Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.626 – 636

RESEARCH ARTICLE

IMPLEMENTATION OF MULTIPLE OPERATING SYSTEMS IN VISUALIZED PLATFORM FOR HYPERGEAR CLOUD COMPUTING

M.Kalaiselvi[#1], H.Lookman Sithic[*2]

[1]Research Scholar, Muthayammal College of Arts and science

[2]Assistant Professor, Muthayammal College of Arts and science

ABSTRACT

Cloud computing is one of today's most exciting technologies, because it can reduce the cost and complexity of applications, and it is flexible and scalable. These benefits changed cloud computing from a dreamy idea into one of the fastest growing technologies today. Actually, virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them.

This paper proposes new security architecture in a hypergear base virtualization technology in order to secure the cloud environment. A system that uses virtualization technology to allocate data center resources dynamically based on application demands. in this project, we introduces vm migration, a technique that transparently migrates only the working set of an idle vm and support green computing by optimizing the number of servers in use. We use the maximum precedence algorithm to reduce the burden in virtual machine. We develop a set of heuristics that prevent burden in the system effectively while saving energy used.

Keywords: Virtualization, hypergear techniques, Vmware ESXi

1. INTRODUCTION

A Cloud Computing is a computing model that makes it resources such as servers, middleware, and applications available over the internet as services to business organizations in a self-service manner. The cloud is a set of hardware, networks, storage, services, and interfaces that enable the Delivery of computing as a service. Cloud services include the rescue of software, transportation, and storage over the internet (either as separate components or a complete platform) based on user request. There are many participants of cloud such as end users, dealing organization and cloud service contributor. As cloud patrons, enterprises have to improve cloud security. Commercial information must be secured in cloud computing. Cloud security is a cooperative task of cloud providers and enterprises. An enterprise is principally in charge for the security of the application, data and possibly other levels of the transportation load. Likewise, vendors can update

application/os/middleware security patches sooner because of higher accessibility of server and resources. in cloud computing promises lower costs, brisk scaling, easier continuation, and service accessibility anywhere, anytime, a key challenge is how to ensure and build assurance that the cloud can holds user data securely and user friendly with/without help of server assessments.

2. CLOUD COMPUTING WITH VIRTUALIZATION

Cloud Computing provides the ability to add capacity as needed, typically with very small lead times. Clearly, Cloud Computing provides a new compelling mechanism for dealing with application services that need to be scalable. A brief introduction of Cloud Computing, its key delivery technology of virtualization, the scalability and the scaling indicators of web applications in a Cloud will be given in the following sections.

2.1 Cloud Computing

Cloud Computing is a way to deliver services over the network. New advances in virtualization technology [7, 8], processors, disk storage, broadband Internet access and fast, inexpensive and powerful servers have all combined to make Cloud Computing a realistic and compelling paradigm. Cloud Computing basically use virtualization technique to turn computer resources into virtual guest machines.

These virtual machines usually reside on some networked physical servers in a hosting environment. However, the virtual guest machines can be moved around, thus breaking direct hardware dependency associated with physical machines. With hardware dependency no longer an issue, the guest system can be insulated from hardware breakdowns, and be automatically moved to another piece of available hardware.

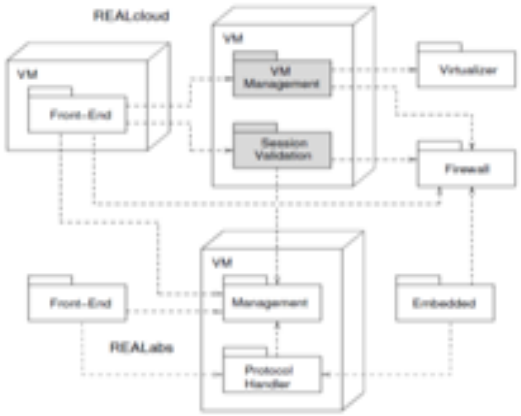

Figure 1: Cloud computing Environment.

A typical Cloud Computing environment with automated provisioning capabilities, advanced virtualization technologies, and virtual machines hosting on physical servers offering Cloud application services to users directly is illustrated in Fig. 1. The user sees only the service and not the implementation or infrastructure required for its delivery. Examples of Cloud services include technology services such as storage, data protection, applications, business processes and even business and consumer services such as email and office applications. Cloud Computing allows users

and companies to use the services and storage that they need, when they need them and, as wireless broadband connection options grow, where they need them. Customers can be billed based upon As a result, Cloud Computing has the potential to overturn the software industry entirely, as applications are purchased, licensed and run over the network instead of a user desktop. This shift will put data centers and their administrators at the center of the distributed network, as processing power, bandwidth and storage are all managed remotely.

The following are typical types of Cloud Computing services depending on nature of offerings:

1. **Application Services** - Any web application is a Cloud application service in the sense that it resides in the Cloud. Google, Amazon, Facebook, Twitter, Flickr, and virtually every other Web 2.0 application is a Cloud application in this sense.
2. **Platform Services** - One step up from pure utility computing are Cloud platform services like Google Apps and Google Apps Engine, and Salesforce's force.com, which hide virtual machine instances behind higher-level APIs.
3. **Infrastructure Services** - Amazon Elastic Compute Cloud (EC2) is a typical Cloud infrastructure service which provides raw virtual machine instances, storage, and computation at pay-as-you-go utility pricing, and is currently the leading provider in this category. Developers are the typical target of this kind of Cloud Computing services.

2.2 Virtualization Technology

Virtualization allows servers, storage devices, and other hardware to be treated as a pool of resources rather than discrete systems, so that these resources can be allocated on demand Platform virtualization is performed on a given hardware platform by a control software, called a hypervisor or virtual machine monitor. This software creates a simulated computer environment, called a virtual machine, for its guest software. The guest software, which is often itself a complete operating system, runs just as if it were installed on a stand-alone hardware platform. The current leading virtualization and software providers include VMware, Xen, KVM, and Microsoft Virtualization.

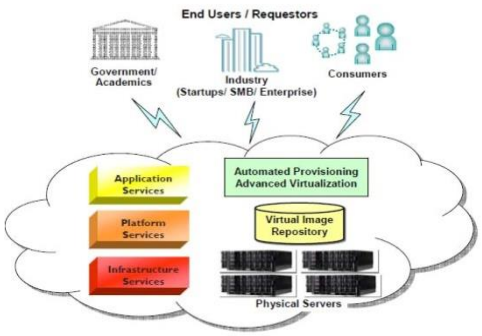

Figure 2: Virtualization Technology

As a means of encapsulation of physical resources, virtualization solves several core challenges of datacenter managers and delivers specific advantages, including:

2.2.1. Higher Utilization Rates: Through virtualization, workloads can be encapsulated and transferred to idle or underused systems. This means that existing systems can be consolidated, so purchasing additional server capacity can be delayed or avoided.

2.2.2. Resource Consolidation: Virtualization allows for consolidation of multiple IT resources. Beyond server and storage consolidation, virtualization provides an opportunity to

consolidate the systems architecture, application infrastructure, data and databases, interfaces, networks, desktops, and even business processes, resulting in cost savings and greater efficiency.

2.2.3. Lower Power Usage/Costs: Using virtualization to consolidate makes it possible to cut total power consumption and save significant costs.

2.2.4. Space Savings: Server sprawl remains a serious problem in most datacenters, but datacenter expansion is not always an option, with expensive building costs and cooling costs. Virtualization can alleviate the strain by consolidating many virtual systems onto fewer physical systems.

2.3 Virtualization Components

In a traditional environment consisting of physical servers connected by a physical switch, it organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management is not typically provided from a virtual switch. Basically, the virtual switch has links from the physical switch via the physical nic that attaches to virtual machines. The resulting lack of oversight of the traffic flows between and among the virtual machines on the same physical level affects security and performance surveying. There are several common approaches to virtualization with differences between how each controls the virtual machines.

A. operating system-based virtualization:

in this approach ,virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest os's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the virtual machines. This approach is simple, but it has vulnerabilities, such as when an attacker injects controlling scripts into the host operating system that causes all guest os's to gain control over the host os on this kernel. The result is that the attacker will have control over all VM's that exist or will be established in the future.

B. application-based virtualization:

An application-based virtualization is hosted on top of the hosting operating system .this virtualization application then emulates each VM containing its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to operating system-based.

C .hyper gear-based virtualization:

The hyper gear is available at the boot time of machine in order to control the sharing of system resources across multiple VM's. Some of these VM's are privileged partitions which manage the virtualization platform and hosted virtual machines. In this architecture, the privileged partitions view and control the virtual machines. This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems. However, it is vulnerable because the hyper gear has a single point of failure. If the hyper gear crashes or the attacker gains control over it, then all VM's are under the attacker's control. However, taking control over the hyper gear from the virtual machine level is difficult, though not impossible. According to this characteristic, this layer chose for implementing proposed security architecture.

3. VIRTUALIZATION HYPERGEAR SECURITY BENEFITS

In a virtualization environment, there are several virtual machines that may have independent security zones which are not accessible from other virtual machines that have their own zones. A hyper gear has its own security zone, and it is the controlling agent for everything within the virtualization host.

Hyper gear can touch and affect all acts of the virtual machines running within the virtualization host. There are multiple security zones, but these security zones exist within the same physical infrastructure that, in a more traditional sense, only exists within a single security zone. This can cause a security issue when an attacker takes control over the hyper gear. Then the attacker has full control over all data within the hyper gear's territory. Another major virtualization security concern is "escaping the virtual machine" or the ability to reach the hyper gear from within the virtual machine level.

Benefits and Weakness of Hyper Gear-Based Systems:

The hyper gear, apart from its ability to manage resources, has the potential to secure the infrastructure of cloud. Hyper gear-based virtualization technology is the best choice of implementing methods to achieve a secure cloud environment.

The reasons for choosing this technology:

1. Hyper gear controls the hardware, and it is only way to access it. This capability allows hyper gear- based virtualization to have a secure infrastructure. Hyper gear can act as a firewall and will be able to prevent malicious users to from compromising the hardware infrastructure.

2. Hyper gear is implemented below the guest os in the cloud computing hierarchy, which means that if an attack passes the security systems in the guest os, the hyper gear can detect it.

3. The hyper gear is used as a layer of abstraction to isolate the virtual environment from the hardware underneath.

4. The hyper gear-level of virtualization controls all the access between the guests' os's and the shared hardware underside. Therefore, hyper gear is able to simplify the transaction-monitoring process in the cloud environment.

4. MULTIPLE OPERATING SYSTEMS IN HYPERGEAR

Over time, organizations tend to relax their security pose. To fight repose of security, the cloud provider should perform standard security assessments. The assessments should be done by someone who is knowledgeable and able to identify issues and fix them.

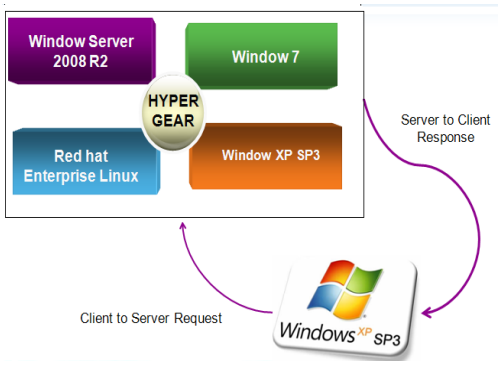

Figure 3: Multiple Operating Systems Using Hypergear Techniques in Client to Server

The report should be provided to each client resources without delay after it is performed so they know application virtualization separates individual instances of an application from the underlying operating system, providing a distinct application terminal for each user. Security consideration for the current state of the overall cloud's security.

5. MULTIPLE OS PROCESS OF HYPERGEAR

Virtualization refers to the logical notion of computing resources from physical constraints. One common pensiveness is referred to as a virtual machine, or VM, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including operating systems, networks, memory and storage.

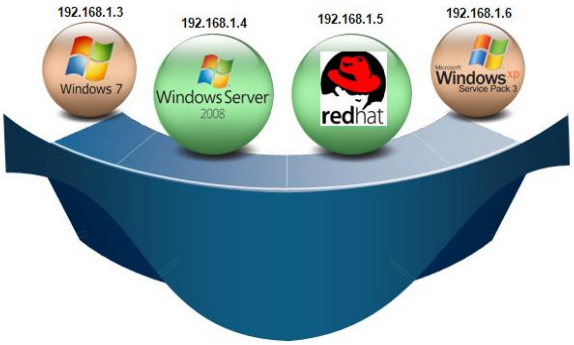

Figure 4: Multiple Operating Systems Using Hypergear Cloud Computing

The term workload is gradually more used to describe the huge array of virtualized resources. For example, a virtual machine is a type of workload. While VMs are the major virtualization technology implemented today, there are a number of other workloads to consider, including application, desktop, network, and storage virtualization models. Operating system (os) virtualization is commonly used to take the resources running in an operating system on a single physical server and separate them into multiple, smaller partitions, such as virtual environments, virtual private servers, visitors, zones, etc.

6. HYPERGEAR MECHANISM IN CLOUD COMPUTING

Working principle:

Virtual computing presents a new trend to distribute and Internet computing to coordinate large scale heterogeneous resources sharing and problem solving in dynamic, multi institutional virtual organizations. The computing resources are highly heterogeneous, ranging from single PCs and workstations, cluster of workstations to file transfer to supercomputers. With virtual technologies, it is possible to construct large scale applications over the virtual environments. Now the virtual technologies are involving towards an Open Virtual Service Architecture (OGSA) in which a virtual provides an extensible set of services that virtual organizations can be aggregated. According to file transfer utility, the resources

and services can be accessed with standard interfaces migration which can be defined and executed. The purpose of virtual computing is to eliminate the resource island and to make computing and services ubiquitous.

However there are many challenges to construct dependable virtual services for example failure of a power leading to power loss of one part of the distributed system physical damage to the virtual computing fabric as a result of natural events or human acts and failure of system or an application software leading to the loss of the services. Due to the diverse failures and error conditions in the virtual environments, developing, deploying, and executing applications over the virtual is a challenge. Dependability is a key factor for virtual computing. To construct dependable virtual services requires an efficient failure detection approach and systematic failure handing mechanism. Many researchers have been done on dependable computing in distributed, parallel, and virtual systems. Here, we present a short review of the techniques and related models.

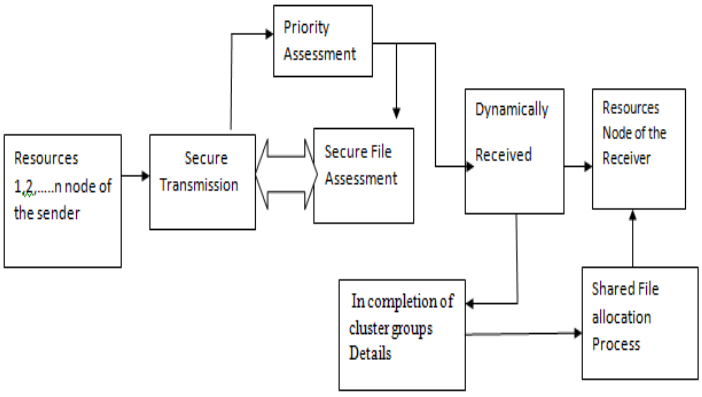

Figure 5: File Requisition

It provided the first formal specification of unreliable failure detectors for reliable distributed system. The presented an adaptive failure detector which can adapt to the changing conditions by reconfiguring itself dynamically, but this approach only reconfigured some system parameters, the system topology could not be reconfigured. Another kind of adaptive failure detection protocol was lazy failure detection the lazy protocol depended highly on the communication patterns between the application processes and may perform poorly for some specific applications. It analyzed several implementations of failure detectors in the context of LAN, and proposed to customize the implementation of the failure detector with respect to the communication pattern of some particular algorithms.

i. Parallel Virtual Systems

Level to level and virtual systems are middle wares that provide a set of services to aggregate an important number of resources inside a unique system. Hence it implies the necessity of managing heterogeneity, scalability, dynamics and fault recovery. The demonstrated the validity of solving some numerical applications on file to peer systems. The project uses to simulate the highest energy file showers. The three level named above are based on file to peer systems and they all share a property. Each parallel task does not exchange any data during the computation No reliable tools are currently available to help the user during the development of parallel applications on a large scale architecture. As a result the user has to solve problems such as heterogeneity, fault tolerance, resource management and scheduling for each new application.

The dynamics of such architectures increase the global difficulty of using those platforms. Those difficulties specific to each middleware should not have to be solved for each application. Advanced tools should solve most of the complexity automatically and transparently for the user by introducing more and more services in the execution layer.

Framework so as to provide some tools that will help users design and execute complex parallel applications. Its goals are to help users during the development and execution steps. Through our work we aim at demonstrating the feasibility of using file transfer and virtual systems for parallel communicating applications. In addition to this we design easy-to-use tools in order to manage underlying middle wares. This article focuses on performance evaluation with a numerical application. The performance evaluation consists in two series of experimentations. The first one corresponds to the hypothesis that the application data are previously generated by a parallel application or available on a distributed persistent storage. The second series of experimentations integrates the peer to peer application generating the matrix involved in the computation. The second section presents the solution in use on the different virtual and peer to peer middle wares through user's point of. It mainly deals with tools and libraries available to design parallel applications. The third section introduces the Framework. It also shows how it interacts with virtual and peer to peer middle wares and presents the first implementation using the web peer to peer system

ii Maximum Precedence algorithm:

A user has a list of numbers and wishes to find the bare minimum value and the upper limit value in the list. A program is required which will allow the user to enter the information from the keyboard and which will calculate the minimum and maximum values that are input. The user is quite happy to enter a count of the numbers in the list before entering the numbers. So easily to share the resources file in secure manner.

In this work, i propose virtualization architecture to secure cloud. In the proposed architecture, i try to reduce the workload spread out security-related tasks between hypervisor and VMs, and convert the centralized security system to a spread one. The distributed security system is a very good way to reduce the workload from HyperGear-based virtualization, but this distribution may inject vulnerabilities to cloud. In addition, distributed security systems have more complexity than centralized ones. Because of several benefits, such as the fault-tolerant capability, of distributed security management, it is not possible to ignore it and
persist on centralized managing, so introduces VM migration, a technique that transparently migrates only the working set of an idle VM and support green computing by optimizing the number of servers in use. To use the maximum precedence algorithm for reducing the burden in virtual machine. To develop a set of heuristics that prevent burden in the system effectively while saving energy used. So secure process of virtualization is maintained efficiently.

Algorithm for when a request for a new instance arrives.

Input: None
Output: None
Algorithm sched_priority
{
Flag=0;
If(P1 is not set)
P1=max available resource node
If(P1 is turned OFF)
Turn P1 ON
If(load factor of P1<0.8)

Assign VM to P1;
Flag=1;
if(P2 is set AND load factor of P2<0.8 AND
Flag=0)
Swap P1 and P2;
Assign VM to P1;
Else if(Flag=0)
P2=P1
P1=current max available resource node
If(P1 is turned OFF)
Turn P1 ON
Assign VM to P1;
Turn OFF all unused nodes;

}

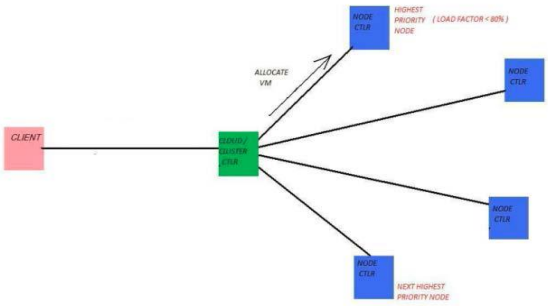

Figure 6: HyperGear techniques is allocated to the highest priority resources

iii Virtual machine migration in Hypergear cloud computing

There are two ways VM migration may come into play. First, within the data center, the cloud provider may need to move re-optimize the placement of VMs to balance load, save power, or avoid resource fragmentation. In this case, VMs in the data center can be moved across physical machines either within or across edge domains. This is done by transferring dynamic VM state from source to destination hosts. Once state transfer is complete, a gratuitous arp message is sent from the destination host to announce the VM's new location. Note that this announcement only reaches hosts in the same vlan in the same edge domain. If both source and destination hosts are in the same domain, fe and cc are not involved in the process.

If the vm is migrated to a different domain, then cc updates the vm's location in its table, including both eid andvlan id.in the second case, the customer may need to migrate Vms between its on-site network and data center. This can be easily achieved if the customer's network and its data center network are configured to be in the same Lan, connected. in this case, fe and cc will register the vm's new location .But from the customer's point of view, the migration procedure is the same as migrating VMs within its on-site lan. Migration between customer site and data center across different subnets is more challenging. We can deploy a feat the edge of customer site network, which can register the location of the VM, and tunnel packets to and from in the data center.

7. CONCLUSION

In this paper, i propose virtualization architecture to secure cloud. In the proposed architecture, i try to reduce the workload spread out security-related tasks between hypergear and VM's, and convert the centralized security system to a spread one. The distributed security system is a very good way to reduce the workload from hypergear-based virtualization, but this distribution may inject vulnerabilities to cloud. In addition, distributed security systems have more complexity than centralized ones. Because of several benefits, such as the fault-tolerant capability, of distributed security management, it is not possible to ignore it and persist on centralized managing, so introduces VM migration, a technique that transparently migrates only the working set of an idle VM and support green computing by optimizing the number of servers in use. To use the maximum precedence algorithm for reducing the burden in virtual machine. To develop a set of heuristics that prevent burden in the system effectively while saving energy used. So secure process of virtualization is maintained efficiently and dynamically changed the resource. Future studies on this work should include further validation on the effectiveness of the maximum precedence algorithm. more specifically, more real-life mission-critical systems should be involved in the validation; besides, how to relax the assumptions adopted in this study should also be further investigated to improve the flexibility of the testing framework.

REFERENCES

[1] F. Sabahi, "Security of Virtualization Level in Cloud Computing," inProc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu, China, 2011,197-201.

[2] K. K. Fletcher, M.S.thesis, "Cloud Security requirements analysis and security policy development using a high-order object-oriented modeling," Dept. Computer Science, Missouri Univ. of Science and Technology, Rolla, Ms, 2010.

[3] Fang Hao, T.V. Lakshman, Sarit ukherjee, Haoyu Song Bell Labs, Alcatel-Lucen" Secure Cloud Computing With a Virtualized Network Infrastructure"

[4] L .Litty, "Hypervisor-based Intrusion Detection," M.S. thesis, Dept. Computer Science, University of Toronto, 2005.

[5] F. Sabahi, "Intrusion Detection Techniques performance in Cloud Environments " in Proc. Conf. on Computer Design and Engineering, Kuala Lumpur, Malaysia, 2011, pp. 398-402.

[6] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masouka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the ACM Cloud Computing Security Workshop, Chicago, Illinois, USA., 2009.

[7] Almond, "A Practical Guide to Cloud Computing Security," 2009.

[8] P. R. Gallagher, A Guide to Understanding Data Remanence in Automated Information Systems: The Rainbow Books, ch.3 & ch.4, 1991.

Author's Details:

H.Lookman Sithic received his B.Sc degree from Bharathidasan University Trichy and M.S. (IT) degree from Bharathidasan University. He has completed his M.Phil at Periyar University. He is having 13 year s of experience in collegiate teaching and he is the Assistant Professor of computer science and applications in Muthayammal college of Arts and Science, Rasipuram affiliated by Periyar University. His main research interests include data mining, Network security.

M.Kalaiselvi received her BCA, degree in Trinity College for women Namakkal from Periyar University, Salem (2007 - 2010) [TamilNadu (India). Then, did MCA degree in Erode sengunthar Engineering College, Erode from Anna University Chennai (2010-2013). She is the M.Phil Research Scholar of Muthayammal College of Arts and Science, Rasipuram. Periyar University, Salem. Her Area of interest is Networking.

