International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Hybrid SWIPER: Synchronization of IP and MAC address to overcome third party attacks in cloud

Mr B.Guruprasath[1], J.Santhiya[2], S.Vigneshwaran[3]
[1] Professor, [2]Assistant Professor, [3]Student B.Tech
Department of IT, A.V.C College of Engineering Mayiladuthurai

Abstract In a third-party Cloud model, provider delivers the cloud service over the Internet. Public cloud services are sold on-demand, typically by the minute or the hour. Customers only pay for the CPU cycles, storage or bandwidth they consume. In cloud, several Virtual machines share the same I/O resources. Here some clouds intentionally slow down the processes of their foe application by using Swiper, which leads to a security threat. Because of this threat, if a user needs to retrieve a file, it may lead to data threats. To overcome this issue, we implement a framework for reducing time delays with low cost. For this, if an exploitation occurring in a physical machine is identified, the virtual machine which is exploiting is paused for some period of time. In mean time, the victim application can complete its process. After this, the adversary machine is unpaused. By using this technique, the retrieval of a file can be done in a secure manner.
Keywords— Cloud, threat, Swiper

I. INTRODUCTION

The cloud computing can be set of hardware, networks, storage, services, and interfaces that merge to deliver aspects of computing as a Service. Cloud services encompass the release of software, infrastructure, and storage over the Internet.

A virtual machine (VM) is an emulation of a particular computer system. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer and their implementations may involve specialized hardware, software, or a combination of both. Once a VM instance is created, you can stop, restart, or delete it as needed. In the CloudStack UI, click Instances, select the VM, and use the Stop, Start, Reboot, and Destroy buttons.In computer security a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either "intentional" (i.e. hacking: an individual cracker or a criminal organization) or "accidental" (e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

Denial of service, a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive. The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both). Denial of service poses the same threat as an infinite delay. Availability mechanisms counter this threat.

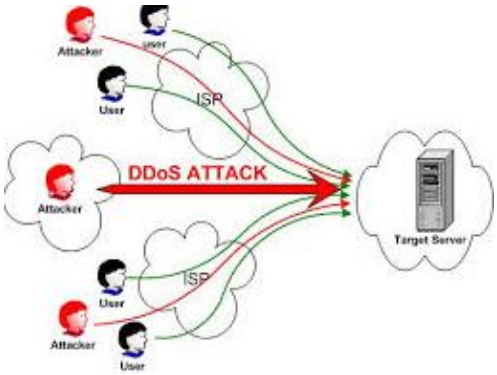

Figure 1 DDos attack

Swiper, a framework that exploits the virtual I/O vulnerability
in three phases: 1) co-location (“sneaking-up2) synchronization (“getting-ready”): and 3) exploiting (“swiping”).

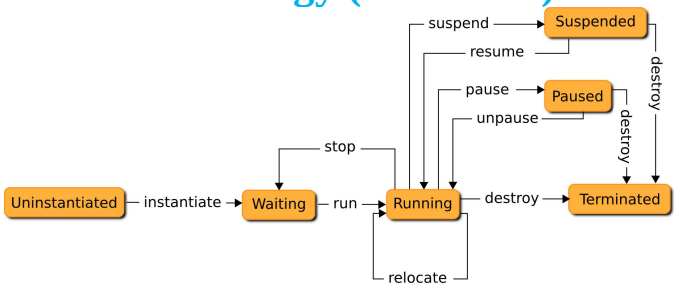

Figure 2 Virtual machine lifecycle

II. LITERATURE SURVEY

Venkat varadharajan[1] "resource freeing attacks improve your cloud performance(at your neighbor expense)",ccs,2012,pp.281–292 proposes contention measurement technique but the disadvantages of this paper is loose overall efficiency because of the load caused by the extraneous and there is no performance isolation in cloud environments

S. K. Barker et a l[2]., "empirical evaluation of latency-sensitive application performance in the cloud," in proceedings of the first annual acm sigmm conference on multimedia systems. Acm, 2010, pp. 35–46 proposes the stream jitter approach but in this paper difficult to provide resource control mechanisms and can't easily configure and manage the risks of performance interference

K. Ye et al.[3], "Virtual machine based energy-efficient data center architecture for cloud computing: a performance perspective**,**" in Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing. IEEE Computer Society, 2010, pp. 171–178 proposed the VM-BASED ENERGY-EFFICIENT DATA CENTER framework

In this project there is no live migration mechanism and the data center can maintain energy efficiency manually

J. Szefer et al.[4], "Eliminating the hypervisor attack surface for a more secure cloud," in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 401–412 proposed No Hype framework and the demerits of this paper is major modifications to the guest OS to perform all system discovery during boot up

G. Wang et al[5]., "The impact of virtualization on network performance of amazon ec2 data cente**r,**" in INFOCOM. IEEE, 2010, pp. 1–9 proposes the spatial experimental approach the problem of this paper is Unstable to provide TCP/UDP throughput and difficult to analyze characteristics of virtualized data centers

III. IMPLEMENTATION

In the existing system markov decision process (mdp) formalization to analyze the attacks in vm resource sharing. Overcome two party attacks with limited number of authentication. Vm monitor and schedulers implemented with synchronization phases

In the proposed system, we implement swiper framework that contains three phases such as co-location, synchronization and swiping

A. Co-location ("sneaking-up"): place the adversary VM on the same physical machine as the victim VM;

B. Synchronization ("getting-ready"): identify whether the targeted application is running on the victim VM and, if so, the state of execution for the targeted application (which we shall elaborate below); and

C. Exploiting ("swiping"): design an adversarial workload

According to the state of the victim application, and launch the workload to delay the victim

In our paper, User will give the request to the admission controller. Admission controller will check the IP address of requested user system whether their IP address is authenticated or not. Smart booking scheduler will allocate the resources if the enough requested resources are there in cloud otherwise it will go for co located and VM migration method to allocate the resources to the user

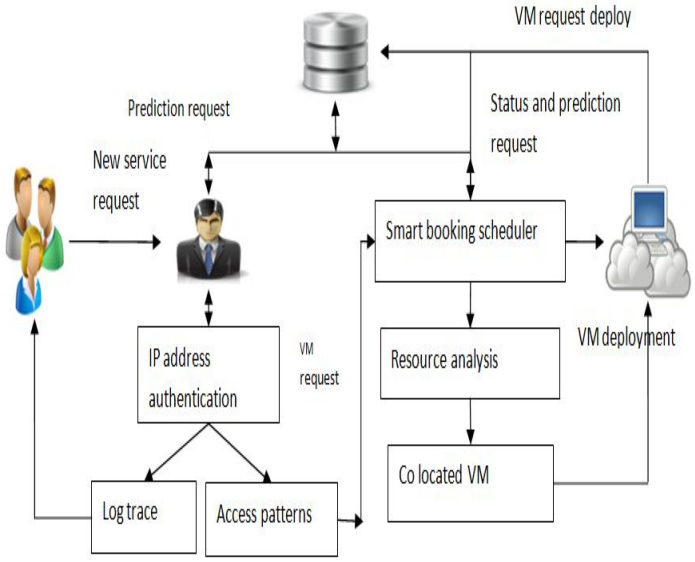

Figure 3 System Architecture

The modules in our paper are described below:

IV. CLOUD RESOURCE FRAMEWORK

Resource Allocation (RA) is the process of assigning available resources to the needed cloud applications over the internet.
The cloud service provider is responsible for maintaining
Cloud provider activities include utilizing and allocating scarce resources. The order and time of allocation of resources are also an input for an optimal resource allocation

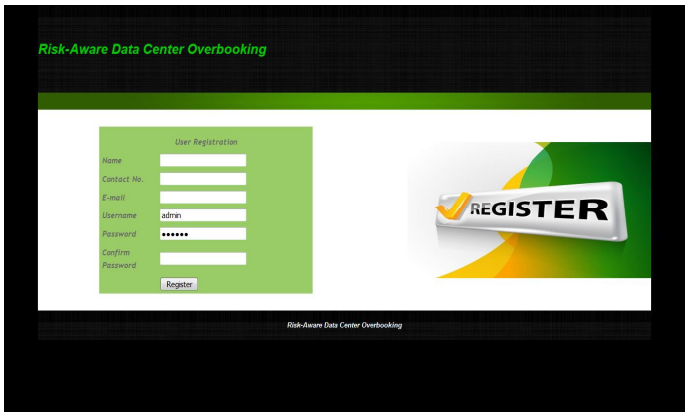

Figure 4 User registration

A. *Demand Analysis*

VM selection policy (algorithm) has to be applied to carry out the selection process. Finding a new placement of the VMs selected for migration
Admission controller analyzes the demands for user requests. When a physical server is considered to be overloaded, it requires live migration of one or more VMs from the physical server under consideration. Selection of VMs should be from the overload and physical servers and finding the best physical. The process of high memory demand is allocated in high free memory VM and other process is allocated in another VM

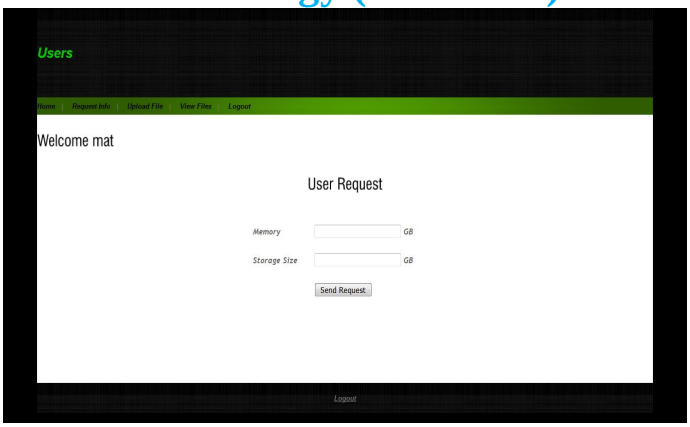

Figure 5 User request for resources

B. Co Located VM

Admission controller makes decision, whether to accept it or not. If the service is accepted, request is sent to overbooking scheduler to analyze horizontal elasticity in virtual machines.

If service is rejected, request is sent to risk assessment controller to analyze capacity of VM. This mechanism provides inter cloud live migration offing new ways to exploit the inherent dynamic nature of distributed clouds.

Figure 6 User request information

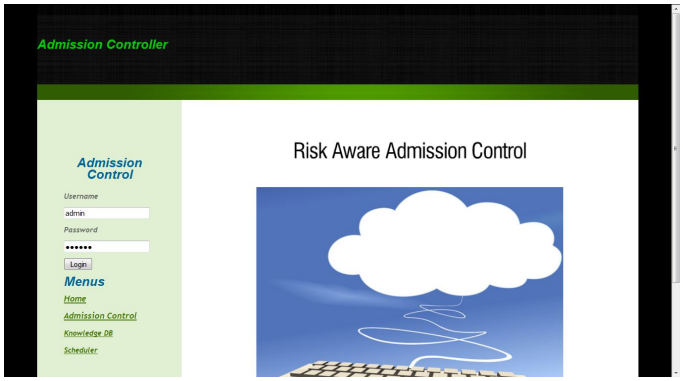

Figure 7 Administration controller login

C. Decision Making

Transitions among schedulable entities executing in a computer system are tracked in computer hardware or in a virtual machine monitor .The virtual machine monitor derives scheduling information from the transitions to enable a virtual machine system to guarantee adequate scheduling quality of service to real-time applications executing in virtual machines that contain both real-time and non-real-time applications.

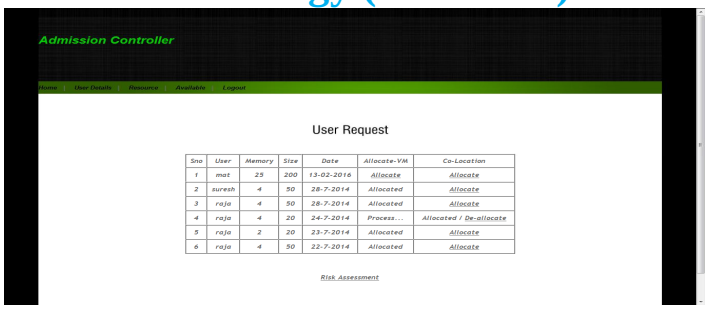

Figure 8 Administration controller allocations

D. Preventing Work Load Attack

If a Virtual machine attacks its controversial application, it goes to its co-location and sends multiple requests to the cloud, which degrades the speed of the application. To prevent this, the Virtual machine which is sending multiple requests in a particular period of time is identified; it is paused for some time. And analyze work is done for finding out the reason behind that vulnerability. After analyzing the Virtual machine, it is unpaused, to carry out its tasks.

Domain can be paused in virsh:

virsh suspend <domain>

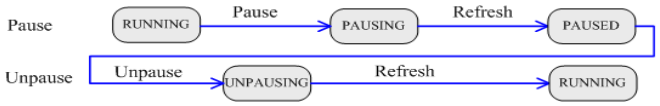

Figure 9 Virtual machine paused and unpaused state

The other way for this is, in Virtual Machine Manager by clicking *Pause* button from main toolbar. When a guest is in a suspended state, it consumes system RAM but not processor resources. Disk and network I/O does not occur while the guest is suspended. This operation is immediate.

Any paused or suspended domain can be resumed by:

virsh resume <domain>

The other way is, by unclicking the appropriate *Pause* button in Virtual Manager.

V. CONCLUSION

Cloud computing is a model for enabling 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 virtual machine in the cloud attacks its foe application, by continually sending requests to the cloud, which leads to slow down of the opponent application. Also this is a security issue in the cloud, while we transfer files in through Internet. To overcome these issues, we implemented a technique to avoid this attack by using the method of storing the data using our system IP and MAC address and the VM migration and co allocation method. Also the Virtual machine is suspended if it becomes a threat to a vulnerable machine. The future work includes, analyzing the amount of vulnerability and threat in the cloud and secure the virtual machine.

REFERENCES

[1] Venkat varadharajan[1] “Resource freeing attacks improve your cloud performance(at your neighbor expense)”,CCS,2012,pp.281–292

[2] S. K. Barker et a l[2]., “Empirical evaluation of latency-sensitive application performance in the cloud,” in Proceedings of the first annual ACM SIGMM conference on Multimedia systems. ACM, 2010, pp. 35–46

[3] K. Ye et al.[3], “Virtual machine based energy-efficient data center architecture for cloud computing: a performance perspective**,**” in Proceedings of the 2010 IEEE/ACM Int’l Conference on Green Computing and Communications & Int’l Conference on Cyber, Physical and Social Computing. IEEE Computer Society, 2010, pp. 171–178

[4] J. Szefer et al.[4], “Eliminating the hypervisor attack surface for a more secure cloud,” in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 401–412

[5] G. Wang et al[5]., “The impact of virtualization on network performance of amazon ec2 data cente**r,**” in INFOCOM. IEEE, 2010, pp. 1–9