A study of Intrusion Detection System for Cloud Network Using FC-ANN Algorithm

Gayatri K. Chaturvedi[1], Arjun K. Chaturvedi[2], Varsha R. More[3]
(MECOMP-Lecturer)[1], (BEIT-Student)[2], (BEE&TC-Student)[3]
Matoshri Aasarabai Polytechnic, Eklahare, Nashik, MS (India).

Abstract **- In our world of ever-increasing Internet connectivity there is an on-going threat of intrusion or denial of service attacks. These intrusions may bring all kinds of misuses. *Intrusion Detection Systems* (IDS) play a very important role in the security of today's networks by detecting when an attack is happening. Due to increasing incidents of cyber attacks, building effective intrusion detection systems are essential for protecting information systems security. Intrusion detection attempts to detect computer attacks by examining various data records observed in processes on the network. Detection precision and detection stability are two key indicators to evaluate intrusion detection systems (IDS). In early stage in order to enhance the detection precision and detection stability, the research focuses lies in using rule-based expert systems and statistical approaches. But when encountering larger datasets, the results of rule-based expert systems and statistical approaches become worse. Thus a lot of data mining techniques have been introduced to solve the problem. 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: (1) lower detection precision and (2) weaker detection stability. The main reason of above problem is that distribution of different types of attack is imbalanced. To solve the above two problems we propose FC-ANN (Fuzzy-Clustering Artificial Neural Network) to enhance the detection precision for low frequent attacks and detection stability.**

Keywords **- Cloud computing, Intrusion detection system, Attacks, security**

1. INTRODUCTION

In this section, Cloud computing is introduced. 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 by 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.

1.1 Introduction

In recent year, Internet has been a driving force towards the various technologies that have been developed. Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer as a service on pay-as you-use basis. Fig. 1 shows the concept [2].

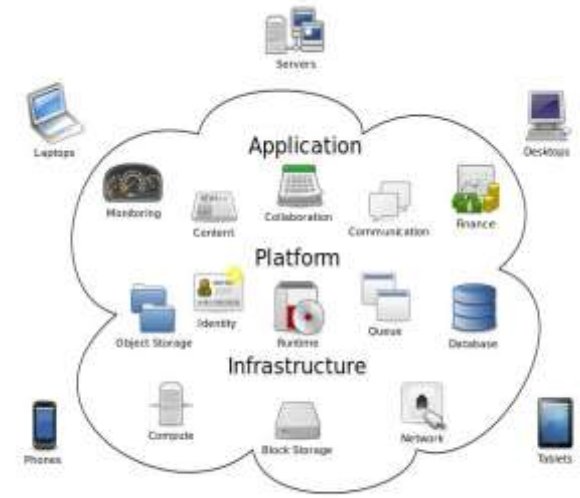

Figure 1.1: Cloud Computing

Basically Cloud computing is seen as a trend in the present day scenario. 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.

With the coming of Internet age, network security has become the key foundation to web applications such as online retail sales, online auctions etc. Intrusion detection attempts to detect computer attacks by examining various data records observed in processes on the network.

1.2 Motivation of FC-ANN based IDS

Evaluation of Intrusion detection system has two key indicators: detection precision and detection stability. In order to enhance the detection precision and detection stability, in the early stage the research focus lies in using rule based expert systems and statistical approaches.

But for larger datasets rule based expert systems and statistical approaches becomes worse. To solve this problem lots of data-mining techniques have been introduced. Among these Artificial Neural Network (ANN) is one of the widely used techniques.

The main drawbacks of ANN-based IDS exist in two aspects: lower detection precision for low-frequent attacks and weaker detection stability. The main reason of these problems is the distribution of different types of attack is imbalanced.

For low-frequent attacks, the leaning sample size is too small compared to high-frequent attacks. It makes ANN not easy to learn the characters of these attacks and therefore detection precision is much lower.

To solve the above two problems, a novel approach is introduced for ANN-based IDS, FC-ANN to enhance the detection precision for low-frequent attacks and detection stability.

1.3 Benefits of FC-ANN based IDS

The general procedure of FC-ANN approach is divided into 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 with fuzzy aggregation module, is introduced to learn again and combine the different ANNs results.

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.

1.4 Aim

In this paper we study FC-ANN approach which aims to detect intrusion. We aim to design models to integrate this approach with others in the future.

1.5 Organization

This paper is organized as follows: First it describes the related work on IDS. Secondly, it describes the security issues in cloud computing. Then the detailed system architecture and proposed model is illustrated.

Lastly, we present the future research and summarize the work.

2. LITERATURE REVIEW

IDS are split into two categories: misuse detection systems and anomaly detection systems [3]. Misuse detection is used to identify intrusions that match known attack scenarios. In order to detect the intrusion, various approaches have been developed and proposed over the last decade.

To overcome the inherent limitations of the client-server paradigm and to detect intrusions in real time IDS is introduced based on distributed agent technology [4].

In year 1997, Porras A. et al devised intrusion detection system based on rule based expert system approach [5]. A rule-based expert IDS can detect some well known intrusions with high detection rate, but in this methodology there is difficulty in identifying new attacks or attacks that had no previously describe patterns and its signature database needs to be updated manually and frequently.

In year 2001, some Intrusion detection system has been implemented on the basis of neural network [6]. These IDS support vector machines and their variants are being proposed to detect intrusions. These Statistical-based IDS, employs various statistical methods including principal component analysis, cluster and multivariate analysis, Bayesian analysis, and frequency and simple significance tests.

Supervised ANN applied to IDS mainly includes multi-layer feed-forward (MLFF) neural networks and recurrent neural net-works. Ryan et al. (1998) and Tan (1995) used MLFF neural networks for anomaly detection based on user behaviors. But in practice the number of training set is very large and the distribution of training set is imbalanced, the MLFF neural networks is easy to reach the local minimum and thus stability is lower.

The second category uses unsupervised ANN to classify input data and separate normal behaviors from abnormal or intrusive ones. Using unsupervised ANN in intrusion detection has many advantages. The main advantage is that unsupervised ANN can improve their analysis of new data without retraining. For low-frequent attacks, unsupervised ANN also gets lower detection precision.

The third category is hybrid ANN which combines supervised ANN and unsupervised ANN, or combines ANN with other data mining techniques to detect intrusion. The motivation for hybrid ANN is to overcome the limitations of individual ANN.

In year 2011, a hybrid ANN introduced called as FC-ANN to solve the drawbacks such as lower detection for low frequent attacks and weaker detection stability of current ANN-based IDS.

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.

Summary-

Various approaches have been developed to address the insider threat in cloud networks. Rule based expert systems and statistical approaches have been adapted to detect the intrusion over cloud networks [5], [6]. But for larger datasets these IDS becomes worse. To solve these problems lots of data-mining techniques introduced. Among these ANN based IDSs are very popular.

Recently FC-ANN approach has been introduced to solve the drawbacks such as lower detection for low frequent attacks and weaker detection stability of current ANN-based IDS.

3. SECURITY ISSUES IN CLOUD COMPUTING

This section describes the security issues in cloud computing.

3.1 Cloud data confidentiality issue

Confidentiality of data over cloud is one of the overt security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service provider's end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case.

3.2 Network and host based attacks on remote Server

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. DOS and DDOS attacks are launched to deny service availability to end users.

3.3 Cloud security auditing

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

3.4 Cloud security auditing

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud users data and application may not be compatible with other vendor's data storage format or platform.

4. ARCHITECURE OF CLOUD IDS MODEL

This section begins with architecture of the cloud IDS model.

4.1 Flowchart of cloud IDS Model

Multi-threaded NIDS model for distributed cloud environment is based on three modules: capture and queuing module, analysis/processing module and reporting module.

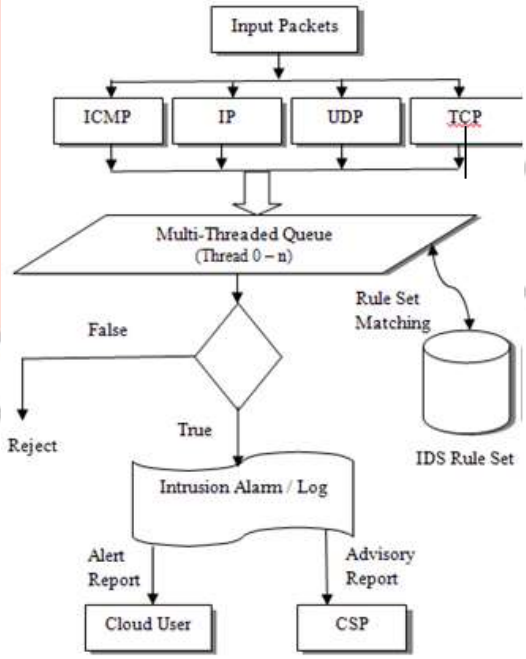

Figure 4.1: Flowchart of cloud IDS

The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set. Each process in a shared queue can have multiple threads which work in a collaborative fashion to improve the system performance.

The main process will receive TCP, IP, UDP and ICMP packets and multiple threads would concurrently process and match those packets against pre-defined set of rules. Through an efficient matching and analysis the bad packets would be identified and alerts generated. Reporting module would read the alerts from shared queue and prepares alert reports. The third party monitoring and advisory service having experience and resources would immediately generate a report for cloud user's information and sends a comprehensive expert advisory report for cloud service provider. Figure 3.1 depicts the flow chart of proposed multi-threaded Cloud IDS.

4.3 System architecture

This proposed model is an efficient and effective distributed Cloud IDS which uses multi-threading technique to improve IDS performance over the Cloud infrastructure. Multi-threaded IDS is a NIDS that uses sensors to sensitize and monitors network traffic as well as check for malicious packets. The system then sends intrusion alarms to a third party monitoring service which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider.

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 multi-threaded IDS approach has been proposed in this paper. The multi-threaded 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 mis-configurations and intrusion loop holes in the system. Figure 3.2, shows the proposed IDS model.

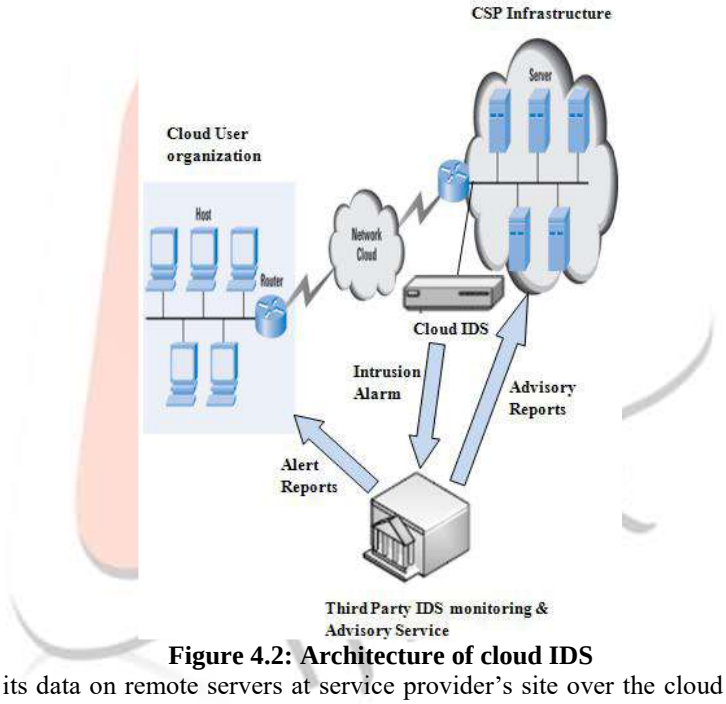

Figure 4.2: Architecture of cloud IDS

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 a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider.

5. FC-ANN FRAMEWORK OVERVIEW

In this section, we elaborate hybrid ANN called FC-ANN. To solve the two drawbacks of current ANN-based IDS 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 5.1.

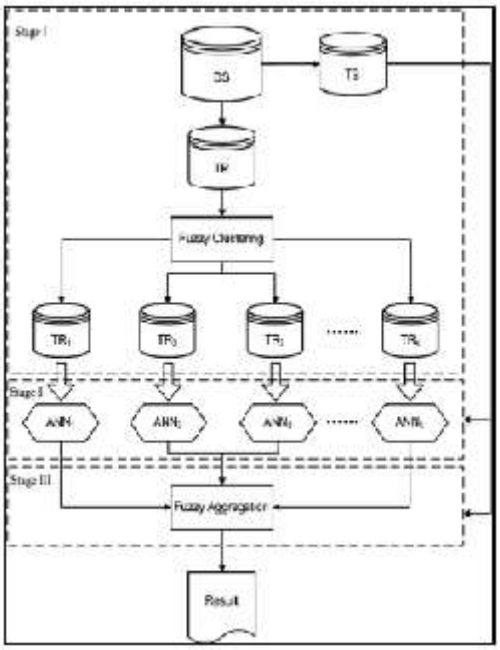

Figure 5.1: Framework of FC-ANN

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 . . . . TR_k are created from TR with fuzzy clustering module.

Stage II: For each training subset TR_i (i=1, 2….k), the ANN model, ANN_i, (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 ANN_i, we simulate the ANN_i 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.

6. CONCLUSION

In this paper, a small step is taken toward understanding the detection of intrusion in cloud network. We have studied architecture of cloud IDS. 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 and applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required.

In this paper we have been studied 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 increased.

Future Work

In future work, we intend to research on cloud IDS approach administered by a third party IDS provider. A third party IDS provider would be the operator of cloud IDS, by keeping configuration setting rights at its own site and cloud service provider could only view the logs information and would not be able to hide intrusion information from the user. Following this approach, the cloud user would be informed directly for intrusions that took place against its VM and data.

REFERENCES

[1] Swati Ramteke, Rajesh Dongare and Komal Ramteke3, "Intrusion Detection System for Cloud Network Using FC-ANN Algorithm", IEEE transaction on network and service management, vol.8, no.2, 2nd june 2011.

[2]S. Sontakke, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4 (page no. 67-71), May 2012.

[3] A. Haeberlen," An Efficient Intrusion Detection Model Based on Fast Inductive Learning", Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007. Tavel, P. 2007.

[4] Mukkamala S., and Sung A. H. (2003) Feature Selection for Intrusion Detection Using Neural Networks and Support Vector Machines. Journal of the Transportation Research Board of the National Academics, Transportation Research Record No 1822, pp. 33-39.

[5] Porras A. and Neumann P. G. EMERALD. (1997) "Event Monitoring Enabling Responses to Anomalous Live Disturbances," In *Proceedings of the National Information Systems Security Conference*, pp. 353-365.

[6] S Mukkamala, G Janowski, A H. Sung. (2001) Intrusion Detection Using Neural Networks and Support Vector Machines. *Proceedings of Hybrid Information Systems* Advances in Soft Computing, Physica Verlag, Springer Verlag, ISBN 3790814806, pp.121-138.

[7] 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.