VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SIGNATURE BASED INTRUSION DETECTION IN CLOUD BASED MULTI-TENANT SYSTEM USING MTM ALGORITHM

N.Thirumoorthy[1], M.Aramudhan[2] and M.S.Saravanan[3]
[1]Department of Computer Science, Jayalakshmi Institute of Technology, Dharmapuri, India
[2]Department of Information Technology, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karikal, India
[3]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, India
E-Mail: saranenadu@gmail.com

ABSTRACT

The improvement of security prevents the malicious attacks from various types of networks. The intrusion by the malicious attackers in real time cloud networks has major issues for security credentials. The various types of attacks are identified in cloud networks are not enough to handle the critical situations. This paper contributes a new class of malicious attacks or intrusions in the cloud network and addresses the mischievous and malicious behaviour, which is the root cause for the modification of cloud network stored data. The cloud based storage services are handled by single or multi-tenant based system. This paper uses the patient healthcare record, which is handled by multi-tenant users for various applications. This is the first attempt to identify the multi-tenant user attacks in cloud network. In this attempt a new algorithm is introduced, that identifies the multi-tenant user database malicious attacks. The basic idea of this algorithm is devised from the wireless LAN malicious attacks. Hence Multi-Tenant Mapping (MTM) Algorithm developed to analyse data flow inconsistency with the less number of packet transfer between the cloud nodes. This type of analysis is presented in this communication. Analysis of information in the unbound values determines whether the database value has been compromised for any attacks. Results show that the proposed algorithm has a promising prediction for malicious attacks for multi-tenant based user data security.

Keywords: cloud network, healthcare records, intrusion, malicious attacks, multi-tenant.

INTRODUCTION

The importance of cloud computing is increasing day by day and receiving a good attention in the scientific, research and industrial communities. A recent study says that cloud computing become a first computing system is top among the ten most important technologies and it has a better future in the coming years.

The intrusion detection methods are mainly categorised into four types, they are signature based, anomaly based, host based and network based. Network-Based: A Network Intrusion Detection System (NIDS) analyses network traffic at every layer of the OSI model for suspicious activity. Wireless: Cloud Network (CN) IDS analyses wireless-specific traffic, including scanning for unauthorized users trying to connect to active wireless network components. Network Behaviour Anomaly Detection: Network behaviour anomaly detection (NBAD) analyses network traffic to identify anomalies that exists if any. Host-Based: Host-based intrusion detection systems (HIDS) analyses system-specific settings including security policies, log audits and software calls.

The malicious attack can be identified using various existing methods. Intruders can attack any type of the wireless networks such as wireless LAN, cloud network, etc. Yet a dense definition of the word seems hard to come by, since the cloud network enters all levels of applications. It is the first attempt to identify the malicious attack in the cloud network based on the wireless LAN (Theuns and Ray, 2002) in this study the various methods of intrusion is discussed. Many of the researchers were involved to provide better security using various tools in the wireless networks. The existing literature from the various published articles deals about the man-in-the middle attack, brute force attack and cyber-attacks, etc. The risk of the cyber-attacks are analysed using various tools at the same time the risk factor for failure of detection is high (JingwenTian and Meijuan Gao, 2009).

The vulnerability refers to the flaws in a cloud network that allows an attack to be successful. A malicious attack is potential attack that may lead to a misuse of information or resources, and the related data. The malicious attack is the merging of threats and cyberspace (Bezemer C-P and Zaidman A, 2010). It generally denotes unlawful attacks and threats of attack against computers, networks, and the information stored therein which is done to threaten or force a government or its people in persistence of political or social objectives. The critical attacks could be act as a tool for the terrorists; it is always because of lack of security in the cloud network.

The main study of this paper is to discuss the various existing malicious threats on cloud networks to propose a new algorithm to identify and prevent the intrusion detection. This study can also help the cloud Infrastructure as a service such as multi-tenant researchers

to find more future solutions. The multi-tenant approach is not new in cloud network. It is similar to distributed system services in the client server technology. The idea of multi-tenant has major difference with distributed services that is apart from computing and storage; it also can handle the different infrastructure such as hardware and application services. The private and public cloud are the two classifications of network services, in this the private cloud has less possibilities of attacks comparing to public cloud network. This paper mainly contributes to propose a new signature type of IDS on Cloud based multi-tenant approach for detecting malicious attacks.

RELATED WORK

The wireless network is working in the field of network security from 1987 when Dorothy Denning published an intrusion detection model (D. E. Denning, 1987). The optimized solution to identify the intrusion in any one of the network is not yet identified. There are so many network security tools available such as antivirus, firewall, etc. But they are not able to cover all security risks in the wireless network (MIT Lincoln Laboratory, 1999). The main work of intrusion detection system is to identify the intrusion in the network. And for that it collects important information from the network and processes the same. If the IDS identified the attack then alert for the possible attack need to be sent to victim node. The existing analyzing method to identify the intrusion is by the abnormal connection that has been detected by using Snort tool.

This snort tool is tested in wireless LAN and not yet implemented in cloud network. The snort tool can work with the DARPA Data Set over the network. IDS works as a network packet sniffer, which is based on comparisons of packet contents with known virus signatures encapsulated as rules, it can initiate action and record events and information related to them in a log file and /or database. Snort is a popular NIDS that is used to audit network packets and compare those packets with the database of known attack signature. The snorts attack signature database can also be updated time by time (Forrest, *et al*., 1996).

The intrusion detection on is not yet attempted to identify intrusion on the various types of private, public and hybrid cloud network. These cloud networks has a approach called Multi-Tenant to connect various cloud users by different web services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PasS). In these above three types of network the more possible attacks can be conducted on private cloud. The following section 3 has the proposed MTM algorithm to deal the intrusion detection using Multi-Tenant based private cloud based network. Before to discuss the MTM algorithm, the possible attacks in cloud network is given in the following sub sections.

Malicious attacks

In Cloud network, the malicious attacks in day-to-day create most dangerous situation in the internet through emails or other source of attacks. The countermeasures are more in cloud network comparing to wireless network. The risks are more in cloud network and increasing day-by-day that is the malicious threats are major in twenty first century. The malicious attacks are categories according to the nature of source of the attack, type of the attack and percentage of attack level. The networks based attacks on the nature of networks are having average percentage of possible malicious attacks. The social networking based attacks on the economic changes of the cloud network having high percentage of possible malicious attacks.

The attacks in intrusion detection system can impact more. The botnets are the type of attack which can occur even through authentic web sites on cloud nodes. The botnets exploit in private cloud. The botnet Malware delivery mechanisms are gaining sophistication and better complicated techniques in private cloud. It can be delivered to a system via emails, USBs, Trojans etc. It can independently switch from one tenant to another in private cloud network.

The malware like Trojan is a small piece of code used by the attackers to interrupt computer operation. The Trojan is also used mostly in wireless networks like sensor, ad-hoc and cloud. Every day a new botnets are introduced by the attackers, according to the report by the Gerogia tech. The Damballa statistics says that three to five percent of database is targeted by the cloud network user in each day. The man-in-the middle attack and distributed denial of service attack were mostly used in the wireless network to attack the target system in the past ten years.

Threats on private cloud network

A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. The remainder of the paper is organized as follows; Section 3 presents the results new proposed algorithm MTM. Next, in Section 4 we define in depth the most important security aspects for each layer of the Cloud model. Later, we will analyze the security issues in Cloud Computing identifying the main vulnerabilities for clouds, the most important threats in clouds, and all available countermeasures for these threats and vulnerabilities. Finally, we provide some conclusions.

MTM ALGORITHM ON CLOUD USING MULTI-TENANT APPROACH

This research study is to design and implement identifying intrusion detection system using signature based approach on Multi-Tenant based Cloud Network. The signature based intrusion detection method used in many type of networks (S. A. Hofmeyr, *et al*., 1998). The signature based intrusion detection is done using various wireless services such as WLAN, Wi-Fi and Cloud Networks (T. Inagaki, 1999). This system should be able to predict the intrusion with less false rate. System should be able to be trained by the user and those trained information should be made use of whenever they are required.

In this paper the Intrusion detection system can be deployed to protect the Multi-Tenant based Cloud Network. It can be deployed between to tenants, between two cloud networks or within cloud network server firms. The threats in the cloud network by the tenants can be detected by well-defined patterns that exploit system weaknesses and application software. Because these types of threats attack follow well-defined patterns and signatures, they are usually encoded in advance and thereafter used to match against the user behavior. It implies that misuse detection requires specific knowledge of given intrusive behavior. These behaviors can be measured by the predefined signature based detection patterns in the form of signatures and these signatures are further used to determine the network attacks. They usually examine the network traffic with predefined signatures and each time database is updated. Hence in our proposed MTM algorithm developed to detect the Signature based Intrusion using the Back Track tool installed in on Linux Environment with VMware.

Working model

The concept of signature based IDS can be achieved using many of wireless services (Zhao Zhenning, *et al*., 1996). Hence this study deals about the cloud based multi-tenant IDS. It is clear that when any person sends data inside the network so first of all it goes to nearest cloud server and check if found malicious attack then server discards the packet otherwise send to destination system.

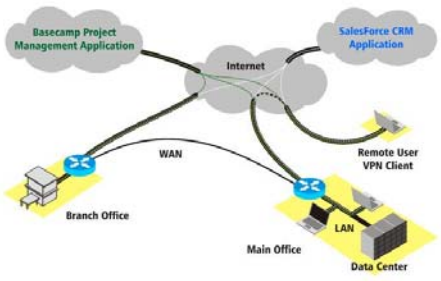

Figure-1. Cloud network model before IDS introduction.

The Figure-1 has the simple architecture of cloud network model before the introduction of IDS. Here the various network types are entering into the cloud datacentre. The data sent from one node of the network to another node of the network through the server checks that packet and if packet is malicious then server discards the packet otherwise send packet from one node to another.

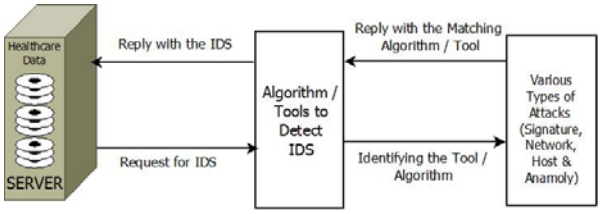

Figure-2. Cloud network model after IDS introduction.

In Figure-2 working of server is clearly mention that how server checks the packet. So, when a packet comes to server then server use comparing tool to check that packet from the database of signature stored in server and if server get result that packet is matched from the database then server discard the packet otherwise server sends the packet to destination system.

SIGNATURE BASED APPROACH TO IDENTIFY THE INTRUSION ON MULTI-TENANT BASED CLOUD USING MTM ALGORITHM

The Private Cloud node has the various SLA based properties. Hence depends upon the profiling of each node can be intruder can attack. Every node has a scope to reduce false alarm rate. Since the scenario comes when an alarm is triggered when there is no attack takes place. The proposed algorithm applied using Linux based BackTrack Operating System through all the connected nodes that is active Multi-Tenant nodes (Grefenstetle J, 1986). The identity of each node is controlled by the central computing node in the cloud. This is essential to withstand even in the case of node failure. Whenever a cloud node trespasses or in bound to the IDS boundary it calculates the likelihood for the particular node. It tracks the signature, builds in details etc. It updates the channel with these details and the particulars are flooded in the index of each node within the boundary (Jiao Licheng, 1995). If the likelihood value is 1 then the node has a primary malicious action then it is navigated to particular path in another layer. This process is iterated until the node value is decreased to 0. If the likelihood value is 0 then the node is not considered to be an intrusion.

In our proposed algorithm we used small world concept. This algorithm works with the concept of multi-tenants in the cloud network. The attacking is done using the transfer of data packets from one tenant to another. The pseudocode of the Multi-Tenant Mapping (MTM) is shown below:

Pseudocode of MTM algorithm

Procedure MTM (MTM_log, MTM_inbound,MTM_outbound,MTM_TriggerAlarm)
begin
Initialize the multi tenant based cloud node to entire path
For all the cloud nodes
Let Initialize all connected parameter=1
Let Initialize all mobility cloud node=1
Check the cloud nodes in same path
Set connected parameter =1
Set unconnected parameter =0
Set channel values=Inf
For all the connected cloud nodes
begin
Apply small world concept
If cloud node=(node_ level2 && node_level3)
TriggerAlarm(1);
Else
Update (MTM_log);
End;
End;
Timestamp(1);
Sleep(1);
Update(MTM_log);
End Procedure

In signature based IDS system if pattern matches then attack can be easily found but when a new attack comes then system fails but snort overcome this limitation by analysing the real-time traffic. Whenever any packet comes into network then snort checks the behaviour of network if performance degrades of network then MTM algorithm stop the processing of packet, discards the packet and stores its detail in the signature database.

The above algorithm has the cloud based intrusion detection for data security for detecting malicious insiders in cloud based multi-tenant system. The initial setup for connecting and configuring the cloud based connected systems with path. For all cloud nodes set the connected nodes parameter as 1 and mobility cloud node as 1. Now this assignment gives the entire network into one. If any unconnected nodes are left in the small network make the parameter value as 0. Set the channel values as infinity because the availability of coverage in the rely of transmission between this small network is low; hence this infinity parameter will provide the available nodes liveliness. Then by applying the small world concept in this network will be given the active nodes in the small cloud based multi-tenant network.

If the cloud node level is 2 or 3 then the alarm is triggered else the log of this MTM algorithm is updated by assigning the timestamp and sleep parameters as 1. So the updated log gives the limit of the inbound and outbound value to keep the node active and attacker status in the network.

MTM performance analysis

The *Detection Rate*, that is the number of intrusion cases detected by the system (True Positive) divided by the total number of intrusion cases present in the test set, it is shown in equation 1.

MTM-DR=Intru. cases detected/ total number of intru (1)

The *False Alarm Rate* is the number of normal outlines classified as attacks (False Positive) divided by the total number of normal outlines and it is represented as shown in equation 2.

MTM-FR=False classification/Total number of outlines (2)

The *True Positive* is a type of areal attack which activates the IDS to create an alarm and it is represented as shown in equation 3.

MTM-TP = Real Attack* Alarm instance (1) (3)

The *False Positive* is a type of an event signing, that is IDS cancreate an alarm when no attack has taken place and it is represented as shown in equation 4.

MTM-FP = MTM-TP (1)/MTM-FR (0) (4)

The *False Negative* is a type of failure of IDS to detect an actual attack and it is represented as shown in equation 5.

MTM-FN = MTM-TP (0)*MTM-DR (0) (5)

The *True Negative* is a type of system when no attack has taken place and no alarm is raised.

MTM-TN = MTM-FP(0)*MTM-TP(0) (6)

The *Noise* is a type of data or intrusion that can activate a false positive.

MTM-N = MTM-FP(1) (7)

IMPLEMENTATION OF SIGNATURE BASED IDS ON CLOUD NETWORK

The implementation of signature based IDS in the cloud network for this first execute the batch file stored in the multi-tenant mapping algorithm. After that the backtrack tool installed in Linux operating system using VMware is started, then two tenants created in the VMware to test the IDS using MTM algorithm. The setup

can be started using physical address of the tenant. The following commands need to be executed to find the Intruder. First the airmon-ng command used to start the networking between the tenants. The airmon-ng command used to detect the channel number. Second the airodump-ng command is used to open the channel to track the data packets. Next the aireplay-ng command is executed to know the authentication for the detected channel number. Finally aircrack-ng command is used to find the key by decryption to open the network. The Internet wicd network manager is used to attack the tenant. For this select the network type and then select the enable the network. After this use the encrypted key to attack the cloud node.

RESULT

The identification of intrusion in each node has data log. Using this log the active cloud users profile can be read by the server controller. The attacker goal is to gain the root of the individual node to gain privilege to the centralized servers to retrieve the information or to exploit the server. Hence we need to prepare separate profiles for privileged user in order to avoid the intruders to gain the access (Wang Guojun, *et al*., 2008).

The advantages over signature based intrusion detection system are (i) fast updating of log, (ii) Multipath navigation for better performance and Reliability, (iii) entrophical model for profiling the network agents, (iv) reduced system load due to six degree separation and (v) quality of Log data is relatively small in size (Wang Guojun, *et al*., 2008).

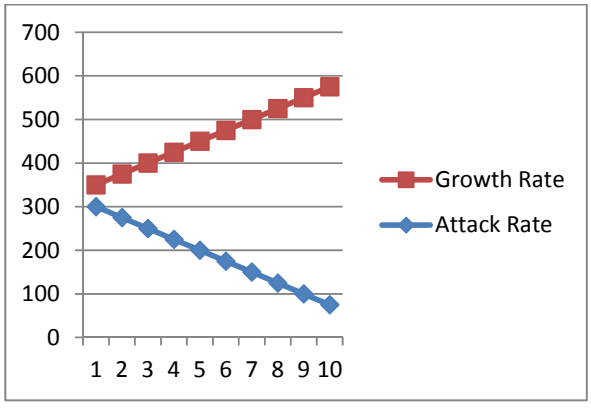

Figure-3. Attack rate vs growth rate.

The attack rate versus growth rate is shown in Figure-4. This result shows that the attack rate is reduced based on the proposed algorithm. The real time results of MTM is shown in Figure-3, that is, the attacks in rising and decreasing level are also shown with outbound and inbound values. The Limitations of this MTM algorithm is t can be seen that misuse detection requires specific knowledge of intrusive behaviour. Collected data before the intrusion could be out of date and yet many times it is hard to detect newer or unknown attacks. Misuse detection has a well-known problem of raising alerts regardless of the outcome. For example a Window worm trying to attack a Linux system, the misuse IDS will send so many alerts for unsuccessful attacks (Luan Qinglin, *et al*., 2008) which may be hard to manage. This model may not always be so practical for inside attacks involving abuse of privileges. The knowledge about attacks is very dependent on the operating system, version and application hence tied to specific environments.

CONCLUSIONS

The security against the malicious attacks can be detected using various from methods on the wireless network. This paper contributed a new class of malicious attacks or intrusions in the cloud network and addresses the mischievous and malicious behaviour, which is the root cause for the modification of healthcare data stored in the cloud network. This paper also can be handled by multi-tenant users for various applications. This is the first attempt to identify the multi-tenant user attacks in cloud network. In this attempt a new MTM algorithm is introduced, that identifies the multi-tenant user database malicious attacks. The limitations of the algorithm are given in the last section. The basic idea of this algorithm is devised from the wireless LAN malicious attacks. Finally the results shows that the proposed algorithm has a promising prediction for malicious attacks for multi-tenant based cloud network.

REFERENCES

Theuns V and Ray H. 2002. Intrusion detection techniques and approaches", Computer Communications. 25(15): 1356-1584.

JingwenTian and Meijuan Gao. 2009. International Conference on Networks Security, Wireless Communications and Trusted Computing.

Bezemer C-P, Zaidman A. 2010. Multi-tenant SaaS applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution.

(IWPSE), Antwerp, Belgium. ACM New York, NY, USA. 58(2): 88-92.

D. E. Denning. 1987. An Intrusion-Detection Model. IEEE transactions on software engineering. 13(2).

MIT Lincon Laboratory. 1999. 1999 DARPA Intrusion Detection Evaluation Data Set. available:

http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html.

Forrest S. A. Hofmeyr A. Somayaji and T. A.Longsta. 1996. A Sense of Self for UNIX Processes. Proceedings. IEEE Symposium on Computer Security and Privacy.

S. A. Hofmeyr, A. Somayaji and S. Forrest. 1998. Intrusion detection using sequences of system calls. Computer Security. 151(6).

T. Inagaki. 1999. Measurement of network performance inmbone. Master's thesis, Graduate School of Science and Technology, Waseda University, Tokyo, Japan.

Zhao Zhenning, XuYongmaom 1996. Introduction to fuzzy theory and neural networks and their application, Beijing: T.Singhua University Press.

Grefenstetle J. 1986. Optimization of Control Parameters for Genetic Algorithm. IEEE Trans on System, Man and Cyber. 16(1): 122-128.

Jiao Licheng. 1995. Neural Network System Theory. Xian: Xi an Electronic Science and Technology University press.

Wang Guojun, Yue Zhiqiang. 2008. Application Research of Support Vector Machine in the Intrusion Detection. Guangxi Journal of Light Industry. 7: 51-52.

Luan Qinglin, Lu Huibin. 2008. Research of intrusion detection based onneural network optimized by adaptive genetic algorithm. Computer Engineering and Design. 29(12): 3022-3025.