International Journal of Engineering Researches and Management Studies

INTRUSION DETECTION PROCEDURE FOR CLOUD SERVERS USING ATTACK GRAPH MODEL

D.SUBA[*1] and A.SENTHIL KUMAR[2]
[*1]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Asst.professor, Dept.of.Computer science, Tamil University, Thanjavur-613010.

ABSTRACT

A recent Cloud Security Alliance (CSA) survey shows that among all security issues, abuse and nefarious use of cloud computing is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In traditional data centres, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. For better attack detection, this research work incorporates attack graph analytical procedures for the intrusion detection process. Our proposed solution can be deployed in an Infrastructure-as-a-Service (IaaS) cloud networking systems, and we assume that the Cloud Service Provider (CSP) is benign. An attack graph is a modelling tool to illustrate all possible multi-stage, multi-host attack paths that are crucial to understand threats and then to decide appropriate countermeasures. In an attack graph, each node represents either precondition consequence of an exploit. The actions are not necessarily an active attack since normal protocol interactions can also be used for attacks. Attack graph is helpful in identifying potential threats, possible attacks and known vulnerable of all known abilities in a cloud system. Since the attack graph provides details of all known vulnerabilities in the system and the connectivity information, we get a whole picture of current security situation of the system where we predict the possible threats and attacks by correlating detected events or activities. In the analysis stage, the AGM suggests the total no of files, file paths, uploaded date of file in the cloud Servers and finally the file sizes. Thus any change or alternation in the above metrics is reflected in the graph as there is a chance of intrusion Occurrence. Hence this research suggests, new techniques to counter against threat which occurs in cloud server environment.

Keywods:- *Cloud Security Alliance, Cloud Service Provider, Attack graph model, Infrastructure-as-a-Service.*

I. INTRODUCTION

In this research work, recent studies have shown that users migrating to the cloud consider security as the most important factor. A recent Cloud Security Alliance (CSA) survey shows that among all security issues, abuse and nefarious use of cloud computing is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In traditional data centres, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security holes in cloud data centres, where cloud users usually have the privilege to control software installed on their managed Virtual Machines, may not work effectively and can violate the Service Level Agreement (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. we propose ATTACK GRAPH MODEL (Network Intrusion detection and Countermeasure selection in virtual network systems) to establish a defence-in-depth intrusion detection framework. For better attack detection, ATTACK GRAPH MODEL incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of ATTACK GRAPH MODEL does not intend to improve any of the existing intrusion detection algorithms; indeed, ATTACK GRAPH MODEL employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise Virtual Machines, thus preventing zombie Virtual Machines. The sections of this research work is grouped as literature survey which includes detecting attacks related to cloud architecture, vulnerabilities counter measures, and other security mechanisms. The existing attack graph model suggests vulnerabilities detection methods relating to normal network objects only, but the proposed method of this research work identifies the vulnerabilities that influences security with relevant to cloud architecture, since deployment of any service in the cloud can't be monitored easily , i.e. exact or dynamic file sizes in particular. The analysis part of this research work, accounts namely the file sizes, file paths, number of files, and date uploaded to detect vulnerability occurrence in cloud architecture.

Existing System

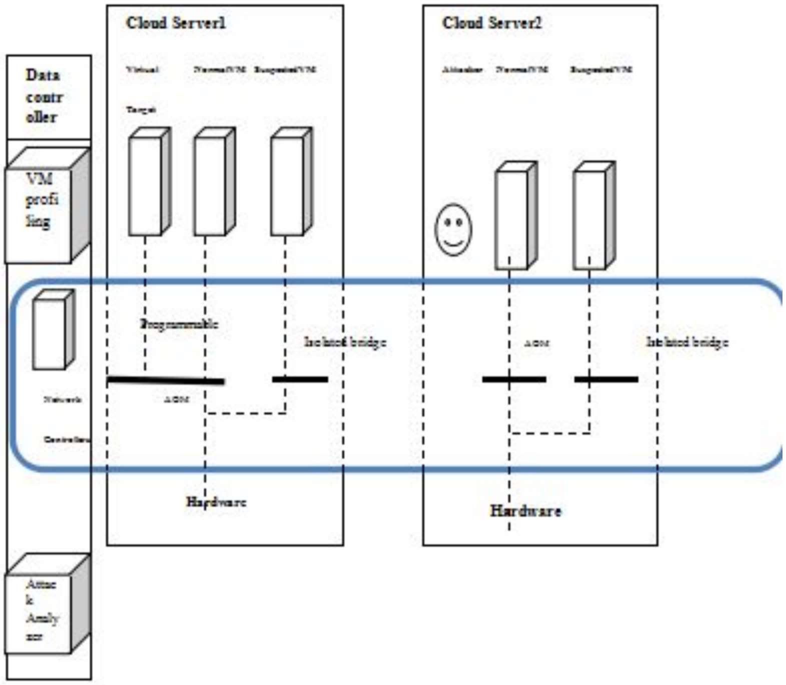
In existing system describes the vulnerabilities could be detected by system administrator i.e. system administrator controlled all host machines.

Proposed System

Our proposed have some solution to detect vulnerabilities in cloud server using attack graph model. The attack graph model using some metrics that is total number of files, file paths, uploaded date of files in the cloud server. If any changes or alteration in the metrics that is occurred in the graph. This research using new techniques to counter against threat occurs in cloud server.

II. SYSTEM DESIGN

The systems architecture establishes the basic structure of the system, defining the essential core design features and elements that provide the framework for all that follows, and are the hardest to change later. The systems architect provides the architects view of the users' vision for what the system needs to be and do, and the paths along which it must be able to evolve, and strives to maintain the integrity of that vision as it evolves during detailed design and implementation.



III. PROCEDURE INPUT DESIGN

INPUT:

User Login name and Password

INPUT:

After login valid user upload the Files

INPUT:

After uploaded successfully checks the file has been modified or not.

Counter Measure Selection Model

INPUT DESIGN:

Attacker attacks multiple cloud servers it has to detect the both.

IV. OUTPUT DESIGN

OUTPUT:

If Valid user Open the window otherwise error page.

OUTPUT:

Files uploaded successfully.

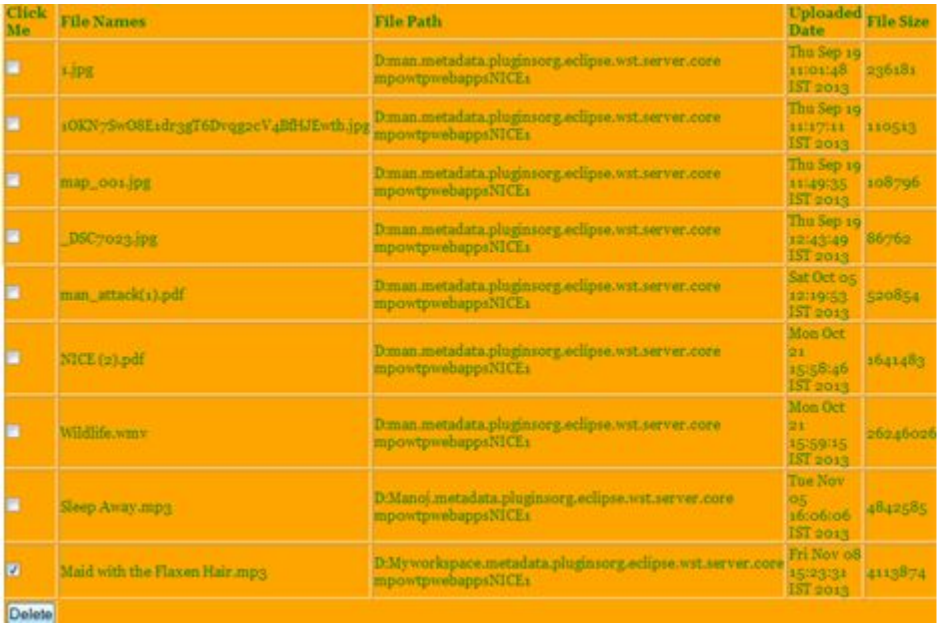
OUTPUT:

If Modified find the attacker else Stores the data.

OUTPUT:

It detects both and removes the attacker from the both cloud.

V. PERFORMANCE ANALYSIS



Click Me	File Names	File Path	Uploaded Date	File Size
□	1.jpg	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Thu Sep 19 11:01:48 IST 2013	236181
□	1OKN7SwO8E1dr3gT6Dvqg2cV4BfHJEwtb.jpg	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Thu Sep 19 11:17:11 IST 2013	110513
□	map_001.jpg	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Thu Sep 19 11:49:35 IST 2013	108796
□	_DSC7023.jpg	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Thu Sep 19 12:43:49 IST 2013	86762
□	man_attack(1).pdf	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Sat Oct 05 12:19:53 IST 2013	520854
□	NICE (2).pdf	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Mon Oct 21 15:58:46 IST 2013	1641483
□	Wildlife.wmv	D:man.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Mon Oct 21 15:59:15 IST 2013	26246026
□	Sleep Away.mp3	D:Manoj.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Tue Nov 05 16:06:06 IST 2013	4842585
☑	Maid with the Flaxen Hair.mp3	D:Myworkspace.metadata.pluginsorg.eclipse.wst.server.core mpowtpwebappsNICE1	Fri Nov 08 15:23:31 IST 2013	4113874

The above figure explain that admin has a ability to view all the details and function of the user and admin can delete the data which can be uploaded by the user.

VI. CONCLUSION

In this paper, we presented Attack Graph Model, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. Attack Graph Model utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of Attack Graph Model and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers.

REFERENCE

1. *Yuan Cheng, Jaehong Park, and Ravi Sandhu"An Access Control Model for Online Social Networks Using User – to – User Relationships"*
2. *B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," IEEE Int'l Conf. Computer Communication and Informatics (ICCCI '12), Jan. 2012.*
3. *H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, Dec. 2010.*
4. *Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting spam zombies by monitoring outgoing messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198–210, Apr. 2012.*
5. *G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: detecting malware infection through IDS-driven dialog correlation," Proc. of 16th USENIX Security Symp. (SS '07), pp. 12:1–12:16, Aug. 2007.*