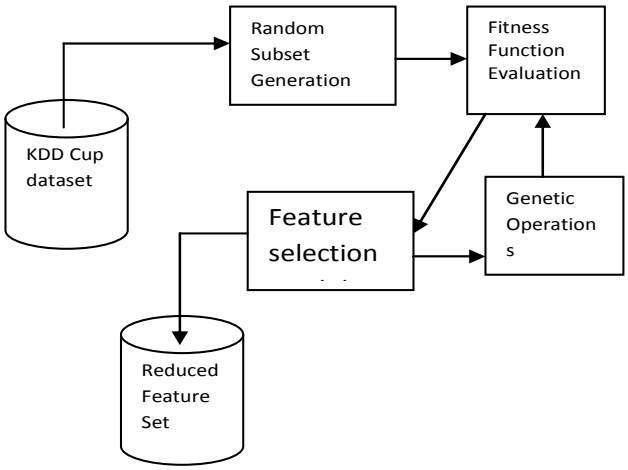

Figure 3: Feature Selection Systems

On the other hand, dependent criterion uses the performance of the classification or clustering algorithm on the selected feature subset in identifying essential features. This approach gives superior performance as it selects features based on the classification or clustering algorithm applied. The approach proposed uses dependent criterion for selecting significant features which are to be used in the detection process. Here predictive accuracy and feature count are used as the primary measures. Even though the computational complexity of this approach is higher than for an independent measure, it provides greater detection accuracy. Since feature selection is performed offline, the complexity involved in this is not related to the detection process and hence the time taken is immaterial.

2) Stopping Criteria

A stopping criterion determines when the feature extraction algorithm should stop. The proposed algorithm terminates, when any one of the following condition is met:
(i.) The search completes when the maximum number of iteration is reached or (ii.) When a good subset is selected i.e., the difference between previous fitness and current fitness is less than the given tolerance value.

3) Validation of Results

One direct way of result validation is based on the prior knowledge about the data. However, in real-world applications, such prior knowledge is not available. Hence, the proposed approach relies on an indirect method which monitors the change of the detection algorithm performance with a change of features. Experiments have been conducted with the full set of features and selected subset of features to compare the performance of classifier. From these experiments, it has been found that the detection accuracy is almost the same in both the cases. Therefore, feature selection can be carried out to improve the performance of the system. In addition, tenfold cross validation was performed to ensure the correctness of classification accuracy.

4) Proposed Genetic based Feature Selection Algorithm

Algorithm: Feature set selection using weighted sum GA.

Input: Network traffic pattern (All features), Number of generations, Population size, Crossover probability (Pc), Mutation probability (Pm).

Output: Set of selected features.

Genetic_Feature_Selection ( ) {

1. Initialize the population randomly with the size of each chromosome equal to the total number of features in the dataset which is equal to 41. Each gene value in the chromosome can be '0' or '1'. A bit value of '0' represents that the corresponding feature is not present in chromosome and '1' represents that the feature is present.
2. Initialize the weights W1 = 0.7, W2 = 0.3, N (total number of records in the training set), Pc and Pm.
3. For each chromosome in the new population {
   a. Apply uniform crossover with a probability Pc.
   b. Apply mutation operator to the chromosome with a probability Pm.
   c. Evaluate fitness = W1 * Accuracy + W2 * (1/ Count of Ones)}
4. If (Current fitness – Previous fitness < 0.0001) then exit
5. Select the top best 60% of chromosomes into new population using tournament selection.
6. If number of generations is not reached, go to line 3.

}

5) Experiment Test Bed

The simple test bed consisted of two computers with similar hardware (CPU: Intel Pentium i7-2720QM (6 MB cache, 2.20 GHz), RAM: 8 GB, NIC: Intel Ultimate-N 6300 (802.11 a/b/g/n), Hard Drive: Seagate 500GB) connected with a cross over cable. Each physical computer hosted five virtual machines (VMs) with Proxmox VE 1.8, an open source virtualization environment. Each VM was running a copy of Microsoft's Windows 7 operating system. We used IPv4 as the communication protocol stack in both the VMs and underlying operating system. Proxmox VE uses a bridged networking model. These bridges are similar to physical network switches, but implemented in software on the underlying Proxmox VE host. All VMs share a single bridge, thus it was as if virtual network cables from each guest were all plugged into a single physical switch. To avoid cross VM communication, VLANs (implementing IEEE 802.1q) are used to separate the networks as if each VM were separately connected to the underlying physical system. Each VM can act as a master or a slave depending on the deployed application. The master node can use resources of one or more slaves at any given time. Each VM has to authenticate every other VM before sharing resources. Even if a VM belongs to the same logical rack, they authenticate each other and communications are routed through the virtual router whose routing daemon is running on the underlying physical machine.

VI. RESULTS AND DISCUSSION

In this work, a new genetic based feature selection approach has been proposed and implemented in order to select subset of important features from the original feature set of KDD cup data set. The important features selected by the genetic based feature selection algorithm are used for classifying the data set in order to find the intrusions. In classification, the existing fuzzy SVM is used in this work. By this process, the 17 relevant features shown in **Table VI-2** have been generated by computing the weighted sum GA values from the 41 features shown in **Table VI-1**, using the proposed feature selection algorithm. From the experiments conducted using these features, it has been observed that feature selection reduces the training and testing time and at the same time produces similar accuracy as that of full feature set.

Table VI-1. Features of KDD Cup dataset

S.No	Feature Name	S.No	Feature Name
1	duration	22	is_guest_login
2	protocol_type	23	Count
3	service	24	serror_rate
4	src_byte	25	rerror_rate
5	dst_byte	26	same_srv_rate
6	flag	27	diff_srv_rate
7	land	28	srv_count
8	wrong_fragment	29	srv_serror_rate
9	urgent	30	srv_rerror_rate
10	hot	31	srv_diff_host_rate
11	num_failed_logins	32	dst_host_count
12	logged_in	33	dst_host_srv_count
13	num_compromised	34	dst_host_same_srv_count
14	root_shell	35	dst_host_diff_srv_count
15	su_attempted	36	dst_host_same_src_port_rate
16	num_root	37	dst_host_srv_diff_host_rate
17	num_file_creations	38	dst_host_serror_rate
18	num_shells	39	dst_host_srv serror rate
19	num_access_shells	40	dst_host_rerror_rate
20	num_outbound_cmds	41	dst_host_srv_rerror_rate
21	is_hot_login		

Table VI-2. 2 Name of the 17 selected features

Name of the selected features
protocol_type, service, flag, src_bytes, dst_bytes, wrong_fragment, hot, logged_in, count, serror_rate, same_srv_rate, diff_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_rerror_rate

Table VI-3 shows the comparison of detection rates between SVM and Fuzzy SVM when they are applied with 17 features returned by the feature selection algorithm. From this table, it can be observed that the detection accuracy of fuzzy SVM is higher than that of neural networks and SVM. Therefore, fuzzy SVM has been selected the proposed IDS intrusion detection system.

Table VI-4 provides the comparative analysis of error rates between SVM and Fuzzy SVM classifiers when they are applied with the 17 features returned by the feature selection algorithm. From this table, it has been observed that the error rate is less in the fuzzy SVM when it is compared with neural network and SVM.

Table VI-5 shows the comparison of the classifier SVM and Fuzzy SVM with full features and also with the fuzzy SVM classification with 17 features. From this table, it can be observed that the error rate is reduced in fuzzy SVM leading to increase in classification accuracy when it is compared with the other two methods. Moreover, the detection time is also reduced when fuzzy SVM is applied with the reduced number of features. The increase in classification accuracy is due to the fact that the confusions made by irrelevant attributes are eliminated by feature reduction. In addition, the classification time is reduced due to the reduction in the number of rules to be applied for decision making with reduced number of attributes.

Table VI-3. Detection Rate Comparisons of SVM and Fuzzy SVM Approaches with feature selection

Class Types	Total Test Samples	Detection Rate (%)	
		SVM	Fuzzy SVM
Normal	47911	96.03	98.75
DoS	7458	90.6	98.3
R2L	2754	53.74	85.48
U2R	200	83.5	89
Probe	2421	83.97	96.53

Table VI-4. Error Rate Comparisons of NN, SVM and Fuzzy SVM Approaches

Class Types	Total Test Samples	Error Rate (%)	
		SVM	Fuzzy SVM
Normal	47911	3.98	1.25
DoS	7458	5.41	2.70
R2L	2754	4.62	1.45
U2R	200	1.65	1.10
Probe	2421	1.60	1.47

Table VI-5. Comparison of SVM, Fuzzy SVM and Feature selected Fuzzy SVM Methods

Algorithm	Detection Accuracy (%)	Error Rate (%)	Training Time (Milli Sec)
SVM	83.5821	6.5147	846
FSVM	92.4612	5.2136	223
Feature Selection +FSVM	98.5123	3.134	112

Figure 4 shows the performance analysis for the four types of attacks namely DoS, Probe, User to Root (U2R) and Remote to Local (R2L) when they are detected with fuzzy SVM with 41 features and fuzzy SVM with 17 features. From **Figure 4**, it can be seen that the detection accuracy is improved when the fuzzy SVM is applied with 17 features. This is due to the fact that the fuzzy rules applied to 17 features are less in number and do not conflicting with each other during decision making.

Figure 5 depicts the false alarm rate produced by fuzzy SVM with 41 features and fuzzy SVM with 17 features in five experiments namely E1, E2, E3, E4 and E5. From the figure, it can be observed that the false alarm rate is reduced when the fuzzy SVM is applied with 17 features. This is due to the fact that the decision accuracy is greater in the feature selected FSVM.

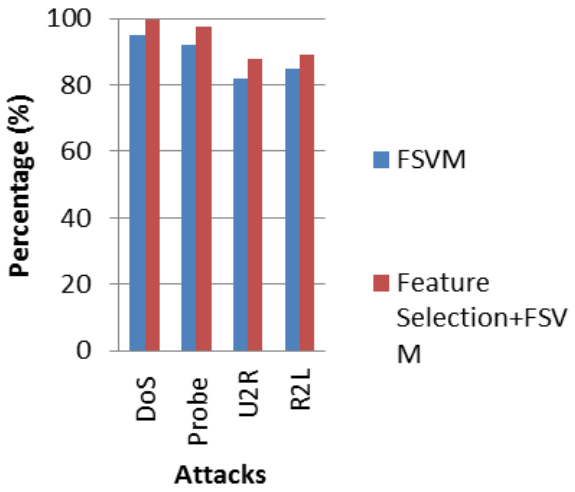

Figure 4: Performance analyses for attacks

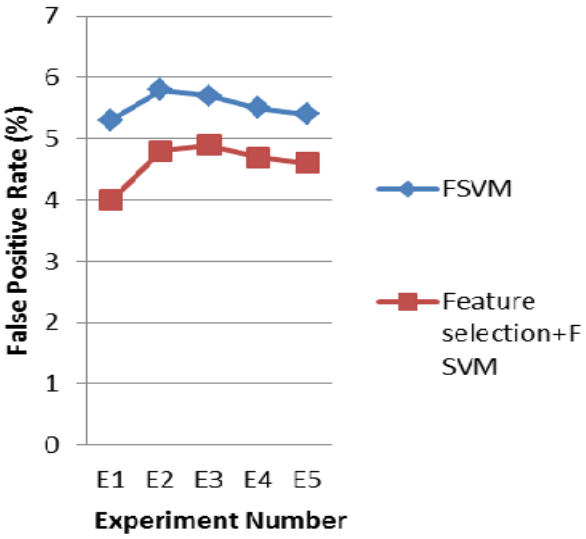

Figure 5: False alarm rate comparisons

VII. CONCLUSIONS AND FUTURE ENHANCEMENTS

In this paper, a new genetic based feature selection algorithm for cloud networks has been proposed. This algorithm is used to select optimal number of features from the KDD cup data set for intrusion detection. Moreover, a framework for intrusion detection that uses this feature selection algorithm and then applies the existing Fuzzy SVM for effective classification of intrusions using KDD Cup dataset for securing the cloud networks has been proposed. The main advantage of the proposed genetic algorithm based feature selection algorithm is that it improves the detection accuracy of the fuzzy SVM classifier by providing minimum and required number of features. This helps to reduce the classification time in addition to the increase in classification accuracy. Future work in this direction would extend the fuzzy SVM with rough sets to further improve the detection accuracy.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the European Commission for its funding through the "Scalable and Adaptive Internet Solutions", SAIL Project (FP7-ICT-2009-5-257448).

REFERENCES

1. Biying Zhang, "A Heuristic Genetic Neural Network for Intrusion Detection", 2011 International Conference on Internet Computing and Information Services, pp. 510-511, 2011.
2. Lei Li, Zhi-ping GAo, Wen-yan Dinl, "Fuzzy multi-class support vector machine based on binary tree in network intrusion detection", International Conference on Electrical and Control Engineering, pp.1043-1046, 2010.
3. DegangChen, QiangHe, XizhaoWang, "FRSVMs: Fuzzyroughsetbasedsupportvectormachines ", Fuzzy Sets and Systems, Vol. 161, pp. 596–607, 2010.
4. Jiaqi Jiang, Ru Li*,Tianhong Zheng,Feiqin Su, Haicheng Li, "A new intrusion detection system using Class and Sample Weighted C-Support Vector Machine, 2011 Third International Conference on Communications and Mobile Computing, pp.51-54, 2011.
5. Safaa Zaman and Fakhri Karray, "Fuzzy ESVDF approach for Intrusion Detection Systems",International conference on Advanced Information Networking and Applications pp.539-545, 2009.
6. Khalil El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems" IEEE Transactions on Parallel and Distributed Systems, Vol. 21, No. 8, pp. 1143-1149, 2010.
7. Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahidur Rahman, Chowdhury Mofizur Rahman, "Attacks Classification in Adaptive Intrusion Detection using Decision Tree", World Academy of Science, Engineering and Technology, Vol. 63, pp. 86-90, 2010.
8. Yuteng Guo,Beizhan Wang, Xinxing Zhao,Xiaobiao Xie, Lida Lin, Qingda Zhou, "Feature Selection Based on Rough Set and Modified Genetic Algorithm for Intrusion Detection", The 5th International Conference on Computer Science & Education, pp. 1441-1446, 2010.
9. Stein, Gary, Chen, Bing, Wu, Annie S., & Hua, Kien A. "Decision tree classifier for network intrusion detection with GA-based feature selection." Proceedings of the 43rd annual Southeast regional conference, Georgia: ACM Publisher, Vol. 2, pp. 136–141, 2005.
10. Cao Li-ying, Zhang Xiao-xian, Liu He, Chen Gui-fen, "A Network Intrusion Detection Method Based on Combined Model", International Conference on Mechatronic Science, Electric Engineering and Computer, pp.254-257, 2011.
11. Chun-Fu Lin, Shen-De Wang, "Fuzzy Support Vector Machines", IEEE Transactions on Neural Networks, Vol. 13, No. 2, pp. 464-471, 2002.
12. P. Schoo, V. Fusenig, V. Souza, M.Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for cloud networking security," in Mobile Networks and Management, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Heidelberg, 2010.
13. Volker Fusenig and Ayush Sharma. Security architecture for cloud networking. Presented in Proceedings of the 2012 International Conference on Networking and Computing, ICNC 2012, IEEE Computer Society, 2012.
14. Christian W.G. Lasarczyk, Peter Dittrich, and Wolfgang Banzhaf, "Dynamic Subset Selection Based on a Fitness Case Topology",Evolutionary Computation, Vol. 12, No. 2 , pp. 223-242, 2004.