International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 122-129 June 2018-Dec 2018 www.csjournals.com

Virtualization: Concepts and Mechanism

Deepti Sangwan, Mukesh Yadav, Kapil
Department of Computer Science & Engineering
Gurgaon Institute of Technology and Management, Gurgaon(Hr.), India

Abstract: Virtualization is very popular technology nowadays where logical operations are separated from the physical environment. It gives the possibility to run several virtual servers, application or complete systems from a single hardware which is most of the times in lots of users centric applications likes e-Learning, business-to-business communication, social networking, computer simulation and enterprise development. In virtualization, hardware utilization resources are used more efficiently, compared to one computer-one operating system model. We have studied the concepts and mechanism of modern virtualization technology to increase the availability and efficiency of the resources more securely.
Keywords: Vmware, Hypervisor, network security, Virtualization, Effects of virtualization.

INTRODUCTION

Today almost all the businesses use information technology infrastructure to improve their productivity and resource management. However a lack of the proper technology to implement such systems will penalise businesses with increased cost and cause them to suffer technical difficulties. Older approaches are obsolete and may cause technical problems. New methods of computing which are based on a virtualized infrastructure will introduce smart management, encourage scalability and promote well organized resource usage.

Using virtualization programs such as VMware Workstation and VirtualBox will considerably improve use of network assets, increase network scalability, create a durable network which is easily managed, allow for the launching of new networks and services in a much shorter time span and, more importantly lower the cost of deployment. Virtualization can reduce the costs of managing a network in many different ways, for example, costs will initially drop by deploying fewer machines and, as a result, fewer machines require less power, meaning lower costs. With virtualization, the cost of computer hardware will be reduced, as applications can run on a single machine without a need for multiple machines and constant hardware upgrades. Nowadays many enterprises are using the virtualization technologies to speed up their workload and promote scalability. The old way of using physical machines alone has become an obsolete and inefficient compared to a virtualized infrastructure which is very cheap to deploy and cost effective to maintain.

Enterprises have saved billions of dollars and resources such as electricity and manpower through using virtualized based infrastructure. They may have reduced their hardware but they are still able to reach their desired results as before with virtualization technologies. Unfortunately, many small businesses do not have enough financial resources, time and manpower to spend on researching performance of various virtualization programs available on the market before acquiring one.

VIRTUALIZATION

The goal of virtualization is to collaboratively utilize the IT resources such as storage, processor and network to maximum level and to reduce the cost of IT resources which can be achieved by combining multiple idle resources into shared pools and creating different virtual machines to perform various tasks simultaneously. The resources can be allocated or altered dynamically. User should be conscious of basic techniques such as emulation, hypervisor, full, para and hardware assisted virtualization while using virtualization in cloud computing environment[13]. In fact Virtualization is a relatively old concept but it has gained more popularity over recent years. Virtualization goes back to the year 1960's, when it was developed to solve problems arising at that time [1]. Virtual machines and virtual monitor concepts have existed since IBM's heyday. Back then virtualization was

developed by IBM to provide timesharing of a mainframe computer [2]. However, nowadays many businesses are under pressure to achieve more with less. The same pressure is also affects system administrators all around the world. They are frequently asked to deliver more benefits to the organization with limited resources [3].

Virtualization is not only used in business-oriented environments but also in education. It is believed the use of virtualization in education dates back to as early as 2002. Virtualization will help education providers save money on maintenance and hardware, provide students with 24/7 access to lab resources and adopt new technologies in much sooner. Various studies prove that many already students use virtual machines to do their lab work instead of using a physical computer. In the beginning the use of virtualization was very costly, programs such as VMware Workstation were very expensive to deploy. Virtualization programs required computers with lots of memory and CPU power which they were very expensive at that time. Thus use of virtualization was only practiced by commercial enterprises. However nowadays computers can easily handle and run virtualization programs and, as a result, everyone with a personal computer can enjoy the benefit of virtualization [5].

To answer changing need, many organizations around the world are adopting a virtualized infrastructure and, as a result, the old way of computing is diminishing. For example, Kingston University in London is changing its information technology infrastructure by throwing away old computers in order to promote a virtualized infrastructure. According to the university it is trying to create a blueprint for virtualized education infrastructure and act as a pioneer for other universities around world which are willing to share the same cause and go virtualized [4].

Axon is a leader in information technology support. The company developed a system monitoring software for virtual based OSs. According to Axon's CEO Scott Green, Axon Performance Manager which is part of BMC tools can be easily integrated with virtual systems within a few days at a low cost. According to Green, virtualization has enormous potential advantages, however, virtual machines still require individual attention. Not having a proper monitoring system will put systems at risk. Green added that 80% of projects which Axon Corporation worked on involved virtualization technologies. Nowadays more businesses are using virtualization and virtualization technologies. Thus it can be said virtualization's popularity has dramatically increased in recent years [6].

Virtualization became a practical choice for system administrators to accomplish more with fewer resources. In computing, the term virtualization means to create a virtual version of a real entity. Applying virtualization to information technology infrastructure will reduce the quantity of unnecessary workstations to a minimum, which in turn will make management easier and costs lower [3], [7].

Stasiewicz [8] argues that virtualization is no longer a new phenomenon but a mature technology. Virtualization is accepted and integrated by many enterprises and it has been used for network infrastructure for many years. According to Stasiewicz, it can now be said that virtualization is not a fringe technology anymore but a technology which is adopted by the mainstream. According to Stasiewicz, virtualization has shown its benefits and advantages for a long time. Virtualization will provide security for network services by reducing the risk of host failure while reducing server resource consumption. Using virtualization and having a long term commitment to it, enterprises can now save money through lower energy costs and fewer hardware upgrades. According to Stasiewicz using virtualization in classrooms is not a new thing. Instructors have brought virtualization to students in many ways and have prepared them for the outside world. By using virtualization in networking classes and hardware classes, have became innovative and allowed students to create large, complex networks with fewer physical machines in a very short time [8].

Benefits of Virtualization

Virtualization can benefit businesses in many different ways by saving time, money and resources. With virtualization everyone can gain benefit, especially system administrators. System administrators can start thinking outside the box and not just focus on a few pieces of machinery. They can work on methods which will improve the quality of the services they offer. As virtualization becomes more popular, the use that comes to mind is to run multiple OSs at the same time. While this may be true it is not the main reason why businesses are moving toward virtualization. The true purpose behind this huge infrastructure

change is to reduce server quantity and facilitate workload, thus saving space, power and time which leads to saving money.

Virtualization technologies offer the following main benefits [9]:

New way of disaster recovery: A virtualized information technology infrastructure will change the old way of disaster recovery by providing a fast, dependable and low budget disaster recovery plan through hardware independent, server consolidation and easy test scenarios.

Minimize system damage: Testing a new software in an OS can cause problems and cause file-system damage. With virtualization software developers can easily test new software in a virtualized environment and, if any damage is caused to the system, it is possible to rollback the system to its original state without any problems.

Reduce software clashes: Running multiple OSs on one machine sometimes causes' systems to crash. With virtualization it is possible to run multiple OSs on one machine without having a worry.

Easy cross-platform development: Software developers can easily test their products in different OSs with just a few clicks. Having all OSs up and running in one place is something which software developers can use to their advantage while saving time.

Save money: On most servers only one application can run because if an application crashes the whole system will crash and, if there are any other applications on that server, they will stop functioning as well. To solve that problem system administrators usually run each application individually on different servers to minimize system failure. This approach perhaps solves the problem but it is very costly and inconvenient, as most of a server's capacity will be left unused. More money is also required to acquire a new server for each new application. However, with virtualization, multiple applications can run at once on the virtual server. Thus businesses can save money and resources.

Save power: Businesses spend a lot of money for energy to run unnecessary servers. However with virtualization fewer physical servers are required thus energy requirements will be reduced to a minimum and less money will be spent.

Save time: With virtualization, fewer servers are required so system administrators can spend more time on performing tasks such as backup, maintenance, installation and recovery plans.

Improved security: With virtualization, system administrators can easily set up and manage honeypot traps.

Easy desktop management: Managing users' desktops can be a cumbersome task but with virtualization system administrator can more easily manage users' desktops.

Run multiple OSs: With virtualization, multiple OSs can run concurrently on a computer system.

Virtualization Approaches

The x86 is the most commonly used CPU architecture in industry. The x86 offers four different levels of protection from 0 to 3, which are described as rings. In this architecture, each ring provides a different level of privilege. Ring 0 is the innermost ring with complete control over hardware and system resources. Ring 3 is the outermost ring with the most limited privileges. Ring 0 is the place where the OS's kernel resides and it is in control of system resources. Applications which are relate to user's are always placed in Ring 3 which only provides limited access to system resources. If an application from Ring 3 tries to access system recourses which are only accessible through Ring 0 this creates an exception and consequently causes a catch. It will result in a change from unprivileged mode to privileged mode so the OS can execute the instruction and the afterward mode will return it to unprivileged while execution continues. The virtual machine monitor runs in Ring 0 which is in charge of virtual machines and system resources. Virtual machine behaviour is exactly the same as an unprivileged user trying to execute an instruction. When an instruction executed virtual machine monitor grabs the trap the instruction mode will change to privileged mode. A virtualization program will virtualize the CPU, I/O, memory and devices. Virtualization is achieved by actively contributing physical system recourses such as memory, CPU and devices to virtual machines. There are several approaches used for x86 CPU virtualization, but full virtualization, paravirtualization and hardware-assisted virtualization are the most common approaches which exist [2].

Full virtualization

In full virtualization a virtual machine fully simulates hardware behaviour and characteristics, which will allow a virtual OS to run in isolation. Full virtualization completely separates the guest OS from the physical hardware. The guest OS cannot determine that it is being virtualized and thus no modification is needed. Full virtualization is the only method of virtualization which does not require hardware or OS help to virtualize important and confidential instructions. Full virtualization provides the best security and isolation for virtual machines and allows easy migration and portability of the guest OS [10].

Para virtualization

The word Para originates from a Greek word meaning alongside. Thus paravirtualization can be translated as alongside virtualization'. It simply means that the guest OS can communicate with a software layer which is called a hypervisor for better performance and efficiency. In paravirtualization, the hypervisor runs directly on top of the hardware. The hypervisor will automatically assign the necessary resources to the virtual machines. Paravirtualization is able to modify the OS's kernel to change non-virtualizable instructions to hypercalls which allow hypercalls to communicate directly with the hypervisor. The hypervisor is also involved in providing hypercall interfaces for important kernel operations such as interrupt handling, managing memory and time keeping. In paravirtualization the unmodified OS is not aware that it is being virtualized and important OS calls are trapped using binary translation [10].

Hardware-assisted virtualization

In hardware-assisted virtualization, the hardware provides the necessary support to create a virtual machine monitor which will allow a virtual OS to run in isolation. Hardware vendors are very interested in virtualization and are rapidly developing new products to make virtualization an easier task to achieve. Example of new improvements made by hardware vendors are Intel Virtualization Technology (VT-x) and AMD's AMD-V which both focuses on privileged instructions with a new CPU execution mode feature that allows the virtual machine manager to run below Ring 0. With hardware assisted virtualization, sensitive calls are automatically captured by the hypervisor, thus binary translation and paravirtualization are no longer required. The state of the guest OS is saved in Virtual Machine Control Blocks (AMD-V) or Virtual Machine Control Structures (VT-x). Intel VT and AMD-V CPU's became available since 2006 [10].

Types of Virtualization

Virtualization is just an abstraction of physical entity and system resources. The same concept will also apply to all different types of virtualization regardless of their type and purposes [11].

Server virtualization

Among the various types of virtualization, server virtualization is that on which most businesses are currently focussed. It is a fact that server virtualization is a big deal for businesses. Businesses can lose a lot of money and time if they choose to ignore it or can save money and time by adopting server virtualization. It is clear nowadays computer server have become huge space wasters and a cause of problems for businesses. Businesses are running out of empty space to place their servers. It seems obvious server virtualization has become a strong point of interest. Problems with servers are caused by their limitations and lack of ability to achieve multitasking. Servers can only serve one function, for instance a web server, file server, mail server, recourse management server and database server each only do one thing and, as a result, a lot of server resources are wasted. However servers can be in a multi- functioning state through the use of virtualization technologies. This will lead to less space required to house servers. Also the efficiency of existing servers will increase by 80-90 percent outranking previous estimations which were 8-14 percent due to server limitations. Server virtualization allows one server to do other servers' jobs by distributing server resources properly among different applications and platforms. Virtualization programs allow businesses to have various OSs and applications hosted locally or remotely, allowing users to access their work freely without being tied to a particular physical location [11].

Desktop virtualization

Desktop virtualization is concerned with workstations and end users. System administrators are often busy configuring, fixing and upgrading computers on a daily basis. The process is very time-consuming and an

inefficient way to mange thousands of computers. This problem for system administrators can be a very cumbersome and onerous task, because each computer must be managed differently based on individual rules and regulations. Having open ports and slots for USB and DVD allows users to install unauthorized software onto their computer. Even an innocent user's computer can be prone to viruses and trojans through accessing the internet or other means. Thus new patches and antivirus updates need to be installed on computers from time to time and computers need to be scanned for viruses regularly. All these problems will make the system administrators' job very difficult. With desktop virtualization however, all these problems can easily be eliminated and the system administrator can focus more on productivity rather than performing time-consuming tasks [11].

There are three different types of desktop virtualization which are as follows [11]:

Remote virtualization: Remote virtualization is where the OS is hosted on a server and accessed remotely by users.

Local virtualization: This method of virtualization allows multiple OSs to run on the users' machine locally.

Application virtualization: Application virtualization is a virtualization method which uses a sandbox or wrapping technique to run applications on a user computer. Therefore the application will not make any changes to the OS's registry or files system. Virtualized applications will immediately work on the user's machine without any need for installation or configuration.

Storage virtualization: Storage virtualization is a virtualization technique which will separate logical storage from physical storage. Logical storage will act as a virtualized part of the hard drive.

Storage virtualization can be achieved through three different methods:

Direct Attached Storage: In this method data storage will be directly connected to the server. This is obviously the easiest method to perform but is very hard to manage.

Network-Attached Storage: In this method, one machine will be used in the network for data storage. This method is considered to be the first step towards storage virtualization. In network-attached storage, one machine acts as data storage simplifying the process of data backup.

Storage-Area Network: A specialized approach which changes how a simple hard drive works. This process is based on using special hardware and software which will convert an ordinary hard drive into a data solution. When businesses have realized that corporate data is a key asset, which needs to be accessible 24/7 they have shifted to storage area network.

Emulation: It is a virtualization technique which converts the behavior of the computer hardware to a software program and lies in the operating system layer which lies on the hardware. Emulation provides enormous flexibility to guest operating system but the speed of translation process is low compared to hypervisor and requires a high configuration of hardware resources to run the software [12].

Virtual Machine Monitor or Hypervisor: A software layer that can monitor and virtualize the resources of a host machine conferring to the user requirements [13]. It is an intermediate layer between operating system and hardware. Basically, hypervisor is classified as native and hosted [14]. The native based hypervisor runs directly on the hardware whereas host based hypervisor runs on the host operating system. The software layer creates virtual resources such as CPU, memory, storage and drivers.

Para Virtualization: This technique provides special hypercalls that substitutes the instruction set architecture of host machine. It relates communication between hypervisor and guest operating system to improve efficiency and performance. Accessing resources in para virtualization [15] is better than the full virtualization model since all resources must be emulated in full virtualization model. The drawback of this technique is to modify the kernel of guest operating system using hypercalls. This model is only suitable with open source operating systems.

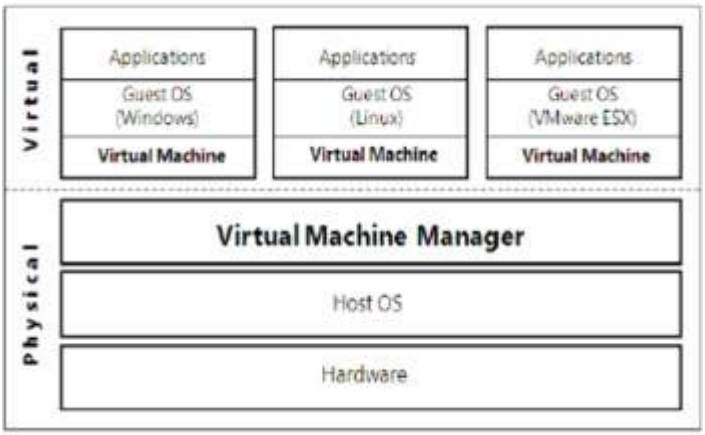
Full Virtualization: Hypervisor creates isolated environment between the guest or virtual server and the host or server hardware. Operating systems directly access the hardware controllers and its peripheral devices without cognizant of virtualized environment and requirement modifications [10].

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 122-129 June 2018-Dec 2018 www.csjournals.com

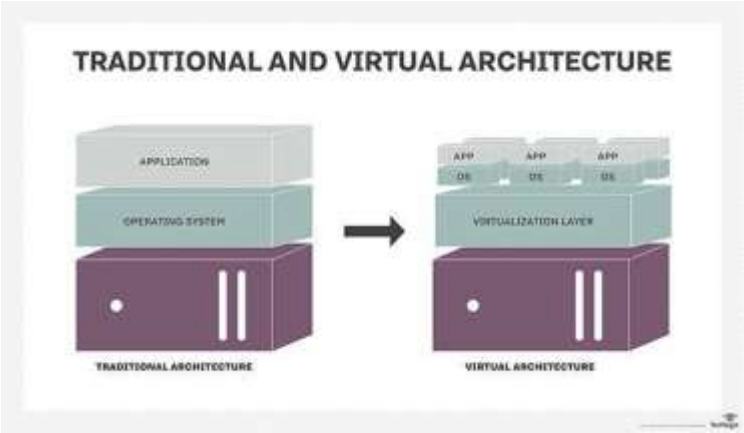
Virtualization Architecture

Virtualization is commonly hypervisor-based. The hypervisor isolates operating systems and applications from the underlying computer hardware so the host machine can run multiple virtual machines (VM) as guests that share the system's physical compute resources, such as processor cycles, memory space, network bandwidth and so on.

Type 1 hypervisors, sometimes called bare-metal hypervisors, run directly on top of the host system hardware. Bare-metal hypervisors offer high availability and resource management. Their direct access to system hardware enables better performance, scalability and stability. Examples of type 1 hypervisors include Microsoft Hyper-V, Citrix XenServer and VMware ESXi[12].



A type 2 hypervisor, also known as a hosted hypervisor, is installed on top of the host operating system, rather than sitting directly on top of the hardware as the type 1 hypervisor does. Each guest OS or VM runs above the hypervisor. The convenience of a known host OS can ease system configuration and management tasks. However, the addition of a host OS layer can potentially limit performance and expose possible OS security flaws. Examples of type 2 hypervisors include VMware Workstation, Virtual PC and Oracle VM VirtualBox



VIRTUALIZATION PLATFORMS

VMware

Any conversation about virtualization for small and medium-sized businesses usually starts around VMware. Although it wasn't necessarily the first, VMware was the company that really put office virtualization on everyone's action item list. The company offers a number of different solutions for different sized businesses with a wide variety of needs. Its ease of use and robust security features have secured its reputation as one of the best options for virtualization at SMBs.

Citrix

An average user may not recognize the company name, but has a good shot at previous knowledge of their popular remote access tools, GoToMyPC and GoToMeeting. Citrix has specifically geared their virtualization software, XenApp, XenDesktop, and VDI-in-a-box toward SMBs and even claims that non-IT staff can easily manage and administer the services. They even provide a free trial to prove it.

Microsoft

Although it may be a little more difficult to manage without an in-house or outsourced IT staff, Microsoft's Hyper-V option is hard to ignore considering its integration with the popular cloud platform Azure. Whether you're a Microsoft loyalist or you just want to minimize the number of vendors in your network, Hyper-V offers everything you need from a virtualization service.

Oracle

This company just keeps getting bigger and bigger. Specializing in marketing software, they also offer database management, cloud storage and customer relationship management software. If you're using any of their services already, there could be benefits to enlisting their virtualization services as well. Oracle does everything, server, desktop and app virtualization, and they believe that consolidation of all of these into one solution is what sets them apart.

Amazon

And since we're on the topic of household names, let's talk about Amazon's EC2 platform, which hosts scalable virtual private servers. The ability to scale and configure capacity is definitely EC2's biggest draw for SMBs, who are preparing for the possibility of rapid growth. Although almost any virtualization service is rooted in scalability, Amazon is leading the pack in how quickly and finely you can adjust your solution to your individual needs.

Virtualization is a really hard topic for most SMBs to tackle. This list only covers the most popular vendors, and there are plenty more out there. Choosing one based on its application possibilities and management requirements is not a subject for the lighthearted. Get in touch with us today so we can break down all of the technobabble into easy-to-understand advice and expertise.

Advantages of virtualization

The recent trends in virtualization are consolidation of data centers thus reducing the managing cost.

Apart of its benefits it has some drawbacks like managing virtual resources is critical and migrating services of these resources are difficult in achieving high availability.

If one server fail VM will be restarted on the other virtualized server in resource pool restoring the required services with minimum service interruption.

Virtual resources are critical for managing and data monitoring. Running applications with high utilization and availability is a challenging issue.

Hypervisor: A hypervisor is a software, hardware or a firmware that provides virtual partitioning capabilities which runs directly on hardware. It is defined as the virtual machine manager which allows multiple operating systems to run on a system at a time providing resources to each OS without any interaction.

Hypervisor controls all the guest systems. As the operating system number increases managing is difficult these leads to security issues. If a hacker gets control over the hypervisor he can control the guest systems by knowing the behavior of the system which causes data processing damage. Advanced protection system is to be developed to monitor the activities of the guest Virtual machine[9].

CONCLUSION

To have physical and virtual controls in the cloud environment one must protect data by implementing strong encrypting techniques using secure connections and applying data loss prevention policies[12]. Access control policies are to be established and client identities are to be checked. Data center platforms, infrastructure and client devices are to be secured by trusted computer policies.

REFRENCES

[1] K. Miller and M. Pegah, "Virtualization: virtually at the desktop," presented at the Proceedings of the 35th annual ACM SIGUCCS fall conference, Orlando, Florida, USA, 2007.
[2] W. Chen, et al., "A Novel Hardware Assisted Full Virtualization Technique," presented at the Proceedings of the 2008 The 9th International Conference for Young Computer Scientists, 2008.
[3] U. Pawar and M. Bhelotkar, "Virtualization: a way towards dynamic IT," presented at the Proceedings of the International Conference & Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.
[4] J. E. Dunn. (2011, 28 November). British university chucks out PCs in major virtualization push. Available: http://www.itworld.com/operating-systems/217799/kingston-university-chucks-out- pcs-major-virtualisation-push
[5] P. Li, "Exploring virtual environments in a decentralized lab," SIGITERes. IT, vol. 6, pp. 4-10, 2009.
[6] R. Jackson. (2008, 28 November). Axon launches SaaS monitoring system. Available: http://computerworld.co.nz/news.nsf/tech/4128752D167403CACC25745D0081A2E6
[7] M. F. Mergen, et al., "Virtualization for high-performance computing," SIGOPS Oper. Syst. Rev., vol. 40, pp. 8-11, 2006.
[8] S. Stasiewicz, "Worth Getting Hyped Up Over Hyper-V?," presented at the Annual NACCQ, 2008.
[9] D. Marshall. (2011, 28 November). Top 10 benefits of server virtualization. Available: http://www.infoworld.com/d/virtualization/top-10-benefits-server-virtualization-177828?page=0,0
[10] VMware. (2007, 31 Jan). A Performance Comparison of Hypervisors. Available: http://www.vmware.com/pdf/hypervisor_performance.pdf
[11] B. Johonnesson. (2001, 28 November). The Different Types of Virtualization. Available: http://bucarotechelp.com/computers/winadmin/89050501.asp
[12] Graziano, Charles. "A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project". Retrieved 2013-01-29.
[13] Jump up, Turban, E; King, D; Lee, J; Viehland, D (2008). "Chapter 19: Building E-Commerce Applications and Infrastructure". Electronic Commerce A Managerial Perspective. Prentice-Hall. p. 27.
[14] Jump up "Virtualization in education" (PDF). IBM. October 2007. Retrieved 6 July 2010. A virtual computer is a logical representation of a computer in software. By decoupling the physical hardware from the operating system, virtualization provides more operational flexibility and increases the utilization rate of the underlying physical hardware.
[15] Jump up, "Strategies for Embracing Consumerization" (PDF). Microsoft Corporation. April 2011. p. 9. Retrieved 22 July 2011