International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183887

A Hybrid Model is Proposed Based in The Combination of Genetic and MAFS in Cloud Environment

[1]V. Chinnasamy, [2]Dr. D. Maruthanayagam
[1]Assistant Professor, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India
[2] Head/Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India

ABSTRACT

Cloud computing is being heralded as an important trend in information technology throughout the world. Data security has a major issue in cloud computing environment; An intrusion detection system (IDS) is a component that helps to detect various types of malicious network traffic which cannot be detected by a conventional firewall. Many IDS have been developed based on machine learning techniques. In recent growth, advanced detection approaches created by combining or integrating multiple learning techniques have shown better detection performance than general single learning technique. The feature representation method is an important pattern classifier that facilitates correct classifications, however, there have been very few related studies focusing how to extractor representative features for normal connections and effective detection of attacks. The objective of this paper is to suggest new security mechanisms using various trust approaches in broker based federated cloud architecture, ranking the providers with the help of regression tree approach using Service Measurement Index security attributes and new hybrid computation intelligence built on the combination of genetic with Artificial Fish Swarm in Intrusion Detection system.

Keywords : Intrusion Detection System (IDS), Genetic, Modified Artificial Fish Swarm (MAFS), Mechanism, Cloud Computing and Regression.

I. INTRODUCTION

Developing a high performance IDS is a very complicated research challenge for the researchers and mainly classification accuracy depends on the features extraction from the dataset [1]. Computation intelligence techniques are used to classify the inward network traffics as either normal or malicious. A lot of computational intelligence approaches have been proposed by the researchers, for example artificial neural network, fuzzy sets, evolutionary computation, expert system approach, rule based approach, artificial immune systems etc. [2]. Denial of Service (DoS) is a type of attack that tries to prevent legitimate users from accessing either the services or resources. Neptune, smurf, Pod and Teardrop are the types of DoS attacks that have been present in KDD CUP 99 datasets. DoS attacks have been emerging attacks that create threat to business and Internet providers around the world. Intelligent computational mechanism is needed to encounter this type of attacks and extend safety environment that increases the confidence of the users to use Internet business. IDS are examined with large amount of data that causes slow training, testing process and low detection rate. So, feature extraction is the challenging task in developing IDS [3].

1.1 Types of Intrusion Detection System

Intrusion Detection Systems **(IDS)** are broadly classified based on the location of audit data, detection of malicious activity and type of action triggered after identified the malicious activity. IDS are classified as either Network based or Host based depends on the location where the audit data collected. Network IDSs (NIDSs) type is used to analyze the network traffic [4]. The level of detection may vary depending on the computational intelligence provided with in the NIDS to another, but most of them have modules in charge of analyzing traffic from the network, transport, and application layers in the OSI model. NIDSs are normally placed outside the system being monitored but in the same network segment, thus enabling them to monitor a complete LAN. Host IDSs (HIDS) is used to analyze the local data of the devices. Most of them analyze the sequence of system calls for the programs running in the device. Within these sequences, optimal HIDS analyze system calls arguments, memory registers, stack states, system logs, user behaviors, etc. The level of performance may vary depending on the computational intelligence provided with in the HIDS.

The classifications depending on the detection of malicious activity are misuse-based, anomaly based and hybrid. Misuse detection category is working based on the behaviors and distinguishes it as either normal or irregular. Anomaly detection [5] is the identification of items, events or observations which do not conform to an expected pattern or other items in a dataset. The type of action triggered when a malicious behavior is detected, an IDS can be active or passive:

(a) **Passive IDS**: when a malicious behavior is detected, an alert is raised and no further action is taken.

(b) **Active IDS**: apart from raising an alert, the IDS try to neutralize the malicious data by executing a predefined action. Some authors refer to active IDSs as Intrusion Prevention System (IPS).

In this work, signature based hybrid model is proposed based on the combination of genetic and MAFS techniques and evaluate the performance of the system.

II. RELATED WORK IN INTRUSION ETECTION SYSTEM UNDER CLOUD ENVIRONMENT

Knowledge-based systems, also called misuse detection systems [6], operate based on a database of known attack signatures. Whenever they encounter an activity matching a signature stored in the database, the corresponding alarm is generated. The advantage of such systems is that their alarms are meaningful, i.e., they contain diagnostic information about the cause of the alarm. On the other hand, their main drawback lies in the system component that enables the generation of meaningful alarms, i.e., the database. The database of attack signatures needs to be kept up-to-date, which is a tedious task because new vulnerabilities and attacks are discovered on a daily basis.

Eddy et al. [7, 8] redefine the audit source location by adding the categories application log files and IDS sensor alerts. This modification takes into account the differences in granularity of log data generated on a host. Furthermore, The addition of IDS sensor alerts reflects the trend to hierarchical ID architectures, in which several IDSs send their alerts to a higher-level instance where the alerts are analyzed and possibly aggregated. The resulting alerts may then be sent to the next-higher instance or presented to the security officer.

Tadashi Dohi et al. [7] described two detection modes such as automatic detection mode and manual detection mode for intrusions in Scalable Intrusion Tolerant Architecture (SITAR) by a continuous-time semi-Markov chain (CTSMC). Based on the Markov chain (EMC) approach, the steady-state system availability and the mean time to security failure (MTTSF) were computed. The necessary and sufficient condition to exist the optimal switching time from an automatic detection mode to a manual detection mode, which maximizes the steady-state system availability, is also found. An adaptive mode control scheme to estimate the optimal switching time without specifying the associated probability distribution function, whose idea behind is based on a statistically non-parametric algorithm by means of the total time on test concept.

Anomaly based Intrusion Detection Systems learn normal and anomalous behavior by analyzing network traffic in various benchmark datasets. Common challenges for IDSs are large amounts of data to process, low detection rates and high rates of false alarms. A new computational technique based on the Online Sequential Extreme Learning Machine (OS-ELM) is presented for intrusion detection. The proposed technique uses alpha profiling to reduce the time complexity while irrelevant features are discarded using an ensemble of Filtered, Correlation and Consistency based feature selection techniques. A new feature-selection approach based on the cuttlefish optimization algorithm which is used for intrusion detection systems (IDSs). Because IDSs deal with a large amount of data, one of the crucial tasks of IDSs is to keep the best quality of features that represent the whole data and remove the redundant and irrelevant features.

This model uses the cuttlefish algorithm (CFA) as a search strategy to ascertain the optimal subset of features and the decision tree (DT) classifier as a judgement on the selected features that are produced by the CFA. An intrusion detection technique based on the calculation of trust of the neighboring node was proposed. Each node observes the trust level of its neighboring nodes. Based on these trust values, neighboring nodes may be declared as trustworthy, risky or malicious. Trustworthy nodes are recommended to the forwarding engine for packet forwarding purposes. The proposed scheme successfully detects Hello flood attack, jamming attack and selective forwarding attack by analyzing the network statistics and malicious node behavior.

A novel feature representation approach, namely the cluster center and nearest neighbor (CANN) approach was proposed [9], in that approach, two distances are measured and summed, the first one based on the distance between each data sample and its cluster center, and the second distance is between the data and its nearest neighbor in the same cluster.

Then, this new and one-dimensional distance based feature is used to represent each data sample for intrusion detection by a k-Nearest Neighbor (k-NN) classifier. The experimental results based on the KDD-Cup 99 dataset show that the CANN classifier not only performs better than or similar to k-NN and support vector machines trained and tested by the original feature representation in terms of classification accuracy, detection rates, and false alarms. It also provides high computational efficiency for the time of classifier training and testing.

A rule-based pattern matching system model [9, 10] was developed, verified against usage of the system and any significant deviation from the normal usage is flagged as abnormal usage. This model served as abstract model for further developments in the field and is known as the generic intrusion detection model.

All the existing systems can be trained for certain behavior gradually making the abnormal behavior as normal, which may make the intruders undetected. Determining the threshold above which an intrusion should be detected is a difficult task. Setting the threshold too low results in false positives and setting it too high results in false negatives). Attacks, which occur by sequential dependencies, cannot be detected, as statistical analysis is insensitive to order of events.

Based on Gavaskar et al. [11] GA is among the most effective tools for searching in large search spaces also it imposes couple of mathematical constraints the same shape as the function of optimization. Moreover, GA strategy is used to get the optimal group of features along with the optimal parameters for any kernel function.GA produces enhanced recognition models that contains some features and parameters through the iterative procedure for reproduction. The proposed hybrid system based on evolutionary algorithm reduces the false alarm rate and increases the rate of accuracy detection.

Authors [10] developed a classifier using an artificial immune system (AIS) combined with population-based incremental learning (PBIL) and collaborative filtering (CF) for network intrusion detection. AIS is a powerful tool in terms of extirpating antigens inspired by the principles and processes of the natural immune system. PBIL uses past experiences to evolve into new species through learning and adopting the idea of CF for classification. The novelty of this work is in its combining of the three above mentioned approaches to develop a new classifier which can be applied to detect network intrusion, with incremental learning capability, by adapting the weight of key features. In addition, four mechanisms: creating a new antibody using PBIL, dynamic adjustment of feature weighting using clonal expansion, antibody hierarchy adjustment using mean affinity, as well as usage rates, are proposed to intensify AIS performance.

Hidden Naïve Bayes (HNB) model [11] can be applied to intrusion detection problems that suffer from dimensionality, highly correlated features and high network data stream volumes. HNB is a data mining model that relaxes the Naïve Bayes method's conditional independence assumption. Our experimental results show that the HNB model exhibits a superior overall performance in terms of accuracy, error rate and misclassification cost compared with the traditional Naïve Bayes model, leading extended Naïve Bayes models and the Knowledge Discovery and Data Mining (KDD) Cup 1999 winner. This model performed better than other leading state-of-the art models, such as SVM, in predictive accuracy. The results also indicate that this model significantly improves the accuracy of detecting denial-of-services (DoS) attacks.

An adaptive blacklist-based packet filter [12] using a statistic-based approach was developed as IDS to improve the performance of a signature-based NIDS. The filter employs a blacklist technique to help filter out network packets based on IP confidence and the statistic-based approach allows the blacklist generation in an adaptive way, that is, the blacklist can be updated periodically.

III. PROPOSED WORK OF THE TRUST MECHANISMS IN FEDERATED CLOUD AND INTRUSION DETECTION SYSTEM

Comparing with all the works present in the literature, broker based architecture is proposed, different trust mechanism are suggested to compute the trust score, based on the trust score, the providers are shortlisted, using regression tree approach the best provider is assigned for the service. The IDS proposed in this thesis is different in many ways. First, it provides a unique architecture for a hybrid IDS that considers both misuse and anomaly. Second, this thesis proposes new computational techniques based on genetic and artificial fish swarm optimization. Third, it uses the standard KDD CUP 99 Dataset for carrying out the experiments. Grade and grade value model is used to compute the trust score, based on that value providers are shortlisted and best provider is selected based on the concept of decision tree.

3.1 Proposed Genetic-MAFSA Based IDS

The design and their implementation of Genetic-MAFSA based IDS have following phases such as, Preprocessing, Feature Selection and Classifier. The architecture of the proposed GA-MAFSA model is shown in Figure-1. The architecture contains two phases (1) Training phase (ii) Testing phase. In training phase, the KDD CUP 99 datasets was used, Data pre-processing, feature selection using genetic algorithm and classifier using MAFSA were implemented in training stage and DoS patterns were identified. Second stage is testing stage, the captured traffic is evaluated as in training stage, pattern identified, matched with database and decision to be taken. New patterns were identified by analyzing the behavior of the traffic, if it was against the legitimate traffic; the pattern was captured and updated in the database.

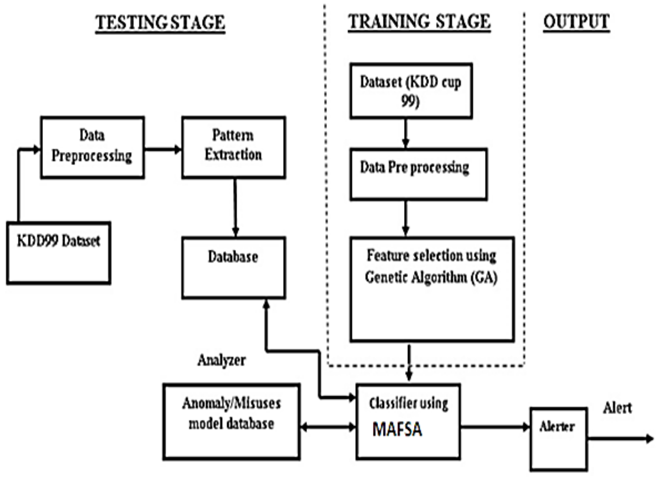

Figure-1: Architecture of Genetic-MAFSA based IDS

3.2 Data Preprocessing

Data Preprocessing is an important step in the machine learning computing that eliminates out of range values, impossible data combinations, missing values etc. Generally data preprocessing includes learning, normalization, transformation, feature extraction and selection. The output of the data preprocessing is the final training set that extracts

Knowledge for the testing phase. The following steps used for data preprocessing.

a) Identifying features and its related values.
b) Converting original feature data value in to numerical data value.
c) Applying data normalization based on min-max normalization.
d) Perform similarity check and remove null values.

3.3 Feature Selection Based on GENETIC Algorithm

Accuracy of the classifier depends on the selection of optimum feature subset. Feature selection method mainly used for selecting subset of features from the original data set. There are two feature selection methods that are already proposed namely filter and wrapper methods. Filter method was mainly based on general characteristics of data features without involving machine language. These features are ranked based on certain criteria, where features with highest rank values are selected as optimal. The main advantages of filter method are low computational cost without involving any machine language algorithm for future selection. Frequently used filter method is information gain method. Wrapper method is mainly used for feature subset selection from the data set based on objective function and analysis of the performance of feature subset.

In this chapter, Genetic Algorithm is used to select optimal feature subset from the datasets. GA reduces the KDD cup 99 features from 41 attributes to 6 attributes features that are related to the characteristics of DoS attack, which reduces 85% of feature space. The six attributes are protocol_type, src_bytes, dst_bytes, count (No of connection to the same host), srv_count (No of connection requesting same service), serror_rate. KDD'99 dataset contains huge number of redundant records. 10% portions of the full dataset contains two types of DoS attacks (Smurf and Neptune). These two types constitute over 71% of the testing dataset which completely affects the evaluation.

Brief Steps about Genetic algorithm that selected features from dataset is presented as algorithm below:

- Initialize a population of Pre-processed data.
- Calculate objective function for each individual.
- Selection of individual solution.
- Perform mating of pair of individuals.
- Perform mutation operation.
- Calculate objective function for newly created population.
- If it satisfies stop the operation.
- Otherwise repeat step-3.
- Return the best features from KDD 99 dataset that reflects the properties of DoS

3.4 Modified Artifical Fish Swarm Algorithm as Classifier

In the initial work, there is a problem in the global, single and feasibility optimization in multidimensional function. To overcome these difficulties, a modified artificial fish swarm algorithm (MAFSA) is proposed. AFSA is the swarm intelligence approach which operates according to the population and stochastic search. AFSA objective function is defined as a food consistence degree in water area. At last, AFs reach to a point which its food consistence degree is highest (global optimum). In this algorithm basic behavior of AFSA is changed. The basic behaviors of AFSA are prey, follow, and swarm.The proposed algorithm includes two parts, preprocessing and mining. The first part offers procedures which are used for estimating the fitness values of AFSA. In this part, the data are transformed and stored in a binary format. After that search range of the particle swarm is set with the help of the IR (item set range) value. The important goal of the system is the MAFSA algorithm is applied to mine the association rules are in the second part of the algorithm. Initially, we process with AFSA encoding, this step is related to chromosome encoding of genetic algorithms. Produce a population of AFSA based on the estimated fitness value is the next step. As a final point, the AFSA searching process takings until the condition is attained i.e., the best AF is found. The minimal support and minimal confidence are represented by the support and confidence of the best AF. Consequently, we can utilize this minimal support and minimal confidence for further association rule mining.

3.5 Calculation of IR Value

This study applies the AFSA in association rule mining, as well as in the calculation of IR value which is included in encoding process. The aim of such an insertion is to generate more significant association rules. Moreover search efficiency is increased when IR analysis is utilized to decide the rule length generated by chromosomes in AFSA. IR analysis is used to minimize the meaningless item sets in the process of AF swarm evolution. This approach addresses the front and back partition points of each chromosome, and the range decided by these two points is referred as IR which is shown in equation (1), IR =[log(mTransNum(m)) + log(nTransNum(n))]

= Trans(m, n) / TotalTrans --- (1)

In the equation 1, $m \neq n$ and $m < n$. where "m" is defined as the length of the item set and TransNum(m) means the number of transaction records containing m products. "n" is defined as the length of the itemset and TransNum(n) means the number of transaction records containing n products. Trans (m, n) is the number of transaction records purchasing m to n products. TotalTrans means the number of total transactions.

3.6 Encoding

Based on the general principle of association rule mining, the connection of the association rule of item set X to item set Y (X → Y) must be empty. Items which appear in the item set X do not appear on item set Y, and vice versa. Thereafter, the IR value calculated is employed to choose the front and back partition points of the chromosomes. In the chromosome coding, the item set before the front partition point is called "item set X," while that between the front partition and back partition points is called "item set Y". In this work the chromosome encoding scheme is "string encoding". Each value represents a different item name, which means that item 1 is encoded as '1' and item 2 is encoded as '2'. The representative value of each item is encoded into a string type chromosome by the consequent order.

IV. SIMULATIONS AND RESULT DISCUSSIONS

The proposed computational intelligence based Intrusion Detection System was implemented in Mat Lab. During the evaluation, 10 percent labeled data of KDD CUP 99 was used for training the proposed IDS. This dataset contains three types of traffics and six types of DoS attacks about four gigabytes and each traffic record has 41 features names whose values facilitate to identify the type category either as normal or attack. It contains a total of 24 attack types that fall into four major categories such as Denial of Service (DoS), probe, User to Root (U2R), Remote to User (R2L). DoS attacks are difficult to deal with because they are very easy to launch, difficult to track and also it is not easy to refuse the requests of the attacker.

A host-based intrusion detection system can monitor the size of the tcpd connection data structure and alert a user if this data structure nears its size limit. Ping of Death attack has been reported when the systems react in an unpredictable fashion when receiving oversized IP packets. Possible reactions include crashing, freezing and rebooting. Ping of Death can be identified by noting the size of all ICMP packets and flagging those that are longer than 64000 bytes.

Based on the description above, the following rule structure derived from the KDD CUP 99 dataset and it is given in the Table-1. In this proposed model, the hidden related information from the features was observed. Learners discussed among others, about possible potential variations in traffic records which help to realize the prior knowledge of anomalous behaviors in advance. This proposed computational technique facilitates prompt detection and distinction of possible individual traffic records from crowd. There are 97,277 normal and 3, 91,450 DoS attacks traffic records in 10 percent labeled KDD CUP 99 data set. 2,80,790 smurf, 107201 Neptune, 2203 back, 979 teardrop, 21 land and 264 pod are in the10 percent labeled KDD CUP 99. After removing duplicated instances class, 97277 normal, 641 smurf, 51820 Neptune, 994 back, 19 land, 918 teardrop, 206 pod are the traffic records considered for training the KDDIDS.AKDD CUP 99 dataset is shown in Table-1. After PSO, the extended rule set identified with respect to each attack is shown in Table 2. Effectiveness of the IDS is evaluated by its ability to make correct predictions. Events are successfully labeled as normal and attacks. False positives refer to normal events being predicted as attacks. False negatives are attack events incorrectly predicted as normal events. Detection Accuracy (DA) is defined as the ratio of the sum of true negative and positive rate and sum of true and false positive and negative rate.

The simulation results show that performance variations among evolutionary algorithms that where used as computational intelligence in IDS are less. Clustering based algorithms performance is better compared to non-clustered. Results reveal that no evolutionary algorithm performs better for all type of DoS attacks. Simulation results of the proposed techniques are shown in Table-3. Compared to the existing, proposed technique is efficient. It reduces more false negative compared to the existing work that reveals in the simulation results in Table-3.In this work, new computational technique was proposed by extracting the role of Genetic and MAFSA. The proposed method performs the classification task and extracts required knowledge using Genetic and MFSA.

The proposed systems are high reliability and adequate interpretability, and are comparable with several well-known algorithms such as Fuzzy clustering. Results on intrusion detection data set from KDD cup-99 repository show that the proposed approach would be capable of classifying intrusion instances with high accuracy rate in addition to adequate interpretability of extracted rules. The results of MAFSA are better than fuzzy clustering technique. In future work, Ant Colony based Optimization technique will be used and their performance will be compared with some existing weight based algorithms.

Sad

TABLE-1. RULE STRUCTURE OF DOS ATTACKS IN KDD CUP 99 DATASETS

Sl. No.	Attack Description	Attack Type
1.	protocol=ICMP,Service=ecr_i,src_byte=1032, flag=SF, host_count=255	Smurf
2.	protocol=tcp,service=private or ctf, flag=SO or SF, serror_rate=1	Neptune
3.	protocol=tcp,service=http, flag = SF or RSTFR,src_byte=54540,dst_byte=7300 or 8314,	Back
	same_srv_rate=1,srv_count>=5	
4.	protocol=UDP,service=SF,src_byte=28,wrong fragment=3,dst_host_count=255	Teardrop
5.	protocol=tcp,service=finger,flag=SO,land=1,srv_count=2,dst_host_srv_error_rate>=0.17	Land
6.	Protocol=ICMP,service=ecr_i,flag=SF,src_byte=1480,wrong_fragment=1,dst_host_count=255,dst_host_diff_srv_rate=0.02	Pod

TABLE-2. EXTENDED RULE SET OBSERVED FROM THE PROPOSED TECHNIQUES

Sl. No.	Attack Description	Attack Type
1.	If (Duration <3) and (protocol_type=icmp) and(dst_byte=125016) Then Buffer overflow	smurf
2.	if {the connection has following information: source IP address 124.12.5.18; destination IP address:130.18.206.55; destination port number: 21; connection time: 10.1 seconds } Then {stop the connection}.	Neptune
3.	protocol=tcp,service=http, flag = SF or RSTFR,src_byte=54540,dst_byte=7300 or 8314, same_srv_rate=1,srv_count>=5	back
4.	If (source_bytes> 265616) and (source_bytes<= 283618) Then Warezmaster Attack	teardrop
5.	If (Duration 0 to 25) and (protocol_ type = tcp and UDP) and (service=ftp OR private OR other domain)	land
6.	If(duration<10seconds) of an FTP connection /session, there are many Hot indicators (hot > 20) being set by a logged user then it is highly likely that is being executed	Pod

TABLE-3. RESULTS OBTAINED FROM THE SIMULATION

Test Data	Training Data	Test data	Deduction accuracy (%)	
			GA-MAFSA	FUZZY CLUSTERING
Normal	97277	60255	99.5	99.2
Smurf	641	400	83	96
Neptune	51820	20500	96	98
Back	994	714	98	96
Teardrop	918	300	96	96
Land	19	07	94	99
Pod	206	101	99.5	98

V. CONCLUSION

In this paper, new computational technique is proposed by extracting the role of Genetic and MAFSA. The proposed method performs the classification task and extracts required knowledge using Genetic and MAFSA. The proposed systems are high reliability and adequate interpretability, and are comparable with several well-known algorithms such as Fuzzy clustering. Results on intrusion detection data set from KDD cup-99 repository show that the proposed approach would be capable of classifying intrusion instances with high accuracy rate in addition to adequate interpretability of extracted rules. The results of MAFSA are better than fuzzy clustering technique. In future work, Ant Colony based Optimization technique will be used and their performance will be compared with some existing weight based algorithms.

VI. REFERENCES

[1]. Daejoon Joo, Taeho Hong and Ingoo Han, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors," Expert System with Applications 25, 2003, pp.69-75.

[2]. Davide Ariu, Roberto, Tronci, Giorgio Giacinto, "HMMpayl: An Intrusion Detection System based on Hidden Markov Models" Journal of computers and Security, vol 30 issue 4 2011 pp 221-241.

[3]. Yeo, C., Buyya, R.: Integrated Risk Analysis for a Commercial Computing Service. In: Proc. of the 21st IEEE International Parallel and Distributed Processing Symposium, Long Beach, California, USA March 2007.

[4]. Sulistio, A., Kim, K., Buyya, R.: Managing Cancellations and No-shows of Reservations with Overbooking to Increase Resource Revenue. In: Proceedings of the 8th IEEE International Symposium on Cluster Computing and the Grid, Lyon, France, May 2008.

[5]. Fujun Feng, Chuang Lin, Dongsheng Peng and Junshan Li: A Trust and Context Based Access Control Model for Distributed Systems. In 10th IEEE International Conference on High Performance Computing and Communications, 629–634, 2008.

[6]. Yogendra Kumar Jain and Upendra, "An Efficient Intrusion Detection based on Decision Tree Classifier Using Feature Reduction," International Journal of Scientific and Research Publication, Volume 2, Issue 1, pp. 1-6, January 2012

[7]. Tadashi Dohi, Toshikazu Uemura, "An adaptive mode control algorithm of a scalable intrusion Tolerant Architecture", Journal of computer and system sciences, Vol 8], 2012, pages 1751-1774.

[8]. W. T.Luke Teacy, Michael Luck, Alex Rogers, Nicholas R.Jennings, " An Efficient and Versatile Approach to trust and Reputation Using Hierachical Bayesian Modelling", Journal of Artificial Intelligence Vol.193, 2012, pages 149-185.

[9]. Wei-Chao lin, Shih Wen ke, Chih-Fong Tsai, " CANN: An intrusion Detection system based on combining cluster centers and nearest neighbors", Journal of knowledge based systems vol 78 2015 pages 13-21.

[10]. Meng-Hui Chen, Pei-Chann Chang, Jheng-Long Wu, "A population based incremental learning approach with artificial immune system for Network Intrusion Detection", Journal of Engineering Applications of Artificial Intelligence, Jan 2016 .

[11]. Levent Koc, Thomas A Mazzuchi, Shahram Sarkani, "A Network Intrusion Detection system based on a Hidden Naïve Bayes Multiclass Classifier", Journal of Expert Systems with Applications Vol 39 Dec 2012, pages 13492-13500.

[12]. Yuxin Meng, Lam For Kwok, "Adaptive Blacklist based Packet Filter with a Statistic based Approach in Network Intrusion Detection", Journal of Network and Computer Applications Vol 39, 2014 pp 83-92.