ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

SECURITY MECHANISM FOR DEFEND AGAINST CO-RESIDENTIAL ATTACK IN CLOUD COMPUTING

J.SIVA BHARATHI[1]
PG SCHOLAR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
KALASALINGAM INSTITUTE OF TECHNOLOGY
KRISHNAN KOIL,INDIA
sivabharathi.3093@gmail.com

R.ANANTHA KUMAR[2]
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
KALASALINGAM INSTITUTE OF TECHNOLOGY
KRISHNAN KOIL,INDIA
r.ananth05@gmail.com

Abstract:

Cloud Computing is a system of using remote servers being hosted on the internet to store, manage and process data. Security is one of the major issues faced by the cloud computing environment while sharing resources over the internet. This paper deals with one such threat called Co-residential attack where venomous users can extract confidential information from others by co-locating on the same server. Previously the attack was mitigated by a new virtual machine allocation policy with other traditional methods of allocation. Further improvement is made for increasing the efficiency of the policy with density-based clustering algorithm by classifying the types of users according to their behavior which circumvent the attack with high potent. Focusing on security, it also integrates workload balance and low power consumption.

Index terms: cloud computing, co-residential attack, virtual machine allocation, workload balance.

1. INTRODUCTION

Cloud Computing is basically sharing of resources over the internet. While sharing the resources over the internet, it also means customers are exposed to additional risks brought about by the other tenants with whom they share the resources. Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. This paper concentrates on one form of cloud security problem called co-residential attack, where malicious users intend to co-locate their virtual machines (VMs) with target VMs on the same physical server, and then exploit side channels to extract private information from the victim. The basic idea behind virtualization is to use software to simulate the existence of hardware. This powerful idea enables you to run more than one independent computer system on a single physical computer system. While many models of cloud computing exist, the Infrastructure-as-a-Service (IaaS) model used by providers such as Amazon's Elastic Compute Cloud (EC2) service offers a set of virtualized hardware configurations for customers. The sharing of a common physical platform amongst multiple virtual hosts, however, introduces new challenges to security. As we use same running servers for set of VMs, one user can pull out sensitive or confidential information from other legal users.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

2.CLOUD CO-RESIDENTIAL ATTACK:

Co-residential attack is defined as a cloud based virtual machine attack where an attacker targets a set of VMs and tries to co-locate their VM with needed VMs. After coresidence is achieved, the attacker will construct different types of side channels to obtain sensitive information from the victim. An easy way to find whether two machines are on the same physical machine is that, when two machines have same Dom0 IP address then they are co-located. By performing a TCP trace route operation the attacker can obtain the IP address of a VM's Dom0. If two Dom0 IP addresses are the same, the corresponding VMs are co-resident. In order to co-locate with the targets, the attacker can either use a brute-force strategy: start as many VMs as possible (the number may be limited by the cost), or take advantage of the sequential and parallel locality in VM placement.

3. RELATED WORK:

Y. Zhang, A. Juels, M. Reiter, and T. Ristenpart described about "Cross-VM Side Channels and Their Use to Extract Private Keys," [1]. The use of virtualization to isolate a computation from malicious users that co-locate with its growing increasingly pervasive. Demonstrating the side-channel attacks with fidelity sufficient to exfiltrate a cryptographic key from a victim VM can be mounted. It includes pre-empting the victim VM with sufficient frequency to enable fine-grained monitoring of its I-cache activity , filtering out enourmous sources of noise in the I-cache arising from both hardware and software effects and core migration that renders many attackers observations irrelevant to the task of extrct victim keys.

Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Virtual Machine Allocation Policies against Co-resident Attacks in Cloud Computing," [2]. Virtual Machine allocation is done at IAAS level. So chances of co-resident attacks are there. Co-resident attack is a major threat to data privacy in cloud computing. Most VM policy perform the best when the servers are properly configured, and oversubscription is enabled. So we have made some servers and VMs and they are being allocated to the servers using Previously Selected Server First (PSSF) policy now in remaining work one agent is being added so that it can check the access of VMs through the policy Management in which VM allocation permission are defined and according to that it decide whether VMs should be allocated or being discard. So that according to this policy result analysis is made and chances of coresident attack become less and secure services are being provides and performance will be improved.

Zhu Jianrong, Li Jing and Zhuang Yi produced a concept called "Utility-based Virtual Cloud Resource Allocation Model and Algorithm in Cloud Computing ,"[3]. A virtual cloud resource allocation model VCRAM-U (Utility-based Virtual Cloud Resource Allocation Model) is proposed. In this, the problem of virtual cloud resources allocation is abstracted as a utility-maximization problem, taking tradeoffs between the utility of the data center and the performance of the applications into account, and maximizing the utility on the premise of meet user's performance. A local decision algorithm and a global decision algorithm are also designed to solve the problem. In addition, this model can get a higher utility of the data center compared with other models. But, when the size of the cloud computing environment becomes larger and larger, there will be some problems with the model and algorithm such as performance bottlenecks.

Bhrugu Sevak tells about " Security against Side Channel Attack in Cloud Computing,"[4]. Using side-channel attack, it can be very easy to gain secret information from a device so it is good idea to provide security against side channel attack in cloud computing using combination of virtual firewall appliance and randomly encryption decryption (using concept of confusion diffusion) because it provides security against both front end and back end side of cloud computing architecture and also provide RAS (Reliability, Availability, and Security). It implements virtual firewall in cloud server so when adversaries identify targeted VM in cloud infrastructure and then place an instantiate VM to targeted VM, virtual firewall prevent this placement step inside channel attack because of we implement virtual firewall in cloud server. Applies randomly

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

encryption decryption using concept of confusion and diffusion.

4.PROPOSED VM ALLOCATION ALGORITHMS:

Initially Density-based clustering algorithm is used for the virtual machine allocation process without any delay for all VM requests. Then our new VM allocation policy is introduced for the purpose of preventing the VMs from co-residential attack. Also this policy improves workload balance and low power consumption with high security.

4.1 DENSITY-BASED CLUSTERING ALGORITHM:

This algorithm involves partitioning the given data set into specific number groups called Clusters. Each cluster is associated with a centre point called centroid. Each point is assigned to a cluster with the closest centroid. Proposed dynamic VM allocation algorithm using clustering is as: Input: List V of Virtual Machine`s with their location around the globe List D of datacenters.

ALGORITHM:

Step 1: Select N points according to the number of datacenters in D

Step 2: Choose datacenter from D

Step 3: Form N clusters of VM`s from V by assigning closest centroid

Step 4: Recomputed the centroid of each cluster

Step 5: Arrange all the requested VM`s in cluster form

Step 6: Allocate the VM`s to the available Host

Step 7: If all the VM`s are allocated

Step 8: Assign the VM`s cluster to the selected datacenter

Step 9: Endif

Step 10: Repeat [2] until D is empty

Step 11: If all the VM`s are created in the datacenters

Step 12: Send the cloudlets to the created VM`s

Step 13: End

4.2 PREVIOUSLY-SELECTED-SERVERS-FIRST(PSSF) POLICY:

This policy mainly mitigates the co-residential attack by reducing the average number of users per server. In order to minimise the number of users per server, when a user creates new VMs, they will first be allocated to those servers that already host or once hosted VMs started by the same user.

ALGORITHM:

Step 1: PSSList={},NPSSList={}

Step 2: foreach server si in S

Step 3: if (si has enough remaining resources)

Step 4: if(si already hosts or once hosted u's VMs)

Step 5: if(si hosts less than N* of u's VMs)

Step 6: PSSList.add(si)

Step 7: else

Step 8: NPSSList.add(si)

Step 9: if(!PSSList.isEmpty())

Step 10: returen PSSList.get(random(PSSList.size())) else

Step 11: Sort(NPSSList,group index,resources left)

Step 12: Sort(NPssList,group index,resources left)

Step 13: i=the number of servers with the same group index and remaining resources as the first server in NPSSList(NPSSList.get(0))

Step 14: Mark NPSSList.get(random(i)) as "previously selected" for u,and return it.

1. Security− PSSF algorithm provides security against co-residential attack by reducing the average number of users for each server. It mitigates the attack completely by avoiding the co-location of two different users.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

2. Workload balance– In the following three circumstances, the new VMs will not be allocated to previously selected servers: (1) every previously selected server already hosts N*VMs of single user, (2) none of the previously selected servers has adequate resources left, and (3) the user has never created any account and started VMs before. In these three cases, PSSF will spread the workload.

3. Power consumption–The most straightforward way to minimize the number of running servers is stacking, or in other words, allocating new VMs to the same server until there is not enough remaining resources. However, this concept does not satisfy workload balance. So we propose a compromised solution that, divide all servers into particular groups; within each group, the load is spread; the next group of servers will not be started until servers in all groups are filled.

5. SYSTEM DESIGN:

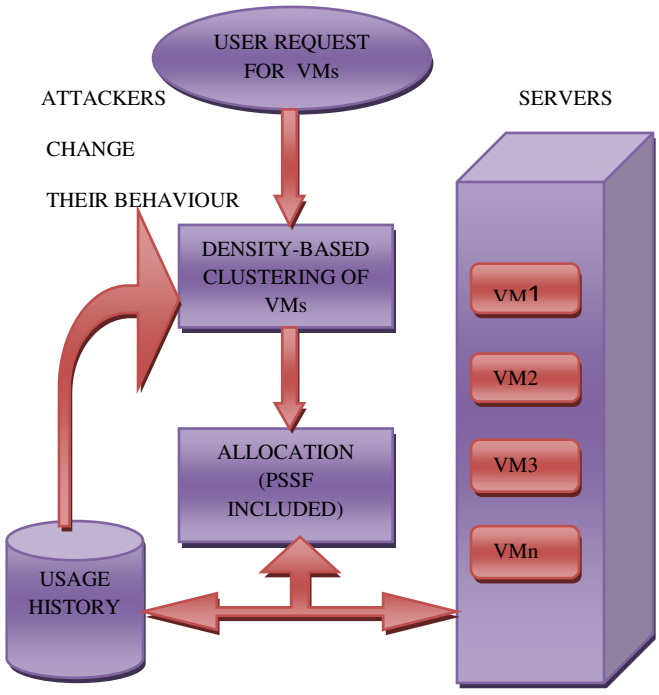

Fig 5.1 Architecture Diagram

The user requests for a VM and the density-based clustering algorithm separates the VM based on their nature. By using PSSF policy the cloud service provider allocates VMs for the users to mitigate against co-residential attack.

6.IMPLEMENTATION ON OPENSTACK:

Openstack is a well known cloud computing open source platform for creating our own private cloud. The proposed algorithms are implemented on the openstack for obtaining the required results. Our new VM allocation policy called PSSF satisfies the objectives in security, workload balance and power consumption. In terms of mitigating co-residential attacks, PSSF limits the number of servers that single user can use, and hence increases the co-residence of VMs belonging to the same user. As a result, the victims cannot be found by the attackers, and it is also harder for attackers. Moreover, this technique is effective in decreasing the probability of attackers achieving co-residence. As for the workload balance, if PSSF does not find any legal server that was selected previously, it assigns the new VM to a lightly loaded server. Finally, in order to bring down the power consumption, PSSF handles the servers in groups, and a new group of servers will not be used until all existing ones are fully used, which proved to be effective in decreasing the number of servers being used.

6. CONCLUSION:

The new VM allocation policy PSSF meets the objectives in security, workload balance and power consumption. In terms of defending against co-resident attacks, PSSF limits the number of servers that one user can use, and hence increases the co-location of VMs be- longing to the same user. As a result, the victims are less exposed to attackers, and it is also harder for attackers to spread their VMs.Hence the legal users can use their VMs without attackers interruption.

7. REFERENCE:

1)Y. Zhang, A. Juels, M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. 19th ACM Conference on Computer and Communications Security (CCS 2012), pp. 305-316, 2012.

2) Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Virtual Machine Allocation Policies against Co-resident Attacks in Cloud Computing," Proc. IEEE International Conference on Communications (ICC 2014), pp. 786-792, 2014.

3) Zhu Jianrong, Li Jing and Zhuang Yi "Utility-based Virtual Cloud Resource Allocation Model and Algorithm in Cloud Computing" International Journal of Grid Distribution Computing Vol.8, No.2 (2015), pp.177-190

4) Bhrugu Sevak "Security against Side Channel Attack in Cloud Computing" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012.

5) A. Hameed, A. Khoshkbarforoushha, R. Ranjan, P. Jayaraman, J. Kolodziej, P. Balaji, S. Zeadally, Q. Malluhi, N. Tziritas, A. Vishnu, S. Khan, and A. Zomaya, "A Survey and Taxonomy on Energy Efficient Resource Allocation Techniques for Cloud Computing Systems," Computing, pp. 1-24, 2014.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016