Secure File Sharing With Intrusion Detection in Cloud Computing

Mr. Ravi V. Kute[1] Mr. Nilesh K. Bodkhe[2] Mrs. Tejaswini G. Ulemale[3] Mr. Sumit S.Sagane[4]
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]PRPCEM Amravati, Amravati University

Abstract— File distributing and sharing is one of the most commonly used services in cloud computing and the requirement of data security grows with the cloud computing spreading. Traditional methods of securing data are challenged by specific nature and architecture of cloud. With increasing sophistication of cyber attackers and advancement of cryptanalysis techniques, encryption alone is not sufficient to ensure data security. This project propose a collaborative model consists of the Intrusion Detection System functions based file sharing system. It introduce a secure data sharing scheme, for dynamic groups in an untrusted server.

Key words: Cloud Computing, Intrusion, Encryption, File Sharing

I. INTRODUCTION

The shared data in online servers, however, usually contains users sensitive information such as personal profile, financial data, health records, etc. and needs to be well protected. Therefore, it becomes a big challenge to protect the privacy of those shared data in server, especially in cross-server and big data environment. Therefore we introduce secure data sharing system of intrusion detection and system. Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group.

A. Motivation:

Now a day's security is more important factor in the network. User is interested more in the security rather than the other factors which are included in the network. In the existing system a data owner only needs to distribute a single key to a user for sharing a large number of documents and the user only needs to submit a single trapdoor to the cloud for querying the documents.

B. Aim:

"To implement a secure data sharing scheme, for dynamic groups in an untrusted server environment. A user is able to share data with others in the group without revealing identity privacy to the server."

C. Objectives:

To introduce a secure data sharing scheme, for dynamic groups in an untrusted cloud server. To propose an approach to detect intrusion in the cloud using pattern matching algorithm.

D. Scope:

The data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group.

II. PROPOSED MODEL

In this paper, we propose a new way to protect data and resources in the cloud computing environment against distributed attacks which can produce from external or internal network.

This model is focused on the infrastructure layer as services where we proposed a collaborative intrusion detection and prevention system working with the hybrid detection technique added to the latter event correlation to use the entire network to correlate information and infer that intrusion occurred at such place infrastructure.

Also to improve functioning of our system in terms of detection and recognition of attacks, we integrate the signature algorithm apriori to generate new attack signatures from known signatures in order to enrich the database of our system and therefore we will be able to detect and block variants of known attack like distributed attack and to reduce the no. of false positives that can occur on cloud architecture.

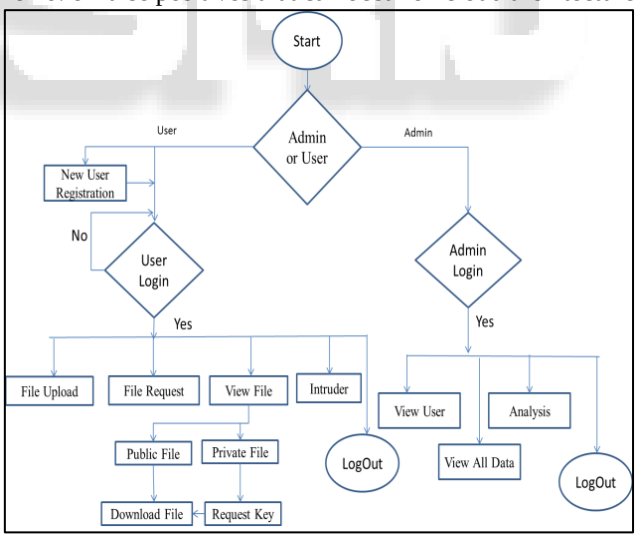

Fig. 1: Flowchart of Proposed System

Fyodor, initial contributor of audit tool Nmap in[3] describes the portscan as recognition phase. During which an attacker determines what type of network protocol or services offers a machine to discover exploitable communication channel in order to establish his attack.

III. VARIABLES OF PORTSCAN

When attacker wants to perform a portscan on network, he can adjust some variables. these variables let the attacker be more descrete or know specific information about remote scanned hosts.

A. Techniques:

Depending on goal of attacker he would use a specific technique rather than another .Most of portscan technique give information about state of the targeted ports whereas other techniques give information about service or operating system.

B. Timing:

An attacker can adjust the speed rate of portscan attack .By doing this, he can evade IDSs, because most of them do not detect portscan when they are executed very slowly.

C. Targeted Ports:

Lee defines different types of targeted ports in[5].her paper introduces vertical horizontal and block scans, presented below. Vertical scans are portscans that target numerous ports on singular remote hosts. Horizontal scan targets only one port on several remote hosts

IV. DISTRIBUTED PORTSCAN

Distribution of attack is to divide it into tasks that will perform by different machines in different ways for these techniques are for its methods of distribution, the attacker has set of machines called scanner used for his work. Authors presents two methods of distribution:

A. Naive distribution:

It consists in a sequential distributed scan , the attacker select one of scanner he control and start scanning the target work with it .When scanner is detected ,the attacker select different scanner and resumes the portscan .

B. Parallel Distribution:

To change this distribution consists in splitting the whole set containing targets and port between scanners. Each scanner ha subtask to perform and then he communicates the result to the coordinator.

V. SECURITY AND CLOUD COMPUTING

Among the main elements of traditional network security and cloud network are the firewalls .All traffic between these networks must pass through firewall. Also firewall filters authorized traffic defined by local security policies. Firewall would not see attacks inside network.

Although security often based on firewalls, we found it is not enough to use only to ensure all protected architecture type cloud. Cloud computing security must be adaptable to dynamic architecture .Cloud users may be malicious or an attacker could have control of one of several internal hosts that's way cloud security must insures applications availability and data integrity.

VI. INTRUSION DETECTION SYSTEM

Security management can be split in three main parts: prevention, detection and correction. IDSs deals with detection part. Article describes intrusion detection as process of monitoring event and analyzing them for sign of intrusion or attempt to compromise the confidentiality, integrity, availability or to bypass the security mechanism for computer or network.

A. Location:

The most common way to classify IDSs is to group them by location. In [9] authors describe the type of IDSs: network based IDSs operate intrusion detection directly on network they detect attack by capturing and analyzing network packets. Host based IDSs operate on information collected from within an individual computer system. They analyze system logs and critical system files to detect intrusion. Distributed IDSs uses several IDSs to correlate events from different places of network.

B. Architecture:

Recently distributed systems spread and this also applies to IDSs. Distributed IDS treat these events all security elements placed at different points in the system studied. Solutions adopt different architectures with respect to analysis of events collected in several places. The first solution to satisfy a centralized analysis, i.e. analyzing single IDS events.

C. Detection Methods:

For detecting malicious activities IDS use detection method. They function automatically, analyze the information they monitor and raise alarm whenever they detect intrusion .Most used techniques are Pattern matching and Anomaly based detection.

D. Pattern Matching:

Consists in scanning information and looking for known patterns into it. Whenever IDS have found a similarity it raises an alarm. Signature based detection can detect known intrusions , so the main weakness of this method is the need of constant update the database containing known patterns.

E. Anomaly Based Detection:

Adopts a simple approach ignore everything that is normal and raise an alarm if that derivate from normality. This kind of detection method can be effective in detecting unknown attacks but it may also generate a huge amount of false alarm.

F. Event Correlation:

This technique presented in[10] is a new method used by CIDS . Event correlation allows the use of entire network to correlate events and deduce an attack occurs in several places in system.

VII. INTRUSION PREVENTION SYSTEM

IPS has been developed from IDS and contain the functionality of latter but they are more sophisticated with the ability to take immediate action to prevent malicious behavior in [11], the paper presents a comparative study between the two systems as shown in table.

IDS	IPS
Installed on network segments and on hosts	Installed on network segment and hosts
Sites on network passively	Sits inline
Central management control	Central management control
Cannot parse encrypted traffic	Better at protecting application
Better at detecting and hacking attacks	Ideal for blocking web defacement

Alerting product (reactive)	Blocking product (proactive)

VIII. ESSENTIAL CHARACTERISTICS

To effectively integrate the cloud computing model detection systems and intrusion prevention must have following characteristics:

A. Detection of Network Attack on Each Layer:

IDPS should be capable of detecting and preventing intrusion at each component like front end, back end or virtual machine and virtual network.

B. Low Computational Cost and Faster Detection Rate:

In cloud computing high number of users are involved. So high number of requests may turn into high traffic rate in cloud. Therefore IDPS should have faster detection at lower cost.

C. Low False Positives:

It can be defined as the number of false alerts generated by IDPS. This should be low for integrated it in cloud .False positive alert may be generated.

D. Low False Negatives:

It can be defined as an inability of IDPS to detect the true intrusion. There are number of reasons for causing the false negatives. If the traffic exceeds due to ability of a switch, not all the network packets passing through such switch can be monitored.

IX. RELATED WORK

Much work has been done for cloud computing and intrusion detection system, but there are still issues that have not been resolved. Researchers working in this field in order to overcome the current security threats in cloud using either only type network IDS to detect distributed attack or intrusion detection and prevention system but with limited functionality to address constraints and security issues that we mentioned at beginning of our work .

The multithreaded NIDS based on three modules: Capture, analysis and reporting .The first module is responsible for capturing the data packets and sends them to analysis module that processes efficiently via set of predefined rules to distinguish bad packets and then generating alerts .Finally the reporting module can read these alerts immediately and prepares reports. At this stage the service called "third party monitoring and advisory service" continues the work by generating and sending report cloud customer information to be aware of intrusion or attack that target its data or its environment work and another report type "comprehensive expert advisory report" sent to the service provider cloud .

The authors in have proposed a method based on implementation of an intrusion detection and prevention system(IDPS)working with technical anomaly detection and detection by signature recognition these two techniques working collaboratively to perform a deep analysis on resources in cloud environment in order to detect intrusions. The proposed system also provided with capabilities of prevention rather than detection so it can stop and block attacks and intrusion s, however implement a centralized IDPS surrounded a distributed system like cloud computing is not beneficial ,because if the node analysis stops the whole architecture will no longer protect ,more than that save and generate new signature of proper functioning of technique based on just threats detected by technique (AD) can cause increased number of false positives and thus degrade system performance.

X. CONCLUSION

To share data flexibly and securely in cloud computing is vital thing. Users always prefer to upload there data on cloud and share the uploaded data among different users. The main drawback of cloud computing is the security issue. Cryptography is a one of best solution which provides security to share selected data with desired cloud data users. Sharing of decryption keys in secure way plays important role. The proposed Public-key cryptosystems provides delegation or leader key of secret keys for different cipher text classes in cloud storage.

In future it provide a secure environment where a data owner can share data with members of his group while preventing any outsiders from gaining any data access in case of malicious activities such as data loss and theft. Cloud is a potential for future research in the context of data sharing in the Cloud.

REFERENCES

[1] Zhongma Zhu and Rui Jiang, "A Secure AntiCollusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 1, January 2016.

[2] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based PrivacyPreserving Authentication Protocol in Cloud Computing," IEEE Transactions On Parallel And Distributed Systems Vol:Pp No:99 Year 2014

[3] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013.

[4] Kaiping Xue and Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," 2366152, IEEE Transactions on Cloud Computing. vol. 2, no. , pp. 459-470, Oct.-Dec. 2014

[5] HUANG Qinlong, MA Zhaofeng, YANG Yixian, FU Jingyi and NIU Xinxin, "EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing," Chinese Journal of Electronics Vol.24, No.4, Oct. 2015.

[6] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013.

[7] Ming Li Member, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, " Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," IEEE Transactions On

Parallel And Distributed Systems Vol. Xx, No. Xx, Xx 2012

[8] Qiang Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, Vol. 9, No. 11, November 2014.

[9] Xinyi Huang, Joseph K. Liu, Shaohua Tang, IEEE, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," IEEE Transactions On Computers, Vol. 64, No. 4, April 2015.

