Chapter 26
A Secured Real Time Scheduling Model for Cloud Hypervisor

Rekha Kashyap
Inderprastha Engineering College, India

Deo Prakash Vidyarthi
Jawaharlal Nehru University, India

ABSTRACT

Virtualization is critical to cloud computing and is possible through hypervisors, which maps the Virtual machines((VMs) to physical resources but poses security concerns as users relinquish physical possession of their computation and data. Good amount of research is initiated for resource provisioning on hypervisors, still many issues need to be addressed for security demanding and real time VMs. First work SRT-CreditScheduler (Secured and Real-time), maximizes the success rate by dynamically prioritizing the urgency and the workload of VMs but ensures highest security for all. Another work, SA-RT-CreditScheduler (Security-aware and Real-time) is a dual objective scheduler, which maximizes the success rate of VMs in best possible security range as specified by the VM owner. Though the algorithms can be used by any hypervisor, for the current work they have been implemented on Xen hypervisor. Their effectiveness is validated by comparing it with Xen's, Credit and SEDF scheduler, for security demanding tasks with stringent deadline constraints.

1. INTRODUCTION

Cloud Computing is a paradigm shift which offers virtualized resources in the form of services. "A Cloud is a type of parallel and distributed system consisting of collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" (Buyya, Yeo, & Venugopal, 2008). Vision of cloud is possible by virtualization technologies which provide a mechanism for mapping VMs to physical resources. It is done by the virtualization management layer, termed as hypervisor which guarantees the isolation between different virtual machines and manages virtualization of physical resources (Chisnall, 2008; Liao, Guo, Bhuyan, & King, 2008;

DOI: 10.4018/978-1-5225-8176-5.ch026

Armbrust, 2009). This mapping is largely hidden from the cloud users. Users of Amazon EC2 (2014) would never know the actual location of their physical resources or their application's execution. As this hypervisor system sits between the guest and the hardware, it can control the guest's use of CPU, memory, and storage, even allowing a guest OS to migrate from one machine to another.

Like a real machine, a VM can run any application, OS or kernel without modifications. Examples of such hypervisors are Xen (Barham et al., 2003), VMware (2007), and KVM (Kivity, Kamay, Laor, Lublin, & Liguori, 2007).

By virtualization resources are decoupled from the users and it provides greater flexibility in terms of resource allocation but at the same time it brings new challenges for provisioning, optimal design and runtime management of systems. The resource allocation problem becomes challenging when the resource needs of Virtual Machines are heterogeneous because of diversity in the applications they run and vary with time as the workloads grow and shrink (Menon, Santos, Turner, Janakiraman, & Zwaenepoel, 2005). Recently, lot of demand for supporting real time systems in virtualized environment has been witnessed. Virtualization adds a layer of technology, which definitely increases the management of security by necessitating additional security controls. Also, combining many systems into a single physical computer can cause a larger impact on security compromise. Cloud Computing preserves vulnerabilities associated with internet applications and additionally that arise from pooled, virtualized and outsourced resources (Buyya, Yeo, Venugopal et al., 2009; Dahbur, Bassil Mohammad et al., 2011). Security is very essential for cloud users as they relinquish physical possession of their computation and data. Plenty of research has been initiated in resource provisioning for hypervisors, still many problems especially for security-aware and real time tasks running on virtual machines needs more attention. Using existing security services to satisfy the applications' security needs, however, incurs security overhead in terms of computation time, which may violate the application's deadlines. The conflicting requirement of optimal real-time performance and a quality security protection imposed by security-critical real time applications introduces a new challenge for resource allocation schemes.

The first work, introduced in this paper SRT-CreditScheduler, is preferred for Real-time VMs where the VM cannot compromise on security but at the same time is not able to specify the exact security requirements. This algorithm ensures highest level of security. The second proposed SA-RT-CreditScheduler is for Real time VMs where the owners specify their range of security requirements to achieve better success rate. The algorithm tries to offer highest security from the range and compromises only when the deadline violates. Both the works are inspired by Smith's and Moore's work where preference is given to smaller processing times and approaching deadlines but proposed work differs, as in them the weightage of preference varies depending on the characteristics of Virtual Machines to be scheduled. The contribution in this work is as follows. The next section discusses the work done in this area. Section 3 depicts the terminologies and strategies used for the proposed work. Section 4 details the proposed SRT-CreditScheduler and SA-RT-CreditScheduler. Section 5 describes the experimentation results and observations and section 6 concludes the work.

2. RELATED WORK

The proposed works have been implemented on Xen hypervisor or Virtual machine monitor. Xen was developed by Barham et al., in 2003 and since then has become one of the most popular hypervisor. It is an type-1 opensource or bare metal Virtual machine monitor. It is possible to run many instances