International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Email: editor@ijarets.org Volume-7, Issue-3 March- 2020 www.ijarets.org

PERFORMANCE ANALYSIS OF SELECTED HYPERVISORS WITH VIRTURAL MACHINE MONITOR

Anshu Mali Bhushan,
Research Scholar, Dept of Physics,
Himalayan Garhwal University

Dr. Rahul Solanki,
Associate Professor, Dept of Physics,
Himalayan Garhwal University

ABSTRACT
Cloud computing is a network-based system where computations and resources are shared. Cloud computing is actually described as a collection of virtualized computer resources. Virtualization technologies paired with self-service capabilities are commonly used by Cloud providers for computing resources via network infrastructures, particularly the Internet, and several virtual machines are hosted on the same physical server. The cloud computing paradigm, which is based on virtualization, allows workloads to be easily deployed and scaled-out by rapidly provisioning Virtual Machines or real machines. A cloud computing platform can offer redundant, self-recovering, and highly scalable programming paradigms, which enable workloads to recover from a variety of hardware and software faults.
Key words: Cloud computing, network infrastructures, physical server

INTRODUCTION

Virtualization is a new technology that allows you to make the most of your computing resources. Traditionally, the computing society has used dual boot, live boot, or virtualization technologies to run two operating systems on a single computer. The physical machine is loaded with more than two operating systems in the dual boot method. The dual operating system is solely installed in the physical machine's environment. The operating system is loaded directly into the primary memory of the physical computer. The operating system is given independent access to the hardware resources. Each operating system's assigned resource is separated from the real machine. Installing the dual operating system on a single workstation does not require any third-party software. When the system is booted at a given point in time, only one operating system is active, which implies the operating system has access to all hardware resources. If the user wants to load another operating system, the physical computer must be forced to reboot/restart in order for the boot menu to choose the preferred operating system. If one of the operating systems fails, the entire physical machine can be affected.

The current version of the International Standard Organization – Operating System (ISO-OS) image file is acquired from approved sources and then written to a CD/DVD device or a USB flash drive in the live boot technique. This booting procedure is completely stress-free.

By selecting the "try out" choices, the operating system is loaded from a USB device or CD/DVD device, which uses the entire primary memory of the physical machine without any alterations to the hard disc of the actual machine. This method is highly useful for testing Linux distributions and hardware.

The virtualization environment can only offer the installation of dual operating systems when using the virtualization method. Third-party software such as QEMU (Quick Emulator), KVM (Kernel-based Virtual Machine), Xen, VMware, Virtual Box, and others construct the virtualization environment. The host OS is the principal Operating System (OS) of the single physical system, whereas the guest OS is the secondary Operating System. The host OS has the ability to allocate hardware resources to the guest OS. The resources of the guest OS are separated from those of the host OS. The real computer will not be harmed if the guest OS fails to execute.

The entire physical system, however, will be affected if the host OS fails to execute. This technology allows two operating systems to run in parallel at the same time. To run the two Operating Systems simultaneously, the actual system does not need to be rebooted or restarted.

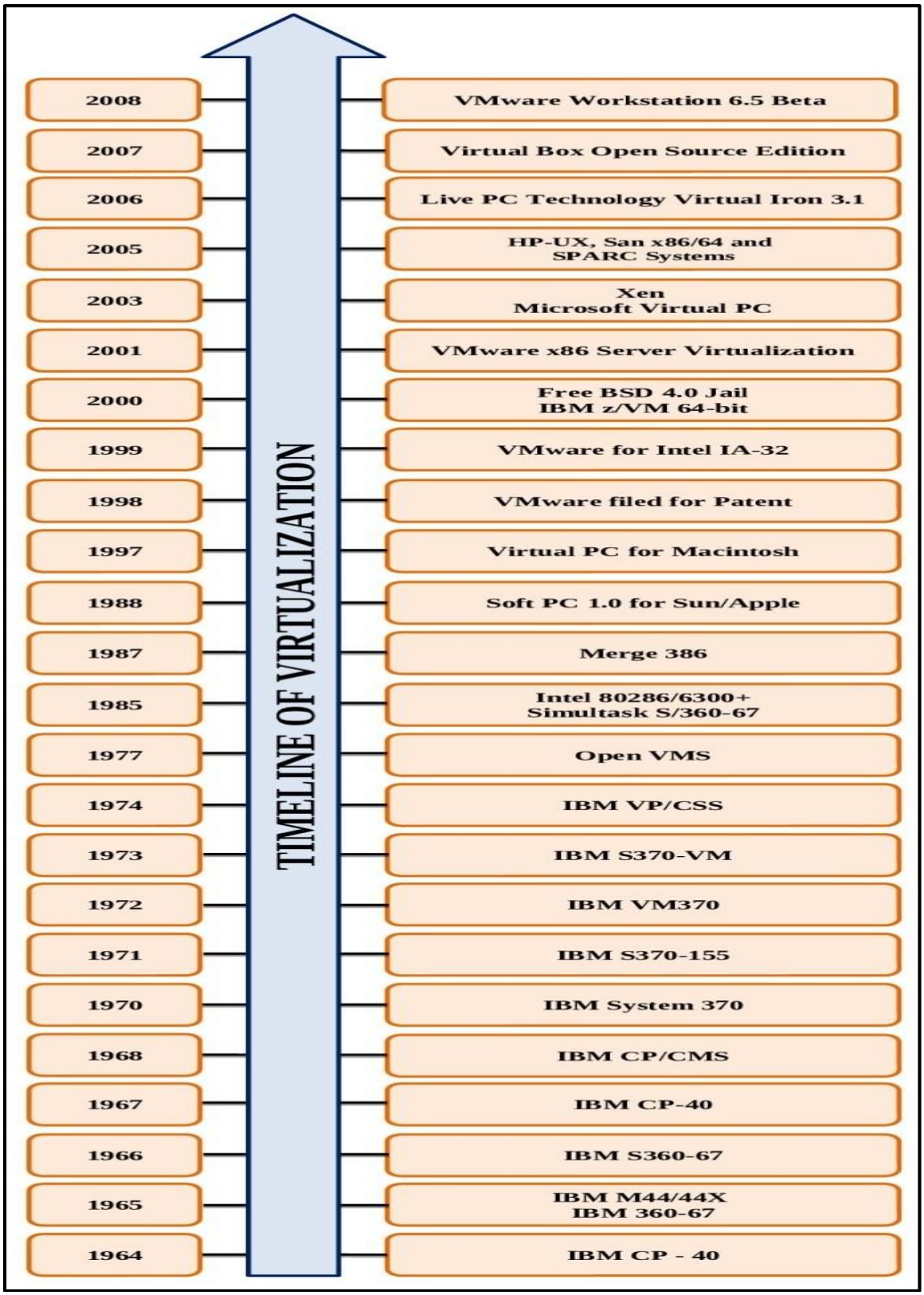

Figure-1 . Timeline of virtualization

Robert P. Goldberg pioneered virtualization in the 1960s, based on a trial system called the IBM M44/44X, which is also known as a virtual machine or pseudo machine. The virtualization technology renaissance is depicted in Figure 1.

Virtualization technology divides a physical computer into more than one independent computer. By partitioning a physical machine using multiple approaches, this virtualization technology supports diverse operating systems. Simultaneous operating environments are deployed over the same physical computer to improve the efficiency of physical computers by enabling virtualization. Isolation, hardware independence, encapsulation, performance and equivalence, control, and compatibility are all criteria that must be established automatically when constructing avirtual machine.

The virtualizable processor isolates the VM, allowing any instruction to be modified or the complicated machine to be tested in any way. Only the highest privileged mode has the ability to perform this isolation process. There are two types of instruction sets: privileged and non-privileged. The machine has two modes of operation: user and kernel/supervisor. A privileged instruction is one that can only be executed by the kernel, whereas a non-privileged instruction can be executed by the user or any programme. In an Operating System (OS), the kernel mode allows the execution of both privileged and non-privileged instructions; however, the user mode can only execute non-privileged instructions, and when a privileged instruction is run in this mode, an interrupt occurs. Interrupt Service Routine will handle this interrupt (ISR). The hypervisor is in charge of accessing hardware resources. The hypervisor runs in supervisor mode, while the guest Operating Systems run in user mode. The hypervisor, which is executed by the Operating System, interprets any privileged instructions.

The Operating System controls access to hardware resources in non-virtualized systems. Non-privileged instructions are only executed in user mode, while privileged instructions are only executed in supervisor mode. Although the Operating System runs in supervisor mode, the programmes run in user mode.

HYPERVISOR OR VIRTUAL MACHINE MONITOR

A virtual machine that is handled by software is referred to as emulated hardware. A virtual machine monitor (VMM) or hypervisor is what it's called. The VMM monitors the development and execution of virtual machines. A single physical machine is divided into a large number of virtual machines, each of which is run by a different operating system. The hypervisor can handle this process. The VMM software layer allows you to run several virtual machines on a single physical computer. The hypervisor is responsible for managing the host processor and resources, allocating memory to VMs, and ensuring that VMs do not interfere with one another. A host OS is the physical machine's primary/major operating system that allows it to handle several virtual operating systems. This host OS makes use of the physical machine's resources and distributes them to virtual OSs as required. A guest OS is a secondary/minor operating system that operates in a virtual environment without the need of dedicated hardware resources.

Hypervisors such as VMware ESXi Server, Hyper-V, Citrix, KVM, OpenVZ, VirtualBox, and Proxmox VE are being used by researchers, trainers, teachers, students, and IT organisations. The following are the characteristics of these hypervisors:

- ESXi Server is a Type-1 and enterprise-class hypervisor that is used to deploy and serve virtual machines. VMware is the company that created it. Elastic Sky X with integration is ESXi's expansion. The ESXi is installed directly on a bare-metal physical server that is in charge of all primary resources. This is inextricably linked to the kernel of an operating system. The most significant advantages of ESXi include efficient hardware partitions, lower upfront expenses, and a higher virtual machine consolidation ratio.
- Microsoft's Hyper-V is a hardware virtualization technology. The hyper-V programme replicates a virtual machine, which is a physical machine. Each VM operates as if it were a machine with an operating system.

The VMs are all one-of-a-kind and identical. This sort of virtualization is particularly useful for transferring VMs to other persons, groups, and systems if any problems arise during workloads.

- Citrix Xen Hypervisor is a virtualization platform that allows you to consolidate and manage a variety of workloads, including applications, network and storage settings, operating systems, scalability, and performance of desktop virtualization. The main benefits of this hypervisor are introspection for zero vulnerability, live patching for reduced operational overhead and downtime, support for all types of GPUs, ease of troubleshooting, and long-term service support/release.
- Kernel-based Virtual Machine (KVM) is an open source hypervisor that manages both Linux and Windows guest operating systems. It provides a solution for Intel VT or AMD-x86 V's hardware extension. It includes loadable kernel components for processors and infrastructure, such as kvm-intel.ko and kvm-amd.ko. KVM is made up of two parts: kernel space and user space, which are Linux-2.6.20 and QEMU-1.3, respectively.
- Virtual Box is a desktop virtualization software that supports x86 and intel-64/AMD-64 bit processors and works as guests and hosts on Linux, Windows, Mac OS X, and Solaris. It's the GNU General Public License (GPL) version of open source software that's publicly available. VirtualBox was established by a German startup that was later acquired by Sun Microsystems. Oracle continues to distribute VirtualBox software after acquiring it from Sun. Additional capabilities such as remote desktop protocol (RDP) and USB compatibility are offered in the closed source version as a "extension pack."
- Proxmox VE (Virtual Environment) is an open source virtualization platform that tightly integrates Linux Containers (LXC) and KVM hypervisors. Virtual machines and web-based interfaces are controlled via KVM and LXC, respectively. It is compatible with both Windows and Linux systems. The Proxmox VE is designed for data centres to manage a variety of tasks, including networking functionality, software-defined storage allocation, disaster recovery tools, and high availability between servers.
- OpenVZ is an open source container-based virtualization software that was originally created for the Linux operating system but has since been extended to include support for Apple OS X and Windows. This container provides virtual private servers as separated hosts and ensures that performance is near to native. Parallels Virtuozzo containers are supplied by Parallels, a Swiss company, and OpenVZ provides a commercial solution for them.

HYPERVISOR CLASSIFICATION

In general, hypervisors are divided into two categories:

- Hypervisor of Type 1
- Hypervisor Type-2

Hypervisor of Type 1

This hypervisor is also known as bare-metal architecture or native hypervisor because it is installed and run directly on top of bare-metal physical machines. On top of this layer, it constructs a slew of virtual computers.

The virtual machine is created using bare metal hardware resources, as are other resource allocations. The resources are divided across the virtual machines that this hypervisor manages. This hypervisor directly accesses the hardware resources, hence the server does not require a base Operating System. The hardware contribution, on the other hand, is minimal. This hypervisor is more scalable, robust, and has higher performance. Figure-2 depicts the Type-1 hypervisor's design, which can be used in a variety of hypervisors including IBM CP/CMS, IBM-SIMMON, Xen Server, Oracle SPARC VM Server and Oracle x86 VM Server, Microsoft Hyper-V, KVM, and VMware ESX/ESXi. Monolithic hypervisors and Microkernelized hypervisors are two subtypes of Type-1 hypervisor.

Monolithic Hypervisor

Monolithic hypervisors must access components that are united as a single entity, such as application programme interfaces, hardware device drivers, I/O stack, kernel, storage, network, input device, and virtualization layer. The hypervisor requires hardware drivers since they are shared by the guest and host operating systems. The

hypervisor necessitates the use of a custom driver. To gain access to the monolithic hypervisor, all hardware resources are shared. It is entirely present in security ring 0. The Monolithic hypervisor's architecture is depicted in a layered fashion in Figure-2. VMware ESXi Server is an example.

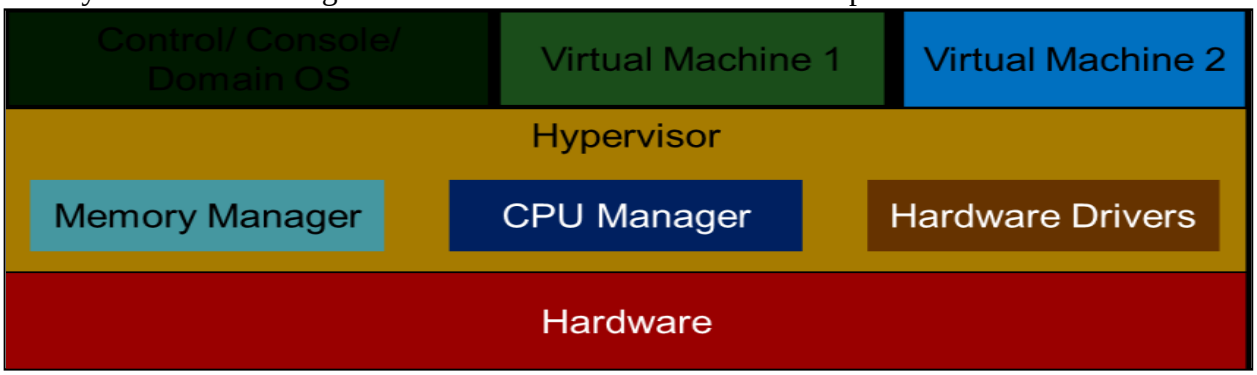

Figure-2 : Type-1 Hypervisor

Figure shows VMware's x86-based Type-1 hypervisor enabling servers to host machines, which was released in 1990. Storage Motion, Fault Tolerance, Site Recovery Manager, Storage and Network I/O Control, and Distributed Resource Scheduler are among the product's features. The Storage VMotion feature allows you to move data files that aid in the creation of virtual machines.

HYPERVISOR TYPE 2

Type-2 hypervisor software, also known as Hosted Hypervisor/VMM, is software that runs on a physical machine in a primary/host Operating System environment.

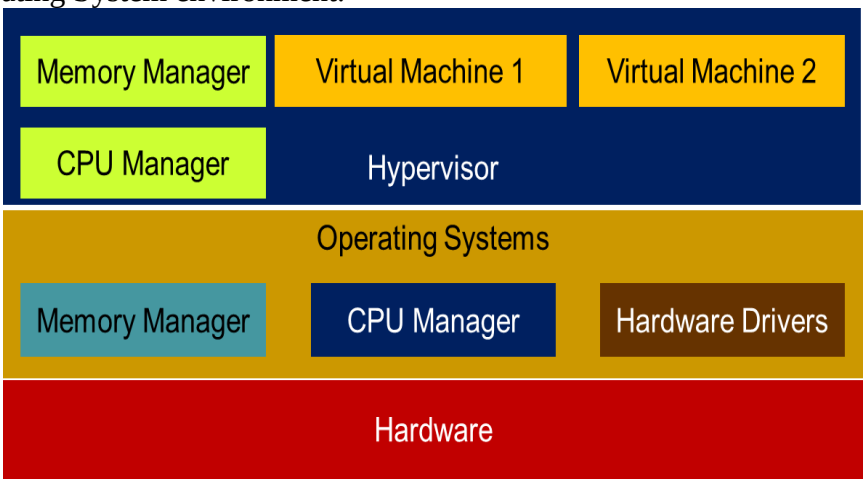

Figure-3 : Type-2 Hypervisor

The Type-2 hypervisor runs a guest Operating System on top of the host Operating System and manages it. The guest VMs are supported by this hypervisor, which manages hypercalls for memory, CPU, network, storage, and other resources through the host Operating System. For the end user, the Type-2 hypervisor is the simplest approach to operate a virtual machine on any computer. Figure-3 shows the architecture of a Type-2 hypervisor, which is found in Oracle Virtual Box, BHyVe, Oracle VM for x86, Solaris Zones, VMware Fusion, VMware Workstation, and Parallels.

HYPERVISORS AND VIRTUALIZATION

Virtualization is a significant feature that allows users to access infrastructure and resources as isolated virtual machines (VMs) (Hassan Takabi et al 2010). A hypervisor, also known as a Virtual Machine Monitor, is a piece of platform-virtualization software that allows different operating systems to run in parallel on a single host machine. While this encourages the creation of virtualized resources for sharing, it also expands the attack surface. As a result, a mechanism to maintain strong VM isolation, arbitrated sharing, and secure communications between

VMs is required. This can be done with the help of a flexible access control and monitoring system that manages the management and sharing capabilities of VMs within a cloud host (Yanpei Chen et al 2010)

CONCLUSION

Advanced study in this subject could lead to the development of a new programme to assess vulnerabilities proactively, which would check network services for vulnerabilities before they were attacked, as well as remedy the worst side effects. For upgrading the mDesk hypervisor, mechanisms like as snapshot, copy, migrate, clone, import, and export could be implemented. These techniques are described further because they can be considered add-on features of this hypervisor. A snapshot mechanism is a copy of the present state of running virtual machines that can be restored to the precise condition when the user wants it. The process of reproducing the desired/existing VM is known as a copy mechanism. A migration mechanism is a method of moving a virtual machine from one location to another, either offline or online. A cloning mechanism is a method of copying an existing virtual machine (VM) and all of its associated disc images. The way of moving an external VM into the mDesk hypervisor is known as an import mechanism. An export mechanism is a means for moving a VM from the mDesk hypervisor to another hypervisor outside of the mDesk hypervisor. Furthermore, a new technical application might be developed to identify and improve the security of virtual machines. It is possible to establish a portable virtual machine that runs the appropriate OS from a portable / pocket hard disc and can be simply operated by connecting the hard disc into any computer using the plug and play method. Finally, this hypervisor might be used to upgrade mobile phones so that they can run two operating systems at the same time while remaining entirely secure.

REFERENCES

- Ada Gavrilovska *et al*, 2020, 'High-Performance Hypervisor Architectures: Virtualizationin HPC Systems', HPC Virt'07 March 20, Lisbon, Portugal.
- Antonino Vaccaro, Francisco Veloso, and Stefano Brusonic, 2020, 'The impact of virtual technologies on knowledge-based processes: An empirical Study', Research Policy, Elsevier.Vol.38, pp.1278–1287
- Bela Shrimali, Hiren B. Patel, 2020, 'Comparative Study for Selection Open Source Hypervisors and Cloud Architectures under Variant Requirements', Indian Journal of Computer Science and Engineering (IJCSE), Vol.7 No.2, pp. 28-45.
- Chunquan Li, Chunyung Hu, Yanwei Wang, 2019, 'Research of Resource Virtualization Technology based on Cloud Manufacturing', Advanced Materials Research Vols. 201-203 (2011) pp.681-684.
- Daniel Baldin and Timo Kerstan Proteus, 2019, 'A Hybrid Virtualization Platform for Embedded Systems', International Federation for Information Processing.pp.185-194
- François Armand, Michel Gien, 2019, 'A Practical Look at Micro-Kernels and Virtual Machine Monitors', IEEE, pp.1-7
- Goldberg, R., 1918, 'Survey of Virtual Machine Research', IEEE ComputerSociety.pp.34-45.
- Goran Martinovic, *et al,* 2018, 'Impact of the Host Operating Systems on Virtual Machine Performance' IEEE Computer Society
- Megumi Ito and Shuichi Oikawa, 2018, 'Meso virtualization: Light weight Virtualization Technique for Embedded Systems', International Federation for Information Processing, pp.496–505
- Ming Zhao, Jian Zhang and Renato J. Figueiredo, 2017, 'Distributed File System Virtualization Techniques Supporting On-Demand Virtual Machine Environments for Grid Computing', The Journal of Cluster Computing 9, 45–56,Springer.
- Pradeep Padala, Xiaoyun Zhu, Zhikui Wang, Sharad Singhal, Kang G. Shin, 2008, 'Performance Evaluation of Virtualization Technologies for Server Consolidation', IEEE, pp. 1-13.
- RajaWasim Ahmad, Abdullah Gani, Siti Hafizah Ab, Hamid, Muhammad Shiraz, Feng Xia, Sajjad A, Madani, 2017, 'Virtual machine migration in cloud data centers: a review, taxonomy, and open research issues', Journal of Supercomputing, Springer Science, Business Media, Vol.71 pp. 2473–2515

- Sugumar T. N. and N. Rajam Ramasamy, 2016, 'mDesk: a scalable and reliable hypervisor framework for effective provisioning of resource and down time reduction', The Journal of Super Computing, Springer, 2018, Vol.65,No.3.
- Thandar Thein and Jong Sou Park, 'Availability Analysis of Application Servers Using Software Rejuvenation and Virtualization', Journal of Computer Science and Technology 24(2), pp.339-346.
- Wesam Dawoud, Ibrahim Takouna, and Christoph Meinel, 2016, 'Elastic Virtual Machine for Fine-grained Cloud Resource Provisioning', Springer-Verlag Berlin Heidelberg-2011.