IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 7 July, 2016

Analysis of risks and skepticism of managers adopting cloud base system infrastructure

Richmond Ikechukwu Ibe (Ph.D.)
Lead Professor of Business Management
Jarvis Christian College
Hawkins Texas

Abstract

Cloud computing has changed the way organizations, and individuals store their information, but there is still skepticism of organizations migrating to the cloud. This study aimed at understanding the skepticism of managers migrating to the cloud. The problem researched was to understand why most executives in various organizations are skeptical migrating to the cloud despite the economic benefits. The purpose of this research study was to investigate into these skepticism of cloud computing despite the economic benefits of cloud computing. This study is limited to managers and executives of organizations who may be skeptical in adopting cloud infrastructure. The theoretical framework for this research was based on system theory. Data was collected using the secondary sources and analyzed using Megastats and excel application software.However, the analysis of the data showed that executives' concerns and the skepticism of adopting the cloud infrastructure were the lack of control of data and difficulties migrating to the cloud. The recommendation to the executive of organizations that may be skeptical of migrating to the cloud because of information security would be to adopt the Cloud as an infrastructure. In this type of cloud base system, the consumer does not have control of the underlying physical infrastructure but has control of the operating systems, deployed applications, storage, and possibly limited control of selected networking components. The significance of this study is that it could help managers and executives of organizations to make better information security decisions. Finally, more research is needed in these areas to fill in the gap in security risk associated with data virtualization, which is cloud computing.

According to National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling global, suitable, on-demand network access to a shared pool of configurable computing resources. These include networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction." (p.2). perceptively, cloud computing has changed the way organizations store their data because of Total cost of Ownership TCO. Despite its advantages, most organizations are still skeptical of migrating to the cloud possibly because of security concerns. To have more visibility into these skepticisms the research study aimed at analyzing, and comparing different services, and deployment models. Comparing deployment models could invigorate the skepticism of the cloud computing.

Background of the study

There are three services models in cloud computing. These include software as a service SaaS, Platform as service (PaaS), and Infrastructure as service (IaaS). Software as Services SaaS delivers a single application through the browser to several users using a multitenant architecture. With SaaS, a provider sells an application to customers on a license basis, in a "pay-as-you-go" model. Platform as a Service (PaaS) Next level up in the pyramid is Platform cloud. PaaS delivers development/operating environments as a service. It includes the set of tools and services designed to make coding and deploying the applications quickly and efficiently. PaaS is similar to SaaS except that, rather than being software delivered over the web, it is a platform for the development/deployment of that software, delivered over the web. IaaS has evolved from a virtual private server (VPS) concept. It provides complete flexibility to consumers in choosing desktops, servers or network resources. Consumers can customize the entire infrastructure package by selecting CPU hours, storage

space, bandwidth, etc. According to Scudder (2011), Rather than buying expensive servers and taking the headache of setting up the data centers, IaaS cloud helps business in reducing IT cost.

Statement of a problem

Cloud computing appears to have numerous advantages over any storage systems. Besides, most managers in various organizations appear to be very skeptical migrating to the cloud despite the economic scale of cloud computing. The problem researched was to understand the skepticisms of managers that hesitate to adopt the cloud infrastructure. The risks implications were assessed that possibly gave clear understanding of the skepticisms and risks associated with the resource assignment of the cloud infrastructure. The resource assignment was mentioned here because it appeared to be a possible risk. According to Winkler (2011), "Virtualization is transitioning from the technology that drives server consolidation and data center operations to a key ingredient in creating a flexible, on-demand infrastructure—another way of describing cloud computing."(para.2). Winkler (2011) stated that, While there are certain issues to address when adopting virtualization in any environment, there are additional security concerns that arise when using virtualization to support a cloud environment." (para.2). Winkler pinpointed that One potential risk has to do with the potential to compromise a virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target. At the scale of the cloud, such a risk would have the broad impact if not otherwise mitigated. To solve the problem, it requires an additional degree of network isolation and enhanced detection by security monitoring.

Purpose of the study

The purpose of this research study was to determine if cloud computing is the solution to organizational data security. Despite all huge investments made in cloud computing yet data bridges has be a concern. This research study aimed at determining the skepticism or the reason for managers not adopting the cloud infrastructure.

Theoretical Framework

The theoretical framework for this research is based on system theory. It is a theory and a particular set of tools for identifying and mapping the inter-related nature and complexity of organizational situations. It encourages explicit recognition of causes and effects, drivers and impacts, and in so doing helps anticipate the effect a policy intervention, which likely to have variables or issues of interest. The system theory view organization as interdependent units that communicates together to overcome ever-changing environment. Below illustrates a conceptual model of system theory perspectives. The system view organization as made up of five different components namely: (a) Environment (b) Input (c) Transformation (d) Output (e) Feedback.

Conceptual Model Frame Work

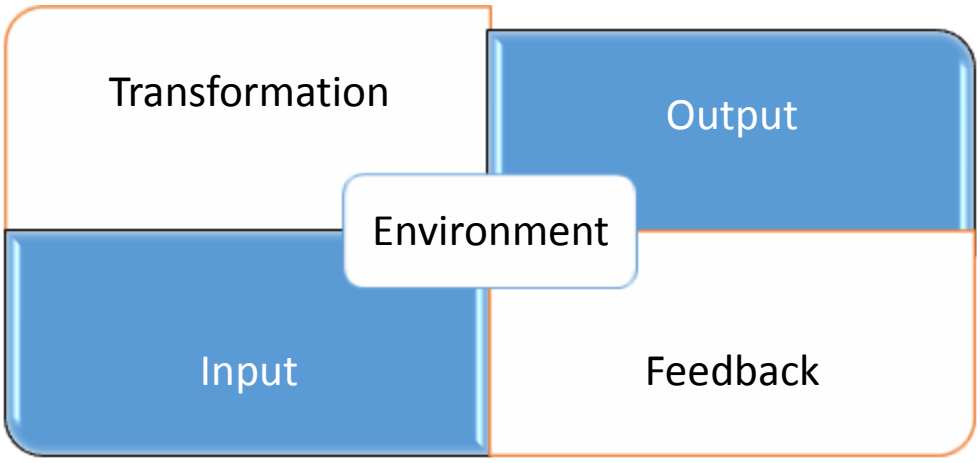

Fig 1: Conceptual Model of Systems perspective

(Conceptual model developed by the Researcher, and the theory was adopted from "Hegel developed in the 19th century a theory to explain historical development as a dynamic process.").

Scope/Limitation

The scope of this study is limited to the analysis of possible risks and skepticism of organizational cloud computing, and the hesitance of executives of organizations adopting cloud computing.

Literature Review

Benefits of Cloud computing and Storage concerns

According to a white paper delivered by Diversity limited, and sponsored by Rack Space (2011), the paper highlighted the benefits of cloud computing that including the following:

a) Virtualization – The ability to increase computing efficiency
b) The democratization of Computing – Bringing enterprise scale infrastructure to small and medium businesses.
c) Scalability and fast provisioning – Bringing the web-scale IT at a rapid pace.
d) Commoditization of infrastructure – Enabling IT to focus on the strategic aspects of its role.

Despite all these great benefits it appears that there remains a security concern. Cost low (2015), asserted that the executive's skepticism behind cloud adoption is "once the data goes to the cloud you lose some control." Companies need to look at data storage and the destruction of unwanted data." According to Winkler (2011), the security concern with virtualization has to do with the nature of allocating and de-allocating resources such as local storage associated with Virtual Machine (VMs). During the deployment and operation of a VM, data is written to physical memory. If it's not cleared before those resources are reallocated to the next VM, there's a potential for exposure.

According to Security of the VMware vSphere Hypervisor article (2014), "Instruction Isolation From a security standpoint, a primary concern is that a virtual machine's running in a highly privileged mode that enables it to compromise another virtual machine or the VMM itself." (p.5). However, Intel VT-x and AMD-V extensions don't enable virtual machines to run at "Ring-0." Only the VMM runs at a hardware privilege level. The guest OSs run at a virtualized privilege level. The guest OS does not detect that it is running at a non-privileged virtualized level as illustrated in fig 2.

Besides, when the guest OS executes a privileged instruction, it is trapped and emulated by the VMM. The article asserted, Intel Hyper-Threading Technology (Intel HT Technology) enables two process threads to execute on the same CPU core. These threads can share the memory cache on the processor. ESXi virtual machines do not provide Intel HT Technology to the guest OS. ESXi, however, can utilize it to run two different virtual machines simultaneously on the same physical core if configured to do so.

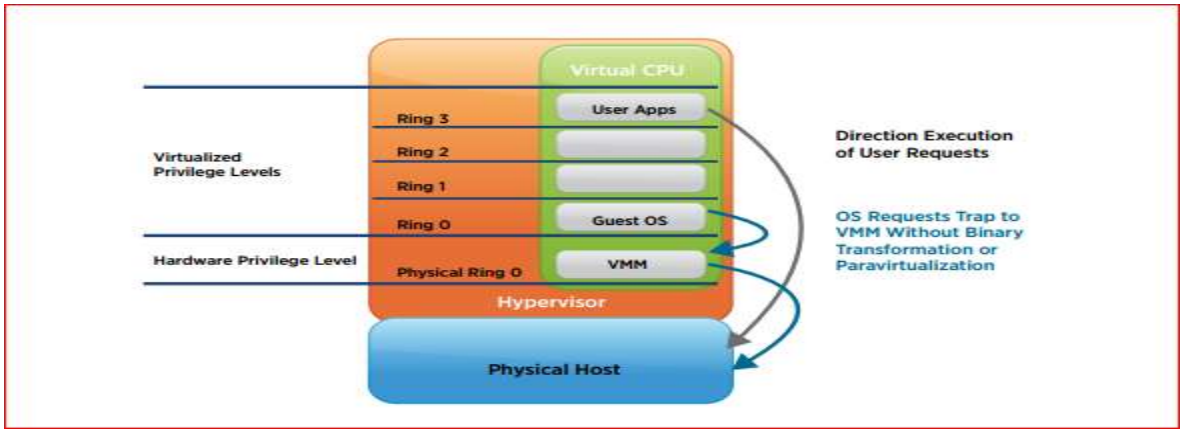

Fig 2 *Instruction Isolation*: (Adopted from Security of the VMware vSphere Hypervisor Article (2014). Retrieved from http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf).

Memory Isolation

According to Security of the VMware vSphere Hypervisor article (2014), "the system administrator defines the RAM allocated to a virtual machine by the VMM via the virtual machine's settings. The VMkernel allocates memory when it defines the resources to be used by the virtual machine. A guest OS uses physical memory allocated to it by the VMkernel and defined in the virtual machine's configuration file. An OS booting on real hardware is given a zero-based physical address space; an OS executing on virtual hardware is given a zero-based address space. The VMM gives each virtual machine the illusion that it is using such an address space, virtualizing physical memory by adding an extra level of address translation. A machine address refers to actual hardware memory; a physical address is a software abstraction used to provide the illusion of hardware memory to a virtual machine. This paper uses "physical" in quotation marks to distinguish this deviation from the usual meaning of the term." (p.5).

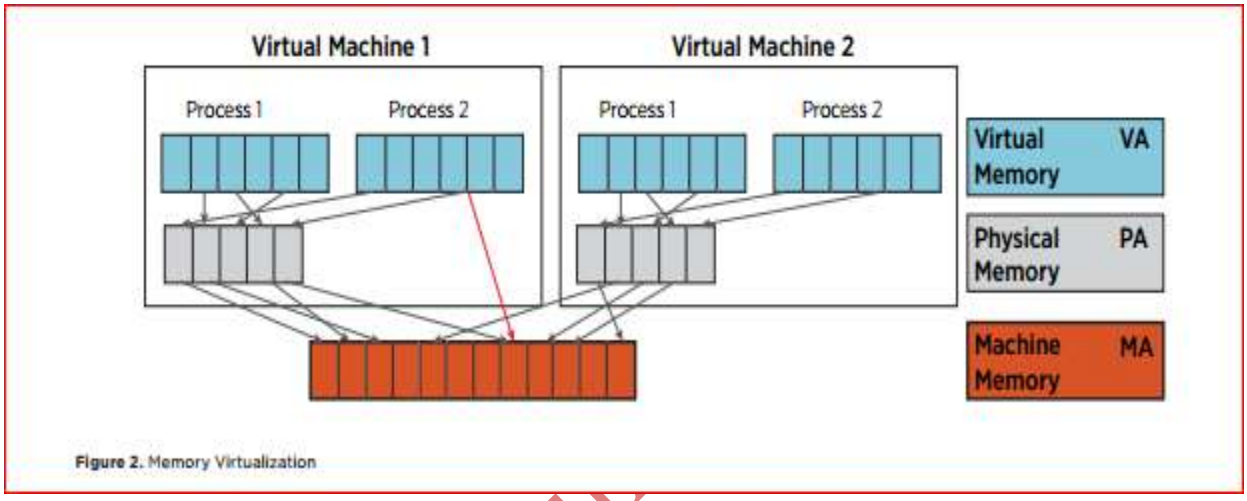

Fig 3*memory Virtualization*: (Adopted from Security of the VMware vSphere Hypervisor Article (2014). Retrieved from http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf).

Research Method/Design

The research method used is the Quantitative method with descriptive statistics. The reason I choose the descriptive statistics is that the conclusion of this research will be based on the secondary data collected. For example, this research study aimed at analyzing the risks of cloud computing and the skepticism of executives adopting cloud infrastructure. According to Leard Statistics (2013), "Descriptive statistics do not, however, allow us to make conclusions beyond the data we have analyzed or reach conclusions regarding any hypotheses we might have made." (para.2). Besides, the findings will be generalized because I used random sampling method for the population.

Population and Sampling Procedure

The population composed of 153-200 IT executives who are knowledgeable in the area of cloud computing and was randomly selected for the study. The sample size was made up of 153-200 IT executives as stated earlier.

Instrument/ Data Collection Techniques/ Analysis

I used secondary data collection technic. Data were collected using the internet sources. Data was analyzed using Megastats and Excel application software.

Data Collection

Table 1: Feds Hesitant Moving IT Services to the Cloud

Issues	Respondent
For control moving to the comfort Zone	Out of 153 IT executive surveyed found that only 44% of the agencies have "mature" data governance practice in the cloud.
When it comes to migrating applications to the cloud	89% are hesitant to lose control of their IT services, according to new survey.
When asked about transitioning IT services to the cloud	43% of the executives "Compared it to giving their son the key to a new convertible."
Comply with the Federal Risk and Authorization Management Program (FedRAMP)	Nine out of 10 agencies are taking steps to manage trust with their cloud vendors, such as keeping security functions on premise (42%) and requiring certification of security measures by cloud vendors (41%).
To address the challenges of datagovernance, agencies require enterprise-wide practices -- including documenting metadata, defining integration processes, and identifying data owners	Sixty-one percent of respondents said their agencies do not have quality, documented metadata; 52% don't have well-understood data integration; 50% haven't defined data owners; and 49% don't have known systems of record.

(Malykhina, E. (2014). Feds hesitate moving IT services to the cloud. Retrieved from http://www.informationweek.com/government/cloud-computing/feds-hesitate-moving-it-services-to-the-cloud/d/d-id/1315616)

Table 2: Top Concerns around Cloud Adoption

Concerns	**Weighted**
Cost	20%
Repudiation	18%
Privacy	14%
Loss of control of services and/or data	23%
Difficulty of Migration to the cloud	23%

(Secondary Data collected from Data-pipe on: Cloud Migration is the Leading Concern of CloudAdopters.https://www.datapipe.com/blog/2014/12/23/cloud-migration-is-the-leading-concern-of-cloud-adopters/).

Data Analysis:

Concerns	Weighted
Cost	20%
Difficulty of Migration to the cloud	23%
Loss of control of services and/or	23%
Privacy	14%
Repudiation	18%

Fig 2: Bar Chart Representing the concerns of the executives for adopting cloud computing.

Data Triangulation

Table 3: Mixed data

Top concerns Around Cloud Adoption			
1st.Concerns	**Weighted**	**2nd. Concern**	**weighted**
Cost	20%	For control moving to the cloud comfort zone	44%
Difficulty of Migration to the cloud	23%	Migrating to the cloud	89%
Loss of control of services and/or	23%	Transitioning IT services to the cloud	43%
Privacy	14%	Comply with federal risk and authorization management	42%
Repudiation	18%	Security	41%
		Quality, documented metadata	52%
		Data Integration	50%
		Organization that has known systems of record	49%

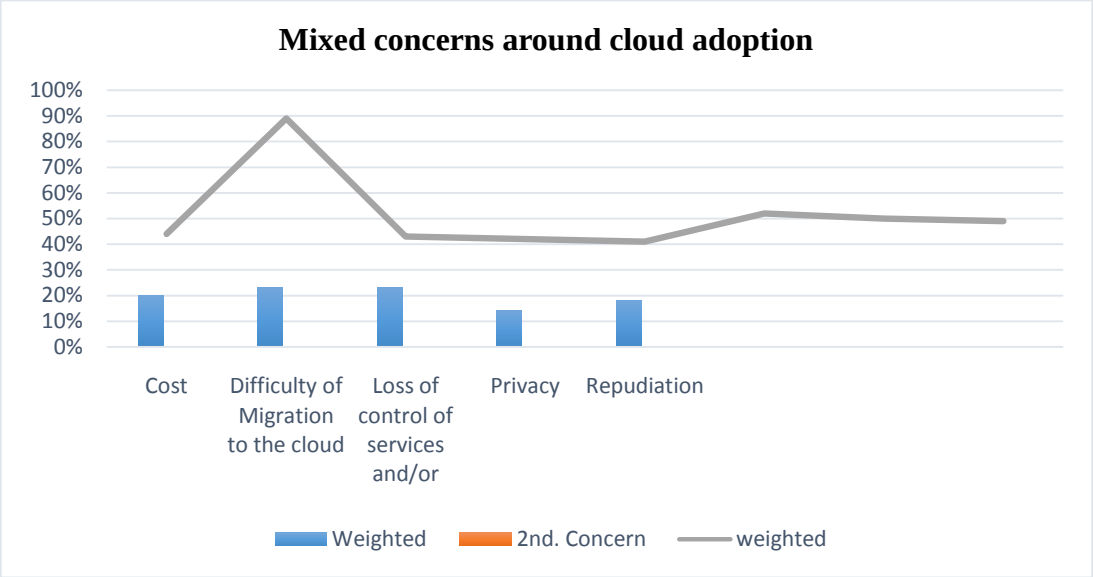

Fig3: Mixed concerns around cloud adoption

Fig 3 represents triangulated secondary data from Data-pipe and Malykina (2014). I observed that migrating to the cloud was a big concern for the IT executives. For example, out of 153 IT executive surveyed by Malykina (2014), about 89% stated that Migrating to the cloud were a big concern. Further, the data retrieved from *Datapipe*survey showed that 23% of the executives were very hesitant Migrating to the cloud. Evidently, about 44% and 23% of the participants from both data triangulated reflected that they didn't want to lose control of their data. Logically, this appears to be the major risk and hesitant of the executives migrating to the cloud. Based on the literature review for this study, (Malykhina, 2014), asserted that out of 10 agencies surveyed nine were taking steps to manage trust with their cloud vendors. These include keeping security functions in-house, which about (42%) of the participants agreed, and (41%)also agreed that certification of security measures by cloud vendors are required.

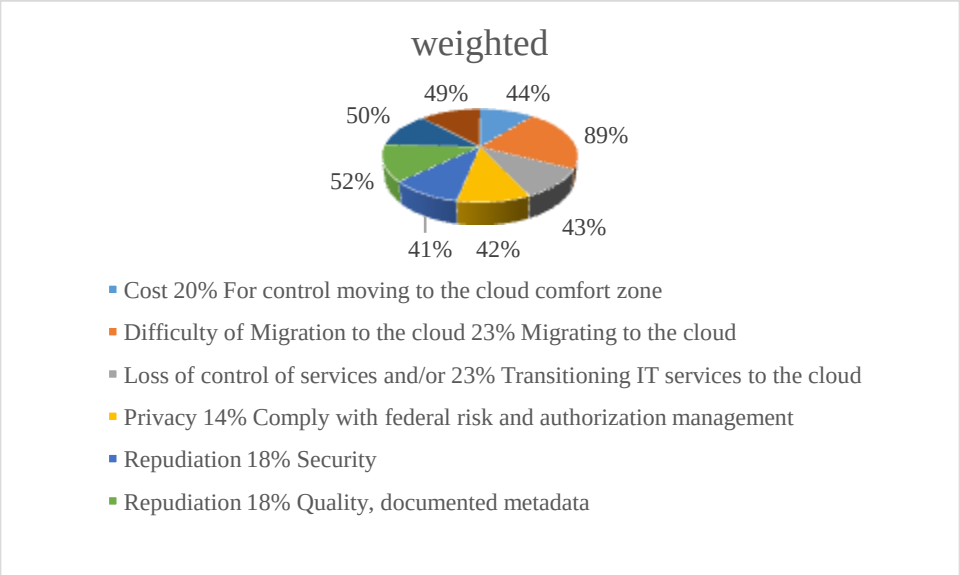

Fig 4: Representation of Data Triangulation in a pie chart

Fig 4 above, represent commonalties in terms of perceptions of the executives that participated in this survey during thetriangulation of data. The pie chat represents the weighted average of perceptions of the 153 executives surveyed. The legend data with different colors showed the corresponding perceptions of the analysiswith a quantifiable percentage.

Discussion

During the literature review, some of the major concerns why some executives were hesitant migrating to the cloud include; "Once data goes into the cloud you lose some control." (Cost low, 2015). This concern appears to be a plausible risk, and how can the data owner ascertain control? For example, cloud companies can have a data center in various locations or in another country where data governance may not uphold strict laws to protect the data. How can one ascertain that the data will be safe?

The second concerns are the virtualization: The virtualization has to do with the nature of allocating and de-allocating of resources such as local storage associated with Virtual Machine (VMs). According to this article, during the deployment and operation of a VM, data is written to physical memory. If it's not cleared before those resources are reallocated to the next VM, there's a potential for exposure based on VMware vSphere Hypervisor article 2014. Although, the article also, suggested that the memory isolation could solve the problem. According to Chan, Shing, Hung, Huang (2005), one possible method to enforce isolation would be the process of segment protection, where the processor's access to memory is possibly limited to one or more linear subranges of physical memory. The process of segments prevents that CPU from writing to the memory in each segment. The system will automatically show flags, which prevent the processor from writing to a particular segment or from executing code in that segment. Besides, it is one way of addressing the major concerns of data loss during the allocation of resources using virtualization. However, one of the dispiriting problems with virtualization is the data governance associated with Data location. Most executives are still skeptical more especially during this time that data breaches are on the increase. For example, when data breaches occur in one country or a location, there are always an accusing fingers, but often times ended up in not intercepting the hacker. According to a press release by Winton (2016), "Chino Valley Medical Center in Chino and Desert Valley Hospital of Victorville, both part of Prime Healthcare Services Inc., had their computer system compromised by a cyber-attack."(para.2). According to the reporter, the status quo was a ransomware, which is a program that prevented these hospitals' device from operating until a fee is paid. When something of this nature occur most managers appears to be more skeptical and preferred managing their data in-house despite the cost.

Recommendations

The recommendation to the executive of organizations that may be skeptical of migrating to

the cloud will be to adopt the Cloud as an infrastructure. In this type of cloud base system, the consumer does not have control of the underlying physical infrastructure but have control of the operating systems, deployed applications, storage, and possibly limited control of selected networking components. The reason for recommending infrastructure as a service is that the consumer can have some control of the data and also share some responsibilities as well.

Conclusion

Cloud computing appears to have numerous advantages over any storage systems. Besides, most managers in various organizations appear to be very skeptical migrating to the cloud despite the economic scale of cloud computing. The problem researched was to understand the skepticisms of the managers not willing to adopt the cloud infrastructure. In this research study, I reviewed some of the concerns of the executive being hesitant of migrating to the cloud. Based on the secondary data collected the executives were very skeptical migrating to the cloud. The possible reason as outlined was the loss of control of data, difficulties in adopting the cloud and lack of trust to the third party vendor managing data. However, I recommend that executives adopt infrastructure as services, and that appears to share some responsibilities from the cloud vendor while maintaining control of the data. Finally, more research is needed in this area to fill in the gap in security risk associated with data virtualization, which is cloud computing.

References

Costlow, T. (2015). Cloud computing gets more support, skepticism from design teams. Article *of Automotive engineering magazine*. Retrieved from http://articles.sae.org/13811/

Chan, W., Shing, E., Hung, J., & Huang, Z. (2005). Operating system Privilege: Protection and Isolation. Retrieved from http://www.read.seas.harvard.edu/~kohler/class/05s-osp/notes/notes9.html

Leard Statistics (2013). Descriptive and Inferential Statistics. Retrieved from https://statistics.laerd.com/statistical-guides/descriptive-inferential-statistics.php

Scudder, R (2011):Visualizing the Workings of Cloud Computing With Diagrams. Retrieved from http://www.brighthub.com/environment/green-computing/articles/127086.aspx
Security of the VMware vSphere Hypervisor article (2014). Secure Virtual Machine Isolation in Virtualization. Retrieved from http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

University of North Carolina, (2010). Determining the Sample size Retrieved from http://www.unc.edu/~rls/s151-2010/class23.pdf

Winkler, V. (2011). Cloud computing Virtual Cloud security concerns. Retrieved from https://technet.microsoft.com/en-us/magazine/hh641415.aspx

Winton, R. (2016). 2 more Southland hospitals attacked by hackers using ransomware. *Press Release.* Retrieved from http://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal- hospitals-ransomware-20160322-story.html

