Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NETWORK INTRUSION BASED ON CLOUD NETWORK

BOHAN
Department of Computer, ShangLuoUniversity, ShangLuo726000 , ShaanXi, China

ABSTRACT

This work aimed at the cloud cluster cyber source intrusion and malicious behavior, analyzes the attack mode, studied its intrusion detection method, the design of intrusion detection system model and structure. System can be effective for cloud service network to provide safe, effective cloud pool resources protection and cluster service guarantee, can effectively prevent, detect intrusion behavior based on cloud services.

Keywords: *Cloud Services, Yun Chi, Network Intrusion*

1. INTRODUCTION

Cloud computing through the development of recent years has become a mature network technology, which have been or are being applied to a number of large-scale network server cluster, including computing, storage server, Internet resources etc.. The simple cloud computing technology in the network service has been everywhere, such as search engines, web mail, as long as the user input simple instructions that can get a lot of information. in this approach, for example [1]. The future such as mobile phone, GPS and other mobile devices can be through cloud computing technology, develop more application services. Cloud computing is one of the main characteristics is of considerable size, the Google cloud computing has over about 1000000 servers, Amazon, IBM, Microsoft, Yahoo and other" cloud" with hundreds of thousands of servers.

Along with the network technology and the wide application of cloud services, based on cloud services cluster computer system, network system and all the information infrastructure security has become the problem that people cares. Great for cloud services cluster cyber source intrusion and malware behavior has become the network development under the new situation of the urgent need to solve the hot issues.

This paper designs a solution for cloud services cluster cyber source intrusion malicious behavior method and system, experiments show that it can effectively prevent and detect intrusion, cutting is simple and practical but also does not occupy a large amount of network bandwidth.

2. INTRUSION DETECTION BASED ON THE CLOUD CLUSTER NETWORK

2.1 Introduction

An intrusion detection based on the cloud cluster network is to Yun Chi within the computer and cyber source for malicious behavior, such as network spy, denial of service attack, attack, monitor (MITM), man in the middle attack from client to client invasion, Rogue AP, flooding attack recognition and response processes, it can not affect the network performance under the condition of network, detection, provide internal, external attack and wrong operation.

Cloud computing services in this short a few years of business process, formation of tens of thousands of cloud cluster, the cloud clusters have a concept of system based on server access logs, call them cloud cluster log system, as shown in Figure1, by which to monitor, analysis of the cloud Service data, which we need to check, analysis of the intrusion data .For example table 1. The cloud cluster port shell call log, so the best way is to build a cloud based service cluster network intrusion detection model site system as shown in figure1.Through the analysis of the original data is extracted for each user to log in each time the operation[3].

A cloud users once the sign of all the operations can be integrated as an event sequence. Every operation event is represented by a corresponding number to denote a type. Such user operation sequences form a cloud service cluster log, as shown in table, It is our analysis premise and foundation.

Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: The Cloud Cluster Port Shell Call Log

time	command	parameter1	parameter2
12：22：10	*mail*	*dir1*	
12：22：21	*vi*	*dir1*	
12：23：12	*mail*	*dir2*	
		……	
12：32：30	*la*	*dir2*	
12：32：54	*mail*	*file1.c*	
13：22：12	*mail*	*predd*	*D*
13：24：11	*gcc*	*file2*	*()*

2.2 The Intrusion Detection Model Based On The Cloud Cluster Network

The intrusion Based on the cloud cluster data is defined as any of the cloud system resources of the unauthorized use of his behavior, data integrity, confidentiality and availability caused destruction, enables users in computer system and network system in which the loss of trust. In this approach, for example [3，4].we use the system is declined to legitimate users service.

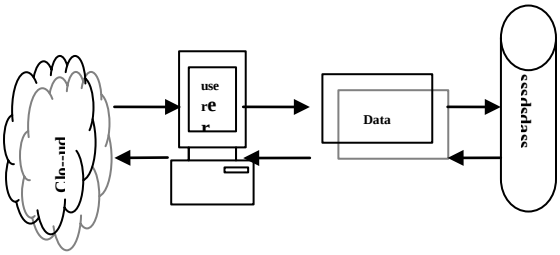

Figure1: Cloud Cluster Log Structure Figure

In general, invasion into external invasions and internal external invasion, invasion from outside the system generally refers to the illegal user's invasion, and the internal intrusion is one who must have access to a system resource permissions, but attempts to acquire more rights to perform unauthorized operation of the internal user's intrusion behavior. Based on the cloud cluster data intrusion detection is based on the cloud cluster server attempted or ongoing intrusion activity. Intrusion detection system is to complete the task of the intrusion detection system. It is a kind of lifting system security data legalization effective method. Based on the cloud cluster data intrusion detection system on transported by server to a user of the system and the assessment of the extent of abnormal data of suspicious, and thus form a cloud service data log records system, since the current behavior is normal. In order to help system administrators for safety management, and the system is subjected to the attacks to take the corresponding pretreatment .The intrusion detection model structure as shown in figure 2. cloud cluster intrusion detection model.

2.3 An Intrusion Detection System Based On The Cloud Service Cluster Of Network

According to different network environments an -d different server cluster and different security policies, the intrusion detection system in the specific implementation is also different. No matter what detection system from its specific structural form appears ,which at least comprises a data extraction, intrusion analysis, in response to the processing of the three part, may also according to safety knowledge base, data storage and other functional modules to provide a more perfect safety detection and data analysis function. Based on the cloud cluster data intrusion detection system structure as shown in figure 3. cloud cluster intrusion detection structure.

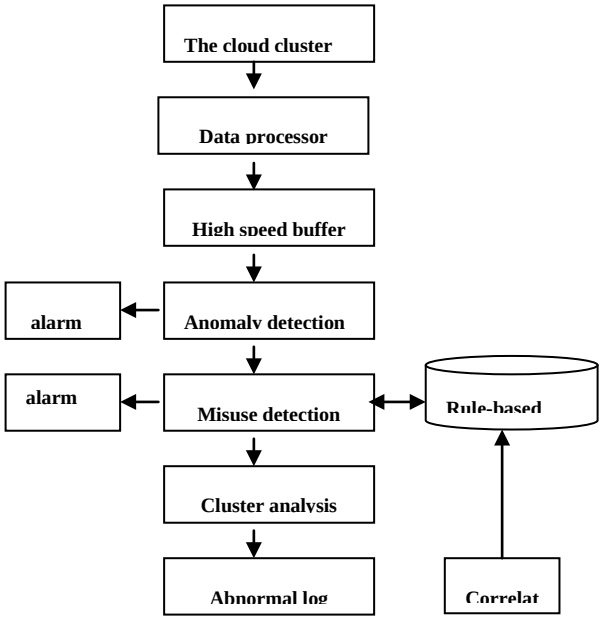

Figure 2: Cloud Cluster Intrusion Detection Model Structure

The data extraction module in intrusion detection system is the basic position, responsible for the extraction of reflecting the protected system operation state of the operation data, and data filtering and other pre-processing work, for intrusion analysis module and the data storage module provides the original security audit data, in-trusion detection system data collector. Intrusion analysis module is the core module of intrusion detection system, its function includes the original data synchro -nization, finishing with known

Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

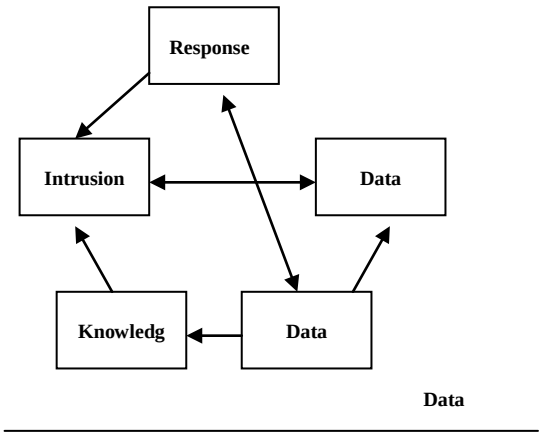

Figure 3: Cloud Cluster

intrusion detection structure organization, classifica -tion, feature extraction and various types of detaile -d analysis, extraction which contain system feature or mode for normal and abnormal behavior judgment. This behavior identification can be perfo -rmed in real-time, can also be a pothook analysis. The response processing module to the system found in the intrusion attacks to take response measures, these response measures including passive and active response.

2.4 An Intrusion Detection Method Based On The Cloud Cluster Network

The intrusion detection based on cloud services for the purpose of detecting occurs in theYun Chi network intrusion. An intrusion detection system can effectively detect attack behavior depends largely on the system the system detection method. The earliest intrusion detection model is Dorothy Denning presented in 1986, it can describe how to use the audit tracking data to improve the security of the computer system. But this method have serious defects, such as too much redundant information, increase the data analysis judgment difficulty, enables network administrators to manage[5]. So a new intrusion detection method and application. The existing intrusion detection system using statistics method, expert system, pattern matching, state transfer to achieve the detection engine, in order to analyze the event log, recognizing a specific pattern, generate test report and the final result of the analysis[6]. In the detection system through three kinds of techniques in intrusion detection analysis: pattern matching, statistical analysis and integrity analysis. The first two methods for real-time intrusion detection, and integrity analysis is used for post hoc analysis.

2.4.1 Pattern matching

Pattern matching is the collected formation user network intrusion and misuse model system database for comparison, as shown in table 2, to identify known intrusions. As shown in table 3, the

Table 2: Network User Behavior Database

UserID	LogingID	User Sequence
1	**001**	**aabbef**
2	**002**	**acdfe**
3	**003**	**aaddf**
4	**004**	**bbaad**

Process can be very simple (as by string matching to search for a simple entry or instructions), can also be very complex (such as the use of formal athematical expression to represent safety state changes). An offensive mode can use a process (such as the execution of an instruction) or an output (such as obtaining permissions) to express. The method is a big advantage is the only collection related data collection, significantly reduce the burden of the system, and the technology is already quite mature. It is associated with virus firewall using methods like, accuracy and efficiency of detection are very high. However, the weakness is the need to constantly upgrade to deal with emerging hacker attacks, can not be detected there has never been a hacking tool[7].

Method summary:

First， only need to specify with the pattern matching, without the need to design how to match;

Second, a plurality of event streams can be independent analysis, without merge, can be processed in parallel audit event;

Third ,good portability, for nothing to do with the system description script invasion characteristics, easy in different operating system and audit event format between graft.

Pattern matching is a relatively mature intrusion detection method , but according to different network environment, there are different methods, such as statistical analysis, complete analysis, state transfer method, the following simple introduce on cloud services cyber source intrusion detection may also apply to focus detection method.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Network User Behavior Pattern

LogingID	User Sequence
1	Read、send a message
2	ID login、check the system log
3	Create directory, upload procedures
4	Read、send a message

2.4.2 Statistical analysis

Method of statistical analysis to the system first object (such as user, files, directories and equipment) to create a statistical description statistical, normal use Some of the measurement properties (such as the number of visits, the operation failed and the number of delay). Measurement properties of the mean value would be used with the network, the behavior of the system were compared, any observed values in the normal value range, is thought to have invaded. For example, statistical analysis may identify an abnormal behavior, because it was found in a late eight to early six points do not login account is two o'clock in the morning trying to login. Its advantage is to detect unknown intrusion and more complex intrusion, disadvantages are false positives, false negative rate is high, and is not suitable for normal user of the sudden change of behavior. Specific statistical analysis methods such as expert system based, model based reasoning and neural network based analysis method, is currently in the research focus and rapid development..

2.4.3 Integrity analysis

Integrity analysis mainly focus on a file or object has been changed, which often include file and directory contents and attributes, it is found Change, be special Luo Hua applications particularly effective. Integrity analysis using strong encryption mechanism, called the message digest function (such as MD5), it can identify even small changes[8,9]. The utility model has the advantages of regardless of the mode matching method and statistical analysis method can detect intrusion, as long as the success of the attack resulted in a document or other object of any change, it can be found. Disadvantages are generally in batch mode to achieve, not for real time response. Nevertheless, integrity testing methods should also be one of the necessary means of network security products. For example, can each day at a particular time open integrity analysis module, the network system to conduct a comprehensive scan.

3. SYSTEM SIMULATION

A client agent system simulation experiments, the system has three main functions, namely: network behavior matching detection, data package interception and member communications and collaboration, we on the three major functions of the test. On the other hand also visited a client agent on the host performance influence.

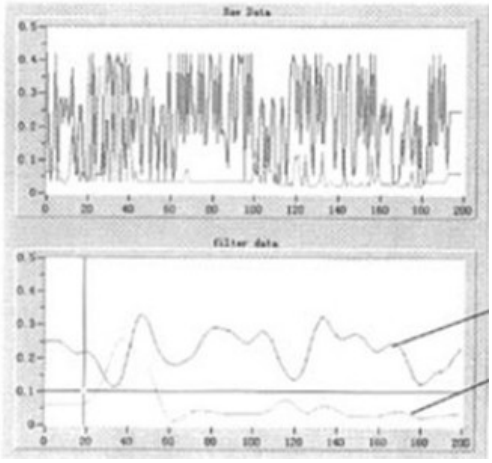

Figure 4: Capture Data Curve Comparison

Figure 4 is the first normal operation and then suddenly into the routine violation of operating conditions, matching test results data curve, Figure 4 with two sets of curves are more clear comparison. In addition, in order to make the results more clearly, the data is digital filter, the filter is a Butterworth digital low-pass filter, filter cutoff frequency 10Hz. From the graph can see, the client agent matching detection module clearly distinguish the two different modes of operation. Therefore the client agent matching detection module can meet the design requirements.

4. CONCLUSIONS

Cloud based service cluster of intrusion detection for the purpose of detecting in the cloud service cluster network intrusion, effective detection for network to provide safe, effective real-time protecting computer system against the intercept and respond to invasion. At present, along with the popularity of cloud services, some key sectors of key industry more and more urgent need of independent copyright intrusion detection technology. Cloud cluster based on network intrusion detection system on the cloud server to the users of the system and abnormal data in the assessment of the extent of the suspicious, and accordingly form a cloud service data log records

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

system, since the current behavior is normal or not, and to the system by the attack and to take corresponding pretreatment. In order to help system administrators to cyber source for safety and reasonable management, which is prevalent in the omnipresent cloud services to provide a safe, effective cloud pool resources protection and security services.

ACKNOWLEDGEMENTS

This work was supported by Shangluo university scientific projects, and project number :10sky016.

This work was supported by Shangluo university scientific projects, and project number :11sky005.

This work was supported by the Shaanxi Provincial Department of education scientific research projects, and project number:12jk0950.

REFERENCES:

[1] Tang, Fu-Hua Yang, Yang Lu, The basic method of data mining and its differences with the expert system, *Computer applications*, Vo119, N o3,2-8

[2] Retired intellectuals, Deng Su, Zhang Weiming. Data Mining and Knowledge Discovery. Calculation sector Monde, 24 version of the topics, 1997.6.30, 3-10

[3] Alex G. Büchner, Maurice D. Mulvenna, "Discovering Internet marketing intelligence through online analytical web usage mining", *ACM SIGMOD Record*, Vol. 27, No. 4, 1998, pp. 54-61.

[4] Jian Pei et al., "Mining Access Patterns Efficiently from Web Logs", *Proceedings of the 4th Pacific-Asia Conference on Knowledge Discovery and Data Mining*, 2000, pp. 396-407.

[5] Piatet sky-Shapiro G, Data Mining and Knowledge Discovering Business Databases, ISMIS,1996, pp. 56-57.

[6] Rakesh Agrawal et al., "Ming Association Rules Between Sets of Items in Large Database", *Proceedings of the 1993 ACM SIGMOD international conference on Management of data*, 1993, pp. 207-216.

[7]Yusuke Ohura, Katsumi Takahashi, Iko Pramudiono et al., "Expreimentson Query Expansion for Internet", *Yellow Page Services Using Web Log Ming*, Vol. 6, No. 2, 2010, pp.4-12

[8] Tang Fuhua. Lu Yangyang, "The basic method of data mining and its differences with the expert system", *Computer Applications*, Vol. 19, No.3, 1999,pp. 2-3

[9] Agrawal R, "Database Mining, A Performance Perspective", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 5, No. 1993, pp. 4-5.