Intrusion Detection System For Cloud Computing

Vikrant G. Deshmukh, Atul G. Borkut, Nikhil A. Agam
Department of Computer Engineering
Indira College of Engineering and Management
Pune, Maharashtra, India

Abstract

Today, Cloud computing has emerged in recent years as a major segment of the IT industry; however, Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario. One of the security issues is how to reduce the impact of denial of-service (DoS) attack or distributed denial-of-service (DDoS) or many other different attacks in this environment. To counter these kinds of attacks, a framework of intrusion detection system (IDS) is proposed. The proposed system could detect various computer attacks by examining various attacker data record observed in processes on the network.IDS is a security layer over cloud server used to detect ongoing intrusive activity in network. Artificial Neural Networks (ANN) can be used to detect the intrusion in the system but there is slight complication that ANN lacks in certain areas that are detection precision for low frequent attacks and detection stability. So we have decided to implement FC-ANN approach based on ANN and fuzzy clustering, to solve the problem. The general procedure of FC-ANN is as follows: firstly fuzzy clustering technique is used to generate different training subsets. Subsequently, based on different training subsets, different ANN models are trained to formulate different base models. Finally, a meta-learner, fuzzy aggregation module, is employed to aggregate these results.

Keyword: Cloud Computing, IDS, ANN, FC-ANN, DoS, DDoS.

1. INTRODUCTION

In recent year, Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Basically Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it.

The advantages of using cloud computing are:

1) Reduced hardware and maintenance cost.
2) Accessibility around the globe.
3) Flexibility and the highly automated process

Where in the customer need not worry about software up-gradation which tends to be a daily matter many researchers have gone through the security issues in cloud computations [3]. For considering this security issue, many researchers purpose different IDSs time to time for building strong security layer over network layer.

In Intrusion detection attempts to detect computer attacks by examining various data records observed in processes on the network some of these IDS's combine features of two or more IDSs which are called as Hybrid Intrusion Detection Systems. Most of the researchers combine the features of Signature based detection methodology and Anomaly based detection methodology.

For a signature based IDS if an attacker attacks slowly and organized, the attack may go undetected through the IDS, as signatures include factors which are based on duration of the events and the actions of attacker do not match. Sometimes, for an unknown attack or new attack there is no signature updated or an attacker attack in the mean time when the database is updating. Thus, signature-based IDS fail to detect unknown attacks. Anomaly based IDS suffer from many false-positive readings. Thus there is a need to hybridize those IDS which can overcome the shortcomings of each other [2]

In this paper we proposed a new approach to ANN-based Hybrid IDS, FC-ANN to which is more efficient than the traditional IDS (Intrusion Detection System)[1].Among these techniques, Artificial Neural Network (ANN) is one of the widely used techniques and has been successful in solving many complex practical problems. And ANN has been successfully applied into IDS. However, the main drawbacks of ANN-based IDS exist in two aspects [16]:

(1) Lower detection precision, especially for low-frequent attacks, e.g., Remote to Local (R2L), User to Root (U2R).
(2) Weaker detection stability.

To solve the above two problems, we propose a novel approach for ANN-based IDS, FC-ANN, to enhance the detection precision for low-frequent attacks and detection stability. The general procedure of FC-ANN approach has the following three stages. In the first stage, a fuzzy clustering technique is used to generate different Training subsets. Based on different training sets, different ANNs are trained in the second stage. In the third stage, in order to eliminate the errors of different ANNs, a meta-learner, fuzzy aggregation module, is introduced to learn again and combine the different ANN's results. The whole approach reflects the famous philosophy ‘‘divide and conquer”. By fuzzy clustering, the whole training set is divided into subsets which have less number and lower complexity. Thus the ANN can learn each subset more quickly, robustly and precisely, especially for low-frequent attacks, such as U2R and R2L attacks.

To illustrate the applicability and capability of the new approach, the results of experiments on KDD CUP 1999 dataset demonstrated better performance compared to BPNN and other well-known methods such as decision tree. The rest of this paper is organized as follows[1].

2. RELATED WORK

A. Intrusion detection in the cloud

In the paper [7], Roschke and Cheng et al. have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. The intrusion detection message exchange format (IDMEF) standard has been used for communication between different IDS sensors. The authors have suggested the deployment of IDS sensors on separate cloud layers like application layer, system layer and platform layer. Alerts generated are sent to “Event Gatherer” program. Event gatherer receives and convert alert messages in IDMEF standard and stores in event data base repository with the help of Sender, Receiver and Handler plug-ins. The analysis component analyzes complex attacks and presents it to user through IDS management system. The authors have proposed an effective cloud IDS management architecture, which could be monitored and administered by the cloud user. They have provided a central IDS management system based on different sensors using IDMEF standard for communication and monitored by cloud user [7].

B. Intrusion detection for grid and cloud computing

In paper [8] author has shown proposed model an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent user actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion. The authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud users [8].

C. Cooperative Intrusion Detection System Frame Work for Cloud computing network

In paper [9], author has presented a framework of IDS for Cloud computing network that could reduce the impact of these kinds of attacks. To provide such ability, IDSs in the cloud computing regions exchange their alerts with each other. In the system, each of IDSs has a cooperative agent used to compute and determine whether to accept the alerts sent from other IDSs or not. By this way, IDSs could avoid the same type of attack happening. The implementation results indicate that the proposed system could resist DoS attack. Moreover, by comparison, the proposed cooperative IDS system only increases little computation effort compared with pure Snort based IDS but prevents the system from single point of failure attack [9].

3. PROPOSED MODEL

Cloud computing provides application and storage services on remote servers. The clients do not have to worry about its maintenance and software or hardware up-gradations. Cloud model works on the “concept of virtualization‟ of resources, where a hypervisor server in cloud data center hosts a number of clients on one physical machine. Deploying HIDS in hypervisor or host machine would allow the administrator to monitor the hypervisor and virtual machines on that hypervisor. But with the rapid flow of high volume of data as in cloud model, there would be issues of performance like overloading of VM hosting IDS and dropping of data packets. Also if host is compromised by an offending attack the HIDS employed on that host would be neutralized.

In such a scenario, a network based IDS would be more suitable for deployment in cloud like infrastructure. NIDS would be placed outside the VM servers on bottle neck of network points such as switch, router or gateway for network traffic monitoring to have a global view of the system. Such NIDS would still be facing the issue of large amount of data through network access rate in cloud environment. To handle a large number of data packets flow in such an environment a hybrid IDS approach has been proposed in this paper. The hybrid IDS would be able to process large amount of data and could reduce the packet loss. After an efficient processing the proposed IDS would pass the monitored alerts to a third party monitoring service, who would in turn directly inform the cloud user about their system under attack. The third party monitoring service would also provide expert advice to cloud service provider for miss-configurations and intrusion loop holes in the system. Figure 1 shows the architecture diagram of system.

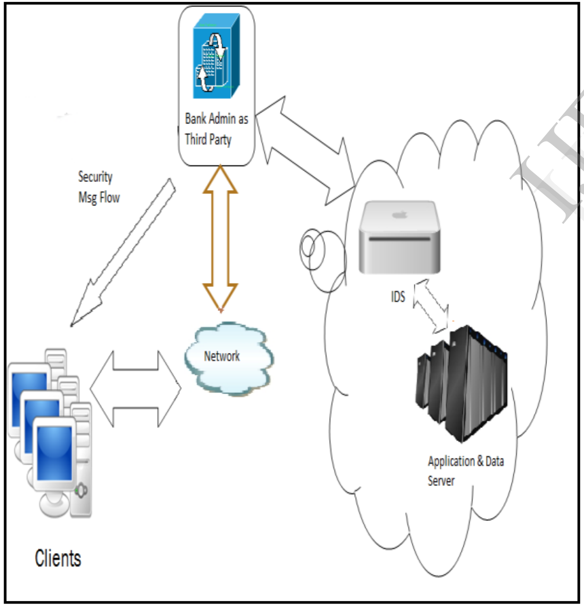

Figure 1.Architecture Diagram of System

In above architecture when user, request for particular software as a service from cloud server that time every request is analyze by intrusion detection system for security purpose. The cloud user accesses its data on remote servers at service provider's site over the cloud network. User requests and actions are monitored and logged through Third party auditor. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider

A. Framework of FC-ANN

In this section, we elaborate our a hybrid ANN, called FC-ANN, to solve the two drawbacks of current ANN-based IDS mentioned in Section I, i.e., lower detection precision for low-frequent attacks and weaker detection stability. FC-ANN approach introduces fuzzy clustering technique into ordinary ANN. By using fuzzy clustering technique, the whole training set can be divided into subsets which have less size and lower complexity. Therefore based on these sub sets, the stability of individual ANN can be improved, the detection precision, especially for low-frequent attacks, can also be enhanced.

Framework of IDS based on ANN and fuzzy Clustering FC-ANN firstly divides the training data into several subsets using fuzzy clustering technique. At same time, it trains the different ANN using different subsets. Then it determines membership grades of these subsets and combines them via a new ANN to get final results. The whole framework of FC-ANN is illustrated in figure (2).

As typical machine learning framework; FC-ANN incorporates both the training phase and testing phase. The training phase includes the following three major stages [1]:

Stage I: At first stage, whole database is dived into training set TR and testing set TS. Then the different training subsets TR1, TR2 . . . . TRk are created from TR with fuzzy clustering module.

Stage II: For each training subset TRi (i=1, 2….k), the ANN model, ANNi, (i=1, 2…k) is training by the specific learning algorithm to formulate k different base ANN models.

Stage III: In order to reduce the error for every ANNi, we simulate the ANNi using the whole training set TR and get the results. Then we use the membership grades, which were generated by fuzzy clustering module, to combine the results. Subsequently, we train another new ANN using the combined results.

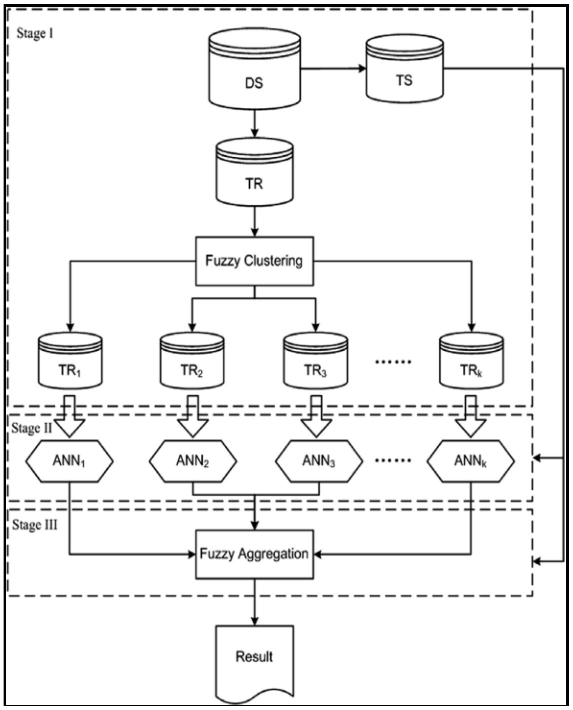

Figure 2.Framework of FC-ANN for IDS

In the testing phase, we directly input the testing set data into the k different ANNi and get outputs. Based on these outputs, the final results can then be achieved by the last fuzzy aggregation module.

B .Fuzzy clustering module

The aim of fuzzy cluster module is to partition a given set of data into clusters, and it should have the following properties: homogeneity within the clusters, concerning data in same cluster, and heterogeneity between clusters, where data belonging to different clusters should be as different as possible. Through fuzzy clustering module, the training set is clustered into several subsets. Due to the fact that the size and complexity of every training subset is reduced, the efficiency and effectiveness of subsequent ANN module can be improved. There are two types of clustering techniques hard clustering techniques and soft clustering techniques. Beside Partition of training set; we also need to aggregate the results for fuzzy aggregation module. Therefore, we choose one of the popular soft clustering techniques, fuzzy c-means clustering, for fuzzy clustering module [1].

C.ANN Module

ANN module aims to learn the pattern of every subset. ANN is a biologically inspired form of distributed computation. It is composed of simple processing units, and connections between them. In this study, we will employ classic feed-forward neural networks trained with the back-propagation algorithm to predict intrusion. A feed-forward neural network has an input layer, an output layer, with one or more hidden layers in between the input and output layer [1].

4. CONCLUSIONS AND FUTURE WORK

Cloud computing is a “network of networks” over the internet, therefore chances of intrusion is more with the erudition of intruder’s attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

In this paper we propose a new intrusion detection approach, called FC-ANN, based on ANN and fuzzy clustering. Through fuzzy clustering technique, the heterogeneous training set is divided to several homogenous subsets. Thus complexity of each sub training set is reduced and consequently the detection performance is incusing the KDD CUP 1999 dataset provide effectiveness of our new approach for low frequent attack. The experimental result dataset demonstrates the effectiveness of our new approach especially for low-frequent attacks, i.e. R2L and U2R attacks in terms of detection precision and detection stability. In future research, how to determine the appropriate number of clustering remains an open problem. Moreover, other data mining techniques, such as support vector machine, evolutionary computing, outlier detection, may be introduced into IDS. Comparisons of various data mining techniques will provide clues for constructing more effective hybrid ANN for detection intrusions in cloud network.

REFERENCE

[1] Gang Wang, Jinxing Hao, Jian Ma, Lihu Huang “A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering”, School of Management, Fudan University, Shanghai 200433, and PR China Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, and Hong Kong

[2] Ajeet Kumar Gautam,Vidushi Sharma,Shiva Prakash “An Improved Hybrid Intrusion Detection System in Cloud Computing “*International Journal of Computer Applications (0975 – 8887) Volume 53– No.6, September 2012* ,School of Information and Communication Technology, Gautam Budha University, Greater Noida, UP, INDIA.

[3] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[4] Christopher Harrison, Devin Cook, Robert McGraw, John A. Hamilton, Jr., *"Constructing Cloud-based IDS by Merging VMI with FMA"*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication. Dept. Computer Science & Software Engineering, Auburn University.

[5] R.Vanathi & S.Gunasekaran **,"**Comparison of Network Intrusion Detection Systems in Cloud Computing Environment",2012 International Conference on Computer Communication and Informatics (*ICCCI* - 2012), Jan. 10 – 12, 2012, Coimbatore, INDIA, *Department of Computer Science Coimbatore Institute of Engineering and Technology, Coimbatore, India E-mail: vanathi.be@gmail.com, 2gunaphd@yahoo.com .*

[6] W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah and M.T. Abdullah, *"A Cloud-Based Intrusion Detection Service Framework "*, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia,43400 UPM Serdang, Selangor Darul Ehsan, Malaysia izura@fsktm.upm.edu.my

[7] Irfan Gul, M. Hussain, "Distributed cloud intrusion detection model", International Journal of Advanced Science and Technology Vol. 34, September, 2011.

[8] Sebastian Roschke, Feng Cheng, Christoph Meinel, "Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[9] Kleber, schulter, "Intrusion Detection for Grid and Cloud computing", IEEE Journal: IT Professional, 19 July 2010.

[10] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.

[11] Kddcup1999data[Online].Available:kdd.ics.uci.edu/Bdatabases/kddcup99/kddcup99.html.

[12] D. E. Denning, "An intrusion detection model," *IEEE Trans. Softw. Eng.*,vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[13] *Muna Mhammad T.Jawhar, Monica Mehrotra,* ―Design Network Intrusion Detection System using hybrid Fuzzy- Neural Network‖, International Journal of Computer Science and Security, Vol. 4.

[14] Chiu, S. L. (1994). Fuzzy model identification based on cluster estimation. Journal of Intelligent and Fuzzy Systems, 2, 267–278.

[15] Wu, S., & Yen, E. (2009). "Data mining-based intrusion detectors". Expert Systems with Applications, 36(3), 5605–5612.

[16] Bhavin Shah, Bhushan H Trivedi, PhD, "*Artificial Neural Network based Intrusion Detection System: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 39– No.6, February 2012.* L. J. Institute of Management Studies Ahmadabad, India.