JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, Jun 2018 E-ISSN: 2347-2693

Anomaly Detection System using Ant Agent Rule Based Multiclass Support Vector Machine (AA-RB-MSVM) Algorithm

A. Manimaran[1*]

[1*]Assistant Professor, Madanapalle Institute of Technology & Science, Madanapalle, India

[*]Corresponding Author: drmanimaranca@gmail.com

Available online at: www.ijcseonline.org

Accepted: 22/Jun/2018, Published: 30/Jun/2018

Abstract— A lot of resources and computing facilities are afforded by Cloud computing through the Internet. It attracts many users with its advantageous features. Despite of this, Cloud system experience several security issues. Distributed Denial of Service (DDoS) attacks is the most dangerous attack in the cloud computing environment. Hence, it is important to develop an Intrusion Detection System (IDS) to detect the attacker with high detection accuracy in the cloud environment. This work proposes an anomaly detection system named Ant Agent Rule Based Multiclass Support Vector Machine (AA-RB-MSVM) Algorithm at the hypervisor layer which is a hybrid approach of various algorithms like Ant Colony Algorithm, Rule based Approach and Support Vector Machine Algorithms to progress the precision of the detection system. The DARPA's KDD cup dataset 1999 is used for experiments. The proposed algorithm shows high detection accuracy and low false positive rate based on the experimental observation when compared with the existing algorithms.

***Keywords*—** DDoS attack, Resource Availability, Cloud Computing, Soft Computing.

I. INTRODUCTION

Cloud computing [1] is scrutinized as the revolution into realism of a long held vision called "Computing as Utility". It is transpired into the market with colossal potential to accomplish the vision, guarantee on-demand services for a customer's software, platform and infrastructure needs. It is defined as [1]" A system, where the resources of data center is shared using visualization technology, which also provide elastic, on demand and instant services to its customers and charges customer usage as utility bill". The Figure 1 depicts the definition of the Cloud computing.

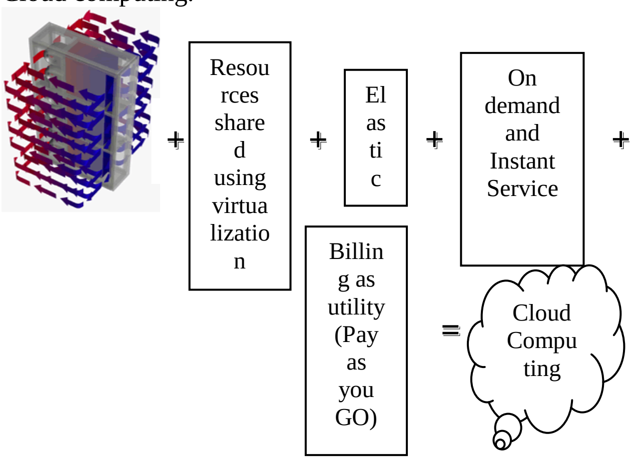

+
Resources shared using virtualization
+
Elastic
+
On demand and Instant Service
+
Billing as utility (Pay as you GO)
=
Cloud Computing

Figure 1: Definition of Cloud Computing

Organizations are now uploading their cosmic capacity of indispensable information into public cloud. The information uploaded in the cloud [2] is susceptible to security hazards like accessibility, concealment and reliability of those organizations. The unremitting facility of cloud technology is the rationale which invites the interlopers to misuse the resources and services afforded by Cloud Service Provider (CSP). Firewall and Intrusion Detection System (IDS) are the enduring solutions suggested to preserve the user's data and cloud resources from malevolent activities. Research finding concerning about the security issues was released by organizations to assist companies which are interested in Cloud Computing. Distributed Denial of Service attacks (DDoS) attacks are intricate to detect by the Firewall. DDoS is an augmented and advanced form of Denial of Service Attacks which targets the remote data centers and floods the servers with massive amount of packets causing unavailability of services to the legitimate users [2]. A traditional-network based or host-based intrusion detection system does not suit for virtual cloud environment [3]. Hence, to protect the Cloud Computing environment from DDoS attack, an anomaly detection system at hypervisor layer [4] should be developed.

Section I contains introduction about the cloud computing and overview of this paper. Anomaly detection in virtual cloud environment is discussed in the section II. Section III provides the related works on attack detection using machine learning techniques. Proposed framework AA-RB-MSVM explanation part is in section IV. Section V describes results and discussion. Section VI concludes research work with future directions.

II. ANOMALY DETECTION IN VIRTUAL CLOUD ENVIRONMENT

To satisfy the requirements of users with lower cost, Cloud computing offered computing facilities and storage resources through Internet. This revolutionary model with its increasing improvements is vulnerable against security threats. As the services are delivered over the internet, the security and privacy on the public network should be a severe concern. An anomaly detection system is needed in the virtual cloud environment to overcome the problems with traditional computing environments.

Hypervisor is a bit of programming, firmware that makes and executes virtual machines. It is the product layer that executes on equipment stage. A machine on which the hypervisor is running virtual machines is eluded as host machine. Hypervisor (VMM) has capacities to screen and look at the system construct and host based occasions in light of virtual environment. Hypervisor gives a virtual working stage and deals with the operation of visitor machines. Each host machine is given a virtual hypervisor that runs independently from host machine. The virtual hypervisors screen the genuine equipment frameworks which give single stage to various VMs. This capacity gives hypervisor based virtualization to obtain a safe framework. The hypervisor, as an equipment component, is utilized to find system based interruption. Hypervisor Detector screens the virtual system activity (system based occasions) to catch the system information and break down it. The Hypervisor Detector is knowledgeable about the database of typical exercises; any deviation from this is advised as irregular action [5]. The representation of Cloud Architecture with Hypervisor Detector is shown in Figure 2.

Virtual machines execute client application process on single equipment stage. Because of its element develop, the virtual machines can powerfully alter their states (new, execute, slaughter). VM can move from one stage to other with no conditions. VM can be stopped up, balanced and be barren. Virtual machines on a solitary equipment stage run different applications that can be put away on various areas of the host machine. Because of element nature of cloud base [5], it is workable for the virtual calculation environment to migrate itself and scale its assets over a multi-area.

Virtualization [6] is to bear the cost of parallel and intuitive access to a vast pool of data focus that backings various cases of OS running on solitary equipment stage and can control the different OS sequentially bringing about equipment virtualization. Hypervisor grants numerous occasions of OSes to share equipment offices on which it is facilitated. The working framework introduced and executed on a virtual machine is called Guest OS. The Hypervisor screens and executes [6] the visitor working framework running on the virtual machines working on it.

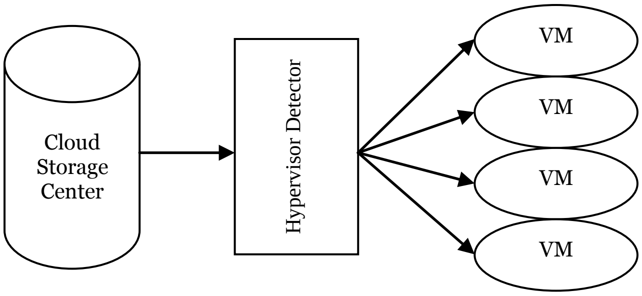


Figure 2: Cloud Architecture with Hypervisor Detector

III. RELATED WORKS

Wang and Gombault [7] proposed a channel choice technique utilizing IG and chi-squared to concentrate nine most critical elements in the system movement. Bayesian system and C 4.5 (a choice tree classifier) were utilized to distinguish DDoS assault in the system. Results got demonstrate that the discovery precision continues as before while the general proficiency made strides. Bolon-Canedo et al. [8] consolidated discretizers, channels and classifiers to enhance the arrangement execution by fundamentally diminishing the list of capabilities. This was connected to both binary and multi-class arrangement issues utilizing KDD Cup '99 benchmark dataset.

A directed inductive learning approach, Group Method for Data Handling (GMDH), was proposed in [9] utilizing solid and ensemble based procedures. Channel highlight choice strategies utilizing IG, Gain Ratio and GMDH were utilized to rank elements amid the pre-preparing stage. Lin et al. [10] proposed an oddity interruption location that identifies new assaults utilizing Support vector machine (SVM), choice tree (DT) and Simulated Annealing (SA). The best elements were chosen from the KDD '99 dataset utilizing SVM and SA to enhance the characterization precision of DT and SVM, to distinguish new assaults. Li et al. [11] proposed a continuous element evacuation strategy that procedure dataset preceding clustering technique, ant colony algorithm and SVM to arrange system movement as either ordinary or abnormality.

Sindhu et al. [12] proposed a wrapper strategy for highlight choice to expel superfluous occurrences from a list of capabilities to accomplish higher identification exactness utilizing neuro tree. A component determination methodology was proposed in [13] utilizing Bayesian system, and NSL-KDD dataset was utilized to assess the chose highlights. Discoveries demonstrated that these elements diminished the assault recognition time and enhanced the grouping exactness and in addition the genuine positive rates. Bhattacharya et al. [14] proposed a multi-measure multi-weight positioning approach that distinguishes imperative system highlights by joining wrapper, channel and bunching strategies to allot various weights to every element. Harsh set component choice methodology has ended up being a productive scientific instrument in light of upper and lower estimation. It presents square with grouping ability with negligible subset.

Olusola et al. [15] proposed a rough set-based component determination technique that chooses essential elements from information utilizing KDD '99 dataset. Sengupta et al. [16] outlined an online interruption location framework (IDS) utilizing both unpleasant set hypothesis and Q-learning calculation to accomplish a greatest characterization calculation that groups information as either ordinary or irregularity utilizing NSL-KDD system movement information. A quick characteristic diminishment calculation taking into account harsh set hypothesis was proposed. The calculation distinguishes imperative elements and disposes of free and excess ascribes to accomplish a powerful arrangement execution.

Akramifard et.al [17] proposed intrusion detection systems for cloud environment using multi-level fuzzy neural networks. Captured data can be classified using two efficient concepts such as Fuzzy min-max neural network and Multi-level fuzzy min-max neural network to identify the appearances of malicious intruders on the cloud environment. Different attributes of the data are considered to examine the user’s behavior pattern. An experimental result shows that the system reduces the false positive rate and false negative rate and increase the attack detection rate.

Bhat et.al [18] designed VMM – IDS anomaly detection system for cloud virtual machines using machine learning techniques. Proposed approach detects the malicious request at the cloud VMM level using naïve bayes tree algorithm and Random forest classifiers. KDD’99 datasets are used to classify the attackers using random forest classifiers and naïve bayes algorithm applied to improve the detection rate. Proposed system proved that the low false alarm rate and high attack detection rate from the experimental results.

Sondhiya et.al [19] introduced Multi Layer Perceptronb (MLP) algorithm of Artificial Neural Networks to detect unknown intruders in cloud environment. MLP algorithm works based on error-correction learning rule, using forward pass and backward pass. Proposed approach projected the neural network soft computing technique to identify the unknown attackers efficiently in cloud environment.

Ramteke et.al [20] recommended novel methodology to detect intruders in cloud VM level using FC-ANN techniques. Fuzzy Clustering and Artificial Neural Network techniques together capture the new attack patterns and store it into IDS database for maintain high detection accuracy. System architecture has capture and queuing modules, analysis/processing module, and reporting module. Multi-threaded IDS placed in the cloud Virtual Machine to handle large number of packet flow. Heterogeneous training sets can be divided into numerous homogeneous subsets using fuzzy clustering technique to reduce the complexity and increase the detection rate.

Mahmoudpou et.al [21] addressed new methodology to detect distributed denial of service attack using fuzzy neural network and evolutionary algorithm. Proposed combination method consists of pre-processing, training data, base phase system, and set parameters by evolutionary algorithm. Adaptive Neural - Fuzzy Inference System (ANFIS) is used to design nonlinear mapping among input and output node. Differential Evolutionary Algorithm applied to calculate the real value functions using evolutionary strategies. Experimental results illustrate that the proposed algorithm achieved optimal results than the existing machine learning techniques.

Anitha et.al [22] represented a real time DDoS attack detection system using Cumulative Sum (CUSUM) algorithm and Adaptive Neuro-Fuzzy Inference System (ANFIS). CUSUM algorithm is used to track variations of the attack characteristic variable X(n) from the observed traffic and threshold value set to raise an alarm. To avoid false alarm rate due to traditional threshold value, ANFIS applied to remove abnormality and select appropriate member function based on CUSUM values. Experimental results prove that the proposed method yield better accuracy using well known “CAIDA” DDoS attack dataset.

A Network Based Intrusion Detection (NIDS) [23] component was developed in Cloud Computing by using Snort and Apriori Algoithm. It is integrated into cloud computing environment to monitor the traditional and virtual network. An intrusion detection component [24] was developed to detect the DDoS attack, by installing Snort in the Virtual switch to capture the network traffic. Nature of the attack is analyzed by the traffic details and informed to the virtual server. Virtual server block the IP address of the malware action in case of any threat issues found. Grid and Cloud Computing Intrusion Detection System (GCCIDS) [3] was proposed which employ an audit system. To discover the intrusions, knowledge and behaviour analysis is integrated with this system. Behaviour analysis was done by using the Artificial Neural Network. Event auditor is used to capture the data from various resources. Based on the data collected, the IDS detect the intrusion

An Intrusion detection system [25] was developed at the Virtual machine monitor layer by using Naïve Bayes and a hybrid approach which combines Naïve Bayes and Random Forest to control and analyze the network flow among the virtual machines in the cloud environment.

IV. FRAMEWORK OF AA-RB-MSVM

In this section, the new approach Ant Agent and Rule Based Multiclass Support Vector Machine Algorithm (AA-RB-MSVM) Algorithm is elaborated. The whole framework of the AA-RB-MSVM Algorithm is discussed with two modules: (i) Feature Reduction and (ii) Classification.

(i) Framework of IDS Based on Ant Agent, Rule and Support Vector Machine Algorithm

At the preliminary level, the data required for the evaluation is taken from the KDD Database. After collecting the required data, the Feature reduction is done at the First Stage. The reduced number of Features is used in Stage II to classify the user as legal user and attacker. Figure 3 explains the framework of the AA-RB-MSVM Algorihtm

Stage I : Feature Reduction is done by calculating the Information Gain Ratio (IGR) and by comparing the IGR with Threshold Value.

Stage II: Ant agent is used to split the dataset into two clusters, and rule is used to identify the legal user and attacker.

(ii) Feature Reduction Module

This stage is done by using the attribute selection and tuple selection. For attribute selection, rules and IGR is used. The data set 'D' is divided into 'n' number of classes C_i. The attributes F_i are chosen based on the maximum number of non-zero values by agent.

Step 1: Calculate the IGR for each attribute A_i ε D by using (3).

$$Info(D) = -\sum_{j=1}^{m}\left[\frac{freq(Cj,D)}{\|D\|}\right]\log_2\left[\frac{freq(Cj,D)}{\|D\|}\right] - (1)$$

$$Info(F) = \sum_{i=1}^{n}\left\|\frac{Fi}{F}\right\| * \inf o(Fi) \qquad --(2)$$

$$IGR(Ai) = \left(\frac{Info(D) - Info(F)}{Info(D) + Info(F)}\right) * 100 \qquad --(3)$$

Step 2: Choose an attribute A_i from D with maximum IGR Value.

Step 3: Split the data set D into subsets (D_1, $D_{2,}$ D3, D_4 ……………D_m) based on the values from A_i, where C_j → jth attribute of class C.

Step 4: Find all the attributes whose IGR Value is greater than the Threshold Value where Threshold Value = 0.5.

Step 5: Store the selected attributes in Set R, and output it.

(iii) Classification Module

This stage is done by using the Ant Agent. Ant Agent automatically determines the number of clusters that are critically required as input for classification purpose and so there will be a decrease in the rate of false positive in the system.

Step 1: Import the selected attributes R from the database.

Step 2: Select two initial cluster by applying Ant based Agents.

Step 3: Compute the Minkowski distance between two classes.

$$dij = \left(\sum_{i=1}^{n}\left\|x_{ik} - x_{jk}\right\|^{p}\right)^{1/p} \qquad ------->(4)$$

$$p \rightarrow order\ \ and\ \ find\ \ Centroid\ \ of\ each\ \ class$$

$$Centroid\ \ C_i = \sum_{m=1}^{nt} x^i m / n_i \qquad ------>(5)$$

```
Step 4: if (d(A,B) > d (A,C)) then
            B is assigned as Normal
      else
            C is assigned as Normal
```

Step 5: Compute mutual information value and check with alarm threshold

$$\overline{Average\ Alarm\ \ Threshold = E \geq\ l\overline{\xi},}\quad DDoS\ occurs$$

$$where, \qquad \overline{\xi} = \frac{1}{n-1}\sum_{ii=1}^{n-1}\left\|\xi_{jii}\right\| \qquad ->(5)$$

$$n \rightarrow total\ \ number\ \ of\ \ alarm\ tests$$

$$l \rightarrow abnormal\ \ value\ \ which\ are\ picked\ as\ invalid$$

$$Alarm\ threshold$$

$$ii(i = ii = n-1) \rightarrow ii\ th\ \ al\ arm\ threshold\ test$$

$$\overline{E} = Mean\ Entropy$$

$$\overline{E} = \sqrt{\frac{Info(D)^2 + Info(F)^2 + IGR(Ai)^2}{3}} \geq 0 \quad ->(6)$$

```
Step 6: If mutual information value is greater than or equal to alarm threshold then
                  Accept the record
      else
                  Reject the Record.
```

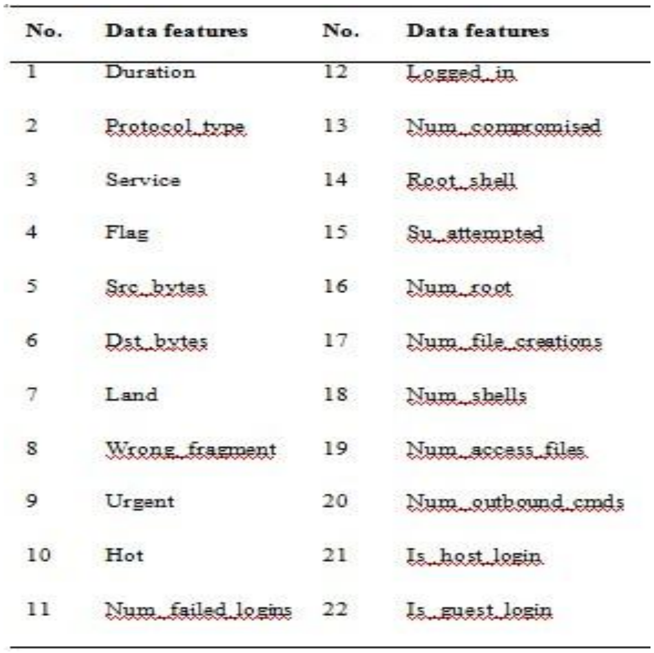
V. Results and Discussion

To evaluate the performance of the approach, the IDS dataset from KDD is used. The proposed algorithm is implemented on Matlab environment.

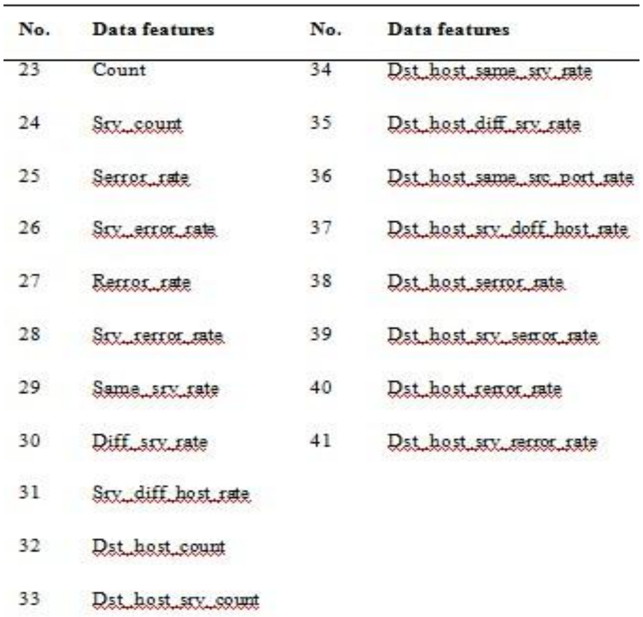
(i) Data Preparation

Table 1 represents the KDD cup Dataset attribute features for experimentation.

Table 1. NSL-KDD dataset features



No.	Data features	No.	Data features
1	Duration	12	Logged_in
2	Protocol_type	13	Num_compromised
3	Service	14	Root_shell
4	Flag	15	Su_attempted
5	Src_bytes	16	Num_root
6	Dst_bytes	17	Num_file_creations
7	Land	18	Num_shells
8	Wrong_fragment	19	Num_access_files
9	Urgent	20	Num_outbound_cmds
10	Hot	21	Is_host_login
11	Num_failed_logins	22	Is_guest_login



No.	Data features	No.	Data features
23	Count	34	Dst_host_same_srv_rate
24	Srv_count	35	Dst_host_diff_srv_rate
25	Serror_rate	36	Dst_host_same_src_port_rate
26	Srv_error_rate	37	Dst_host_srv_doff_host_rate
27	Rerror_rate	38	Dst_host_serror_rate
28	Srv_rerror_rate	39	Dst_host_srv_serror_rate
29	Same_srv_rate	40	Dst_host_rerror_rate
30	Diff_srv_rate	41	Dst_host_srv_rerror_rate
31	Srv_diff_host_rate		
32	Dst_host_count		
33	Dst_host_srv_count		

(i) Evaluation Criteria

The measures taken for evaluating the performance are:

$$\Pr ecision = \frac{TP}{TP + FP} \quad ---------> (7)$$

$$\operatorname{Re} call = \frac{TP}{TP + FN} \quad ----------> (8)$$

$$Detection\ Accuracy = \frac{TP + TN}{TP + TN + FP + FN} * 100 \quad ----> (9)$$

$$False\ Positive\ Rate = \frac{FP}{FP + TN} * 100 \quad -------> (10)$$

By using the proposed Algorithm, the total number of attributes is reduced to eight. The reduced attributes are service, src bytes, wrong fragment, srv_count, dst_host_count,dst_host_srv_count,dst_host_same_src_port_rate and dst_host_srv_diff_host_rate. The proposed algorithm is compared with existing Support Vector Machine (SVM) Algorithm and Fuzzy Clustering-Artificial Neural Network (FC-ANN) Approach. Figure 4 gives the number of attributes reduced by the proposed algorithm and existing Algorithms. Figure 5 depicts the time of execution taken by the algorithms. It is observed that the proposed algorithm reduced the number of attributes to minimum when compared with the existing algorithms, and time taken for execution is also less when compared with existing algorithms.

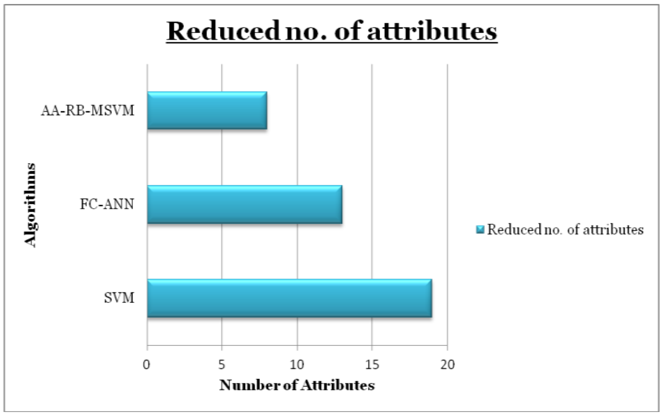


Figure 4: Reduced no.of attributes

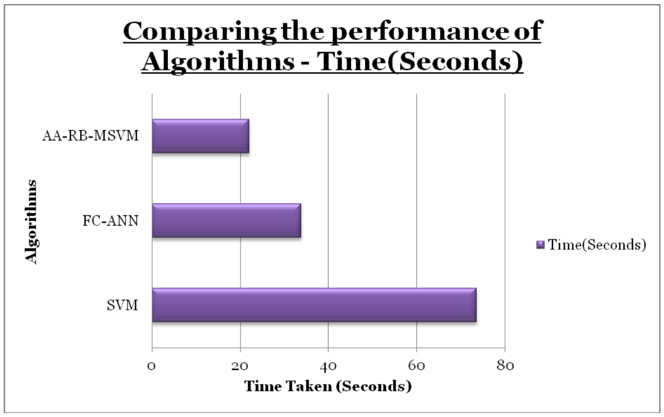


Figure 5: Comparing the performance of Algorithms – Time (Seconds)

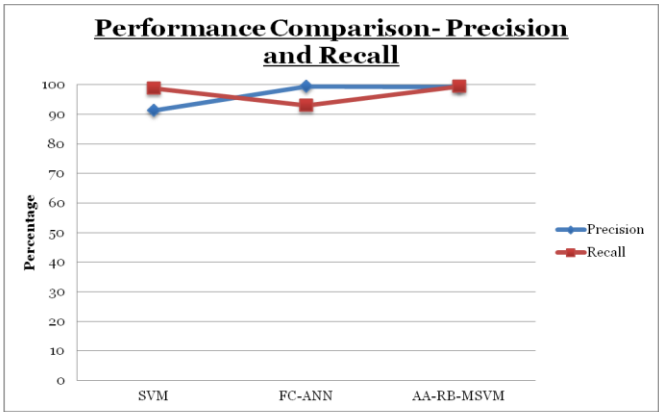


Figure 6: Performance Comparison – Precision and Recall

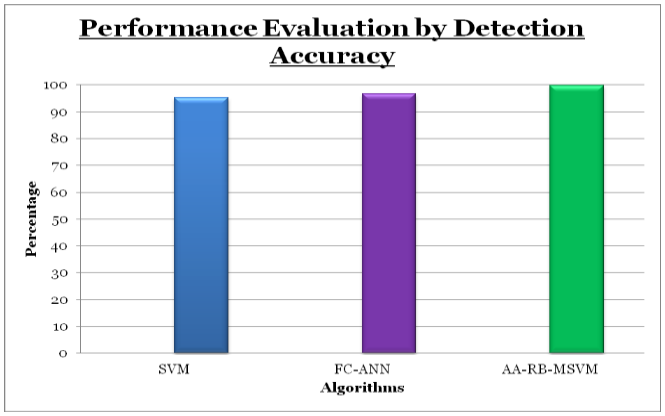


Figure 7: Performance Evaluation by Detection Accuracy

Figure 6 evaluates the performance of the algorithm by using the metrics, precision and recall. The values obtained by using the proposed AA-RB-MSVM Algorithm is better when compared with other two algorithms. Figure 7 and Figure 8 justifies the performance of the proposed algorithm by comparing the detection accuracy and False Positive Rate. It is observed that the proposed algorithm shows increased level of accuracy and also there is a reduction in the rate of false positive rate too.

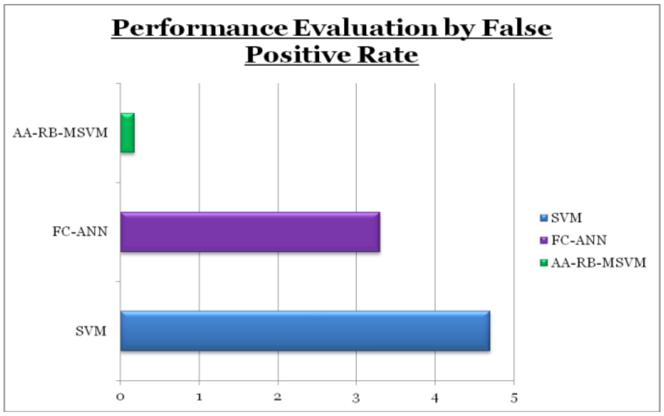


Figure 8: Performance Evaluation by False Positive Rate

VI. Conclusion and Future Scope

This work proposes an anomaly detection algorithm called Ant Agent Rule Based Multiclass Support Vector Machine (AA-RB-MSVM) Algorithm at the virtual machine monitor layer. It is designed with a hybrid approach which combines Ant Colony Algorithm, Rules Based Concept and Support Vector Machine Algorithm. This works in two phases. The first phase is the Feature reduction phase which reduces the number of attributes from 41 to 8. The second phase is the classification plase, which classifies the user as legal or attacker. The proposed algorithm shows a promising results with a high detection rate of 99.82% and also the false positive rate is reduced to 0.18%. Hence, the proposed algorithm is suggested as a better one for detecting the DDoS attacks with reduced false positive rate. Future scope of this research work is to implement this framework in the real cloud environment in order to solve real world problems for maintaining cloud resource availability to its intended users.

References

[1] Md. Tanzim Khorshed, A.B.M Shawkar Ali, Saleh A. Wasimi, " A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems, Vol 28, 2012, pp 833-851.

[2] Hai J, Guofu X, Deqing , "AVMM-based intrusion prevention system in cloud computing environment", J Supercomputer Springer Science, Bus Media 66(3):1133–1151. 2013

[3] Vishnu Patidar, Makhan Kumbhkar, "Analysis of Cloud Computing Security Issues in Software as a Service", International Journal of Scientific Research in Computer Science and Engineering, Vol.2, Issue 3, pp 1-5, June 2014.

[4] Pandeeswari.N, Ganesh kumar, "Anomaly detection system in Cloud Environment using Fuzzy Clustering based ANN", Mobile Network and Applications, Vol 21 (3), pp 494-505, August 2015.

[5] A Bala, Y Osais, “Modelling and simulation of DDOS Attack using SimEvents”, International Journal of Scientific Research in Network Security, Vol 2(1), pp 39–45,2013.

[6] Vinothina V, Sridaran R, Padmavathi G,” A survey on resource allocation strategies in cloud computing”, International Journal of Advanced Computer Science Applications, Vol 3(6), pp 97–104, 2012

[7] W Wang, S Gombault, W Wang, S Gombault, Proceedings of the 3rd International conference on Risks and Security of Internet and Systems (CRiSIS’08), in Efficient detection of DDoS attacks with important attributes(IEEE, Tozeur, 2008), pp. 61–67

[8] V Bolon-Canedo, N Sanchez-Marono, A Alonso-Betanzos, Feature selection and classification in multiple class datasets: an application to KDD Cup 99 dataset. Expert Syst Appl 38(5), 5947–5957 (2011)

[9] Z Baig, S Sait, A Shaheen, GMDH-based networks for intelligent intrusion detection. Eng Appl Artif Intel 26(7), 1731–1740 (2013)

[10] S Lin, K Ying, C Lee, Z Lee, An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. Appl Soft Comput 12(10), 3285–3290 (2012)

[11] Y Li, J Xia, S Zhang, J Yan, X Ai, K Dai, An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Syst Appl 39(1), 424–430 (2012)

[12] S Sindhu, S Geetha, A Kannan, Decision tree based light weight intrusion detection using a wrapper approach. Expert Syst Appl 39(1), 129–141 (2012)

[13] F Zhang, D Wang, Proceedings of the 8th International Conference on Networking, Architecture and Storage (NAS), in An effective feature selection approach for network intrusion detection (IEEE, Xi’an, 2013), pp. 307–311

[14] S Bhattacharya, S Selvakumar, Multi-measure multi-weight ranking approach for the identification of the network features for the detection of DoS and Probe attacks. Compt. J. 1-21 (2015)

[15] A Olusola, A Oladele, D Abosede, in Proceedings of the World Congress on Engineering and Computer Science. Analysis of KDD’99 intrusion detection dataset for selection of relevance features (San Francisco, USA, 2010), pp.1-7.http://www.iaeng.org/publication/WCECS2010/WCECS2010_pp162-168.pdf

[16] G Geng, N Li, S Gong, The Proceedings of International Conference on Industrial Control and Electronics Engineering (ICICEE), in Feature Selection Method for Network Intrusion Based on Fast Attribute Reduction of Rough Set (IEEE, Xi’an, 2012), pp. 530–534

[17] Akramifard, H., et al. "Intrusion Detection in the Cloud Environment Using Multi-Level Fuzzy Neural Networks." Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2015.

[18] Bhat, Amjad Hussain, Sabyasachi Patra, and Debasish Jena. "Machine learning approach for intrusion detection on cloud virtual machines." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2.6 (2013): 56-66.

[19] Sondhiya, Richa, Maneesh Shreevastav, and Mahendra Mishra. "To improve security in cloud computing with intrusion detection system using neural network." Int. J. Soft Comput. Eng 3.2 (2013).

[20] Ramteke, Swati, Rajesh Dongare, and Komal Ramteke. "Intrusion Detection System for Cloud Network Using FC-ANN Algorithm." International Journal of Advanced Research in Computer and Communication Engineering 2.4 (2013).

[21] Mahmoudpour, Saeid, and Seyed Javad Mirabedini. "Diagnosis of Distributed Denial of Service Attacks using the Combination Method of Fuzzy Neural Network and Evolutionary Algorithm." Indian Journal of Science and Technology 8.28 (2015): 1.

[22] Anitha, R., et al. "A Real Time Detection of Distributed Denial-of-Service Attacks Using Cumulative Sum Algorithm and Adaptive Neuro-Fuzzy Inference System." Advances in Computer Science, Engineering & Applications. Springer Berlin Heidelberg, 2012. 773-782.

[23] Chirag NM, Dhiren RP, Avi P, Muttukrishnan R (2012) Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing. In: Proceedings of 2nd International Conference on Communication, Computing & Security, Procedia Technology, 6:905–912. doi:10.1016/j.protcy.2012.10.110

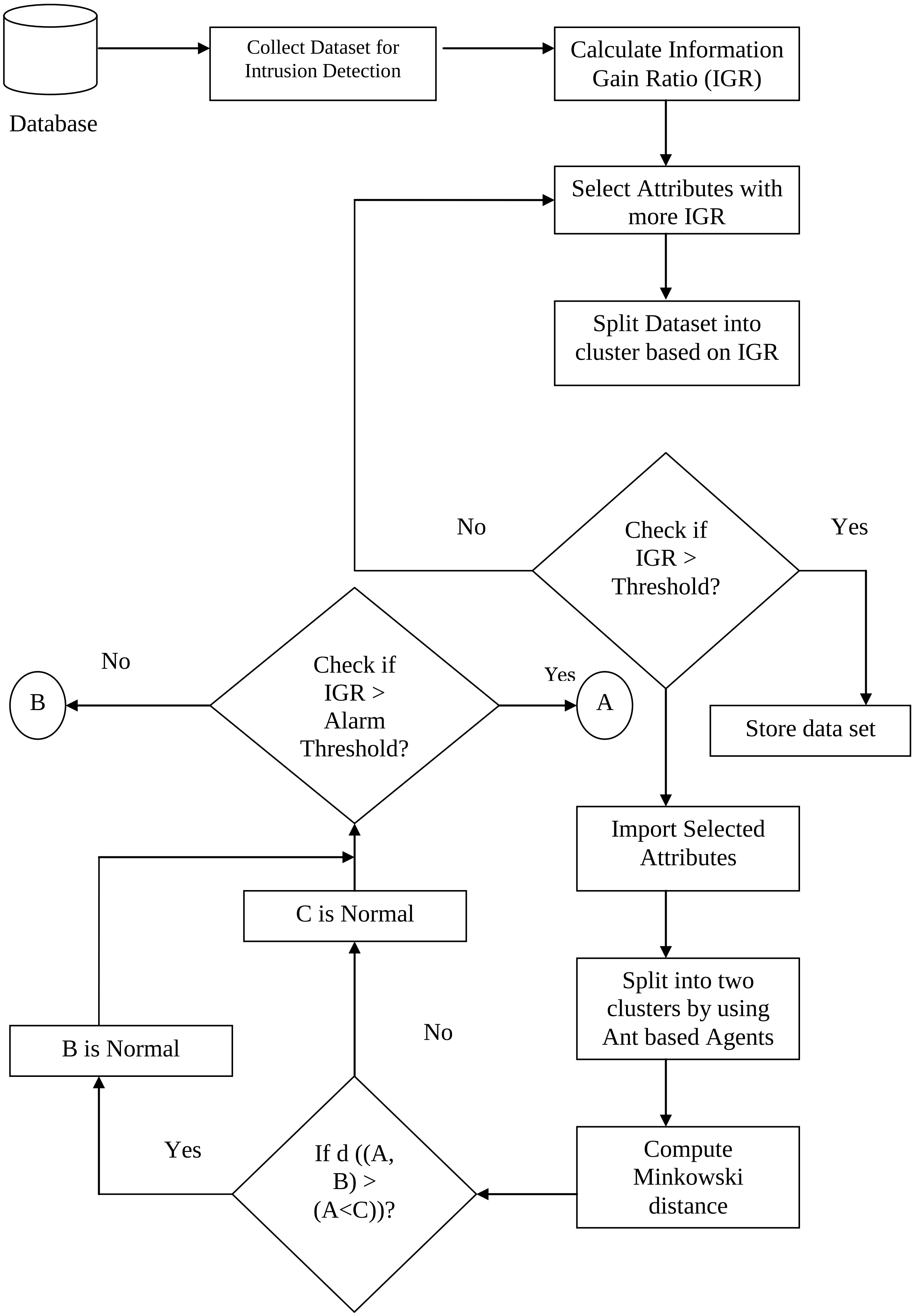
[24] Bakshi A, Yogesh B (2010) Securing cloud from DDOS attacks using intrusion detection system in virtual machine. In: Proceedings of second International Conference on Communication Software and Networksp260–264. doi:10.1109/ICCSN.2010.56

[25] Amjad HB, Sabyasachi P, Debasish J (2013) Machine learning approach for intrusion detection on cloud virtual machines. Int J Appl Innov Eng Manag 2(6):57–66

Authors Profile

Dr. A. Manimaran pursed Bachelor of Science from Bharathidasan University, Trichy in 2006, Master of Computer Applications from Anna University in year 2009 and Ph.D from Bharathidasan University in 2018. He is currently working as Assistant Professor in Department of Computer Applications, Madanapalle Institute of Technology & Science, Andhra Pradesh. He has published 9 research papers in reputed international journals. His main research work focuses on Network Security, Cloud Computing and Internet of Things. He has 4 years of Teaching Experience and 4 years of Research Experience.

.


Database
Collect Dataset for Intrusion Detection
Calculate Information Gain Ratio (IGR)
Select Attributes with more IGR
Split Dataset into cluster based on IGR
No
Check if IGR > Threshold?
Yes
Store data set
No
B
Check if IGR > Alarm Threshold?
Yes
A
Import Selected Attributes
Split into two clusters by using Ant based Agents
Compute Minkowski distance
C is Normal
B is Normal
No
Yes
If d ((A, B) > (A<C))?

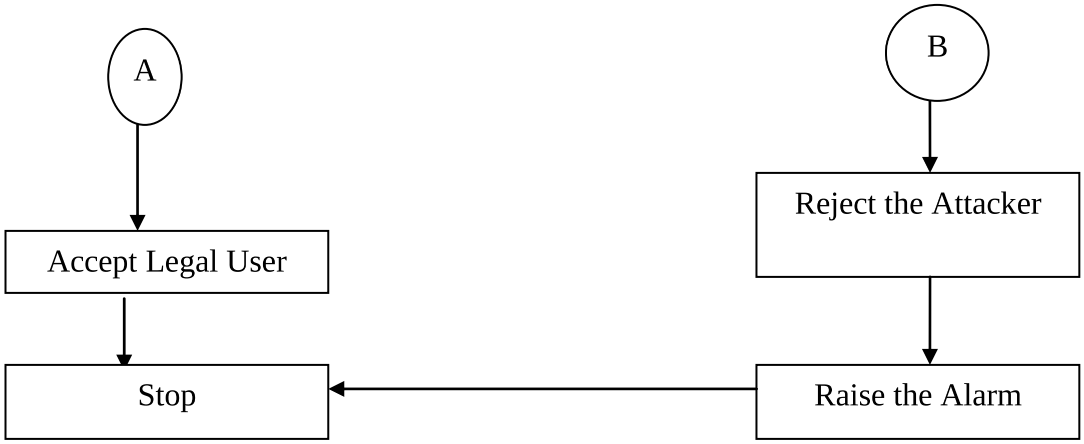


Figure 3: Framework of the AA-RB-MSVM Algorithm