ISSN: 0971-2143
Vol-31-Issue-21-May-2020

STUDY ON CO-RESIDENT ATTACKS IN CLOUD COMPUTING

Ruchika Bhutada[1], Bhargavi Chevva[2], Anurag Muthyala[3]
[1]Student, CSE Department Sreenidhi Institute of Science and technology, Yamanampet, Hyderabad-501301
[2]Student, CSE Department Sreenidhi Institute of Science and technology, Yamanampet, Hyderabad-501301
[3]Student, CSE Department International Institute of Information Technology, Gachibowli, Hyderabad-500032

ABSTRACT

Cloud computing, a profound technology has come a long way since its inception. But, it has privacy, security and maintenance issues that need to be addressed. The prominent security concerns are data breach and loss, denial of services, abuse of cloud services, Co-Resident attacks etc. Our paper discusses two essential topics. First, detection and analysis of certain security problems using Intrusion Detection and Prevention System. Secondly, the paper focuses on reviewing a conventional threat, co-resident attack (known also as side channel attack, co-location attack etc.) We review an algorithm based on semi supervised learning technique to prevent the attacks in the virtual environment.

Keywords: Cloud computing, cloud security, IDPS, Co-resident attacks

1. INTRODUCTION

Cloud computing is the evolving arena of today's technological world. Cloud computing provides us with the opportunity to utilize high speed computation along with great models on someone else's software. The services are Infrastructure as a Service (IaaS) Software as a service (SaaS) and Platform as a service (PaaS). Each service has its own application

The description of cloud computing provided by The US National Institute of Standards and Technology (NIST) is as follows: The NIST Definition of Cloud Computing:(NIST, http://csrc.nist.gov):
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
The features of cloud computing are: On demand service: Cloud can be utilized by the user's based on their requirement. Cloud services are provided to the user on pay per use basis. Broad network access: Resources on cloud can be accessed from anywhere, at any time via multiple range of devices (i.e., laptop, mobile, personal computer, tablet etc.) Resource pooling: Multi tenancy is a characteristic of cloud computing. Here,

ISSN: 0971-2143
Vol-31-Issue-21-May-2020

more than one instances can be created over the same primary software (server). Rapid elasticity: Cloud resources can be expanded as per user's requirements. Cloud computing constitutes of four deployment models namely public, private, hybrid and community cloud. Each model can be customized based on the requirements of the particular business model
or setup is needed for providing on demand network access to utilization of resources are achieved with the help of virtualization. Through virtualization abstraction of fundamental computing resources such as hardware and storage can be achieved. In virtualization, more than one computing environment can exist on the same physical server. This is known as a co-location or co-residence. Each computing environment is referred to as a Virtual Machine(VM). The VM's on a server enjoy all computing resources of the server and are almost unaware of the existence of other VM's on the same server. In cloud, user's information is stored on the servers. The users are ignorant of where their data is being stored. So the major concern of cloud are its security issues. Few prominent security threats are Data breach and loss, account and service hijacking, malicious insiders, shared technology vulnerabilities, colocation attack, denial of services, abuse of cloud services etc. Due to high chances of such attacks, the confidentiality and privacy of customer's data is at stake. Intrusion Detection and Prevention System (IDPS) can be used to detect the occurrence of any attack and measures to prevent such attacks.

In a cloud, data of each user is stored independently using virtual isolation. But there exists a possibility of illegal access of a user's data by a malicious user co-located on the same server. It is known as co-resident attack or side channel attacks. They are stealthy in nature and mostly go undetected. Our paper mainly focuses on prevention of co-resident attacks. The remaining information of the paper is arranged as follows, as we know that Cloud computing has many interesting and advantageous features due to which it is being adopted by infrastructures, government agencies. But, it has security and maintenance problems which will be discussed in part 2 of the paper. In the next part the focus is on Intrusion Detection and Prevention System (IDPS)to protect computer resources from any attacks. Part-4 deals with a method to tackle security threat: Co-Resident attacks (also known as side channel attacks or co-location attack or co-residency). A preventive algorithm based on semi supervised learning to tackle co-resident attack is reviewed in part 4 of the paper.

SECURITY CONCERNS

In today's technological era data is a major resource and handling it efficiently is a tedious task. Cloud computing provides scalable resources and on-demand service. But there are many security concerns which need to be tackled. Few prominent security threats are Data breach and loss, account and service hijacking, malicious insiders, shared technology vulnerabilities, co-location attack, denial of services, abuse of cloud services etc. Due to high chances of such attacks, the confidentiality and security of customer's data is at stake. Some of these threats such as Brute force attack can easily be detected and resolved. On the other hand, attacks like co-resident attacks are very difficult to detect. Co-resident attacks or side channel attacks are the most challenging threats to detect and resolve. In cloud, more than one Virtual Machine (VM) instance is allocated on the same physical server. Our paper focuses on a solution to these attacks. Co-resident attacks occur on the same physical server.

B.CO-RESIDENT ATTACKS

Co-resident attacks target sensitive information in other virtual machines on the same physical server.

ISSN: 0971-2143
Vol-31-Issue-21-May-2020

Virtualisation techniques [1] provide logical isolation between VM's that locate on the same server (i.e., co-resident VM's). This means that programs running on one VM should not interfere with other programs that run on co-resident VM's. Nevertheless, this can happen in real cloud systems.

Intrusion detection and prevention system (IDPS) mainly focus on identifying possible incidents or threats posed to a system. In our model, we mainly divide the possible side channels based on the risk they pose to the cloud and its user's. viz. high, medium and low risk. The presented approach focuses on clarifying the VM requests based on their behaviour there by analysing the risk factor. Malicious user's are categorized as high risk and further increase the cost of the attacker to be further categorized as low risk. We use clustering analysis to perform this categorization into two categories as below.[8]Signature based: In signature based IDPS, attacks are detected by comparing observed events against known specific patterns. Signaturebased detection is the easiest form of IDPS. It is very successful at locating known attacks but fails largely at locating previously unknown attacks and attacks disguised using evasion techniques, and other types of known attacks.

Anomaly based: Anomaly based detection techniques are used to detect malicious behaviour based on normal behaviour of user's, hosts, network connections, or applications.

Normal profiles are modelled by observing the characteristics of typical activity over a particular time period. In Anomaly based detection, observed events are compared against definitions of an activity that is considered to be normal. Artificial neural network (ANN) based IDS: Artificial Neural Networks are used to identify intrusion based on pattern recognition techniques. Fuzzy logic based IDS and data mining techniques are used to detect malicious behaviour present on the network traffic.

2. LITERATURE SURVEY

For the process of virtualization, Vattikonda et al. [2] proposed to completely remove or slightly modify the high resolution clocks that many side channels depend on, while Jin et al. [4] redesigned the architecture of cloud computing organizations. More afresh, Zhang et al. [5] suggested to carry out periodic timeshared cleansing of cache, in order to make the side channel more turbulent. Furthermore, Varadarajan et al. [6] presents a scheduling mechanism named minimum run time (MRT) which is effective in preventing side channel attacks based on cache. These two methods need lesser modifications to existing cloud platforms and hence are easier to position. Though the researchers in [1] proposed a smart online technique(OSDF) to identify malicious user and mitigate such VM's into a quarantine zone for further analysis. Their main objective was to prevent co-resident attacks by (increasing the tracing complexity of executing VM's).
The technique uses BoSC technique to learn the behaviour of hosted VM's. The Linux tool strace was used to obtain a list of syscall and maintain the frequency of syscall provoked by a particular VM. Based on it, any VM if found malicious is migrated to another host. The proposed technique could positively decrease the number of attacks from 270 to 1, but observed an increase in down time during migrations. The effective time required to carry out a task has drastically increased for both stateless and state full applications due to frequent network disconnections. Moreover, the additional overhead of maintaining the syscall list makes it difficult to adapt in real time cloud services.

ISSUES REGARDING ATTACKS

ISSN: 0971-2143
Vol-31-Issue-21-May-2020

Allocation of user's requests plays an important role in predicting the chances of colocation. Cloud providers allocate their VM requests based on their VM allocation policy. The commonly used policies are: Most VM policy, Random VM policy and Least VM policy. In Most VM policy, user's requests are sent to the same server until it cannot handle any more of them. In Least VM (Virtual machine) policy, the user's requests are widely spread onto different servers for better computing capabilities. In Random policy, VM requests are randomly allocated among the servers. Among these three existing VM policies the risk of co-location is seemingly high in case of Most Virtual Machine policy followed by Least Virtual Machine policy. In Random policy, though co-location is highly unpredictable, the chances are quite considerable. Usually in such VM allocation situations, the attacker:

(1) starts a number of VM's (2) Checks if colocation is achieved with desired target. (3)Turns off those VM's which are no longer needed. (4)The malicious use continues the above steps until co-location is achieved.

In most simple case, attacker follows the above technique from single account. It is quite easy to detect.

The attacker may create many accounts and create only one VM from each account and thereby increasing chances of co-location. This can be prevented by using PSSF(Previously Served Server First) VM allocation policy. IN PSSF the new VM request from a user is allocated to the server which once or is hosting the same user's VM. This allows only VM's of the same user to co-locate on a server, thereby considerably decreasing the chances of colocation with malicious users. However, a VM request from a new user treated normal and allocated another server.

When PSSF is deployed, the possible behaviour of attacker include :(1) create more VM requests from different accounts otherwise all of them will be stacked together. (2) Start one VM request from each account. This will increase risk of colocation.

PSSF treats all user's requests equally which is advantageous to the Attacker. So classification of VM's is required.

We take into consideration the differences between the behaviours of illegal users those of who are the attackers and authorized that is the legal user's. By applying clustering analysis,[9] and constructing multiple semi supervised
SVM's, we classify all user's into three categories − high risk (malicious), medium risk (uncertain), and low risk (legal) − and modify the VM allocation process accordingly.

The defence mechanism consists of two main parts which are the modules: 1. The detection module 2. The response module. When a user demands to start a new VM, the detection module loads previous data from the database, classifies the user into one of the three types: low/medium/high risk. (This is done by clustering analysis and partial labelling.) The outcome is sent to the response module. It allocates VM's to specific servers based on their behaviour. This results in allocation of similar types of VM's hosted on the same server.

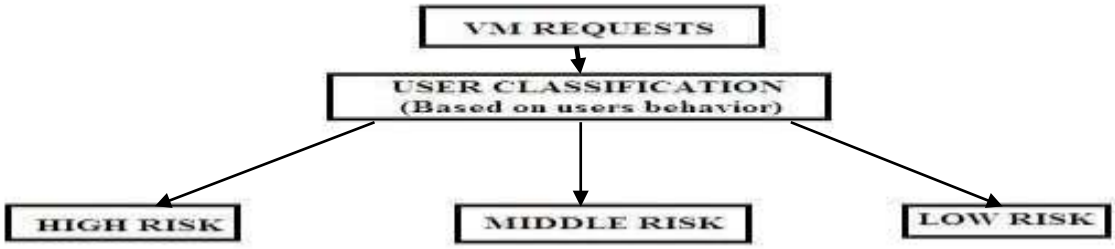
ISSN: 0971-2143
Vol-31-Issue-21-May-2020

CLUSTERING ANALYSIS

For the next step, in our research we studied that the users where to be classified into three domains, this being based on their activity on the cloud. This classification is important as it helps us concentrate on what is to be dealt with first, to up hold the cloud's security. The Virtual Machine requests are analysed based on their behaviour previously stored in the dataset. Here instead of analysing individual account, they are categorized into groups of accounts which are comparatively lesser in number

Fig-1 Users to be classified.

After clustering of nodes into groups, each node is labelled as either low risk(if the behaviour of corresponding nodes in the group is similar to that of normal or legitimate user's) and into



high risk(if the behaviour of the VM's in the group is similar to that of high risk). Few nodes which are unable to be classified into either low risk or high risk continue to be medium risk.

Once the classification of the new VM request is categorized, it is allocated to the particular server accordingly. We proceed once the labelling is done, from the figure1 we have for example, three kinds users indicated with symbols #, % and @. We then classify them as HR, MR and LR that stands for high risk, medium risk and low risk as shown in figure 2.

PARTIAL LABELING

Fig-2 Partial classification

COST OF ATTACKER

ISSN: 0971-2143
Vol-31-Issue-21-May-2020

The major criteria is not to identify a malicious user or attacker as high risk but to prevent the attacker being categorized as low risk. Once the attacker gets categorized as high risk, it is not possible to achieve co-residence with target virtual machine.

To be reclassified once again as low risk, the attacker will start VM's and keep them running for a considerable amount of time and not start many VM's at the same time. The attacker need to control his actions to prevent from being reclassified as high risk or low risk. This provides an opportunity for the attacker to be classified as low risk but with high cost.

The cost function [9] of the attacker may be defined as:

$$C(N, LEN) = -\frac{w_1/MAX_{1}^{95} + w_3 + b}{\alpha w_2 + w_4} + \left\lceil \frac{N}{4} - 1 \right\rceil len_{min}$$

Wa= this denotes the probability of cost of attack and co-location. Here (a=1,2,3,4) Where, w is the normal vector.

MAX195 = 95th percentile of active percentage.
b = constant
α = MAX495\ MAX295
N= total number of VM's started.
Len(min) = third quartile of the VM's running time.
When being labelled as low risk is more expensive, the attacker can create a new account. But to do this, attacker needs to pay the initial cost. Thus the overall cost of the attacker is increased minimizing chances of co-resident attacks. This is a complicated problem for which very few solutions are provided. This paper reviews an innovative solution including studies from artificial neural networks, signature detection etc. The attacker's cost provided here can be taken as a reference for further research purposes.

DRAWBACKS

One of the drawbacks is the limited classification levels. Sometimes, a user may have features which are closer to any of the above clusters. This leads to inefficient classification. Another drawback is the classification is not unsupervised. It cannot add new classifications or consider new features for classifying them.

3. CONCLUSION

The paper reviews a mechanism to prevent the stealthiest security problem of cloud computing Co-Resident attacks. It specifies a way to categorize VM's into high, low and medium risk and allot them to servers hosting the VM's of similar kind. The paper also discusses a secure VM allocation technique known as Previously Selected Server first (PSSF) policy which limits the attacker's possibilities. Thus the paper reviews and studies a possible approach to solve co-resident attacks thereby contributing to the advancements in cloud computing and a window of arenas for future scope and research in this field.

ISSN: 0971-2143
Vol-31-Issue-21-May-2020

FUTURE SCOPE

The approach studied enables a scope for further study in this field. Co-resident attacks are considered a complicated problem for which very few solutions are provided. This paper reviews an innovative solution including studies from artificial neural networks, signature detection etc. The attacker's cost provided here can be taken as a reference for further research purposes.

4. REFERENCES

[1] P. Barham et al., "Xen and the art of virtualization," ACM SIGOPS Oper. Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.
[2] B. Vattikonda, S. Das, and H. Shacham, "Eliminating fine grained timers in Xen," in Proc. 3rd ACM Workshop Cloud Comput.Secur. Workshop (CCSW), 2011, pp. 41–46.
[3] J. Wu, L. Ding, Y. Lin, N. Min-Allah, and Y. Wang, "XenPump: A new method to mitigate timing channel in cloud computing," in Proc. 5th IEEE Int. Conf. Cloud Comput.(CLOUD), Jun. 2012, pp. 678–685.
[4] S. Jin, J. Ahn, S. Cha, and J. Huh, "Architectural support for secure virtualization under a vulnerable hypervisor,"in Proc. 44th Annu.IEEE/ACM Int. Symp. Microarchitecture (MICRO), Dec. 2011, pp. 272–283.
[5] Y. Zhang and M. K. Reiter, "Düppel: Retrofitting commodity operating systems to mitigate cache side channels in the cloud," in Proc. ACM SIGSAC Conf. Comput.Commun.Secur.(CCS), 2013, pp. 827–838.
[6] V. Varadarajan, T. Ristenpart, and M. Swift, "Scheduler-based defenses against cross-VM side-channels," in Proc. 23rd USENIX Secur.Symp., 2014, pp. 687–702.
[7] Y. Azar, S. Kamara, I. Menache, M. Raykova, and B. Shepard, "Colocationresistant clouds," in Proc. 6th ACM Workshop Cloud Comput. Secur., 2014, pp. 9–20.
[8] Han, Yi. (2015). Defending against coresident attacks in cloud computing.
[9] Yi Han, TansuAlpcan, Jeffrey Chan, Christopher Leckie, and Benjamin I. P. Rubinstein "A Game Theoretical Approach to Defend Against Co-Resident Attacks in Cloud Computing: Preventing Co-Residence Using Semi-Supervised Learning", March 2016.