THE INFLUENCE OF INFORMATION SECURITY ON THE ADOPTION OF CLOUD COMPUTING: AN EXPLORATORY ANALYSIS

[1]Omondi John Opala, Ph.D, [2]Shawon Rahman, Ph.D., and [3]Abdulhameed Alelaiwi, Ph.D

[1]Network Consulting Engineer, Cisco Networks System, USA
[2]Associate Professor, Dept. of Computer Science, University of Hawaii-Hilo, Hawaii, USA
[3]Department of Software Engineering, King Saud University, Riyadh 11543, Saudi Arabia

ABSTRACT:

Cloud computing is the current IT buzzword synonymous with outsourced data center management and agile solution architecture. It has the potential to improve scalability of large enterprise network delivery of services and the capability to revolutionize how data is delivered as a service. At its core, cloud computing is not a new technology but rather a new approach to distributed shared pooling of IT infrastructure linked together to offer centralized IT services on demand. The study results determined that management's perception of security, cost-effectiveness and IT compliance factors significantly influence their decisions to adopt cloud computing. The results of multiple linear regression analysis testing in this study showed that managements' perception of cost-effectiveness is more significantly correlated to their decision to adopt cloud computing than it is to security.

KEYWORDS:

Cloud computing,distributed computing, software as a service, infrastructure as a service, cloud security, and cloud compliance.

1. INTRODUCTION

The traditional network delivery method requires rigid capacity planning, which limits IT organization's ability to offer on-demand software management, rapid solutions provisioning and related IT services. The cloud-computing model has the potential to revolutionize information technology (IT) delivery service, but adds complexity in security, and IT compliance integration with an organization's procedures[1]. Cloud computing's elastic capabilities provide customers automatically with resources such as unlimited storage space, creating an illusion of unlimited network capacity and [2]availability. The need for cloud computing arises from the deluge of raw data, high availability, cost efficient IT delivery solutions, and demand for high compute intensive applications. The adoption of cloud [3]computing provides benefits to organizations that include pay-as-you-go billing, on-demand capabilities, and reduction in IT operational expense. The security risks associated with the existing cloud adoption model revolve around the issues of determining data ownership, confidentiality, integrity, privacy, and [4]virtualization.

DOI : 10.5121/ijcnc.2015.7404

A. Background of the Study

The phrase cloud computing, made public by Google's CEO Eric Schmidt, is a metaphor for the delivery of information technology (IT) shared [5]resources as a service to increase capacity and availability. The cloud computing model includes on-demand IT delivery services such as infrastructure, software, database and desktop services to IT organizations[6]. The National Institute of Standards and Technology sees cloud computing as a business model of enabling ease of on demand access to a pool of shared services,[7]which can be provisioned dynamically with minimal support[8].The cloud computing model essentially includes on-demand IT delivery services such as infrastructure, software, database and desktop services to IT organizations.

Most researchers define cloud computing[9]as an innovative way of enhancing the capacity to provide pay-as-you-go billing, on demand computing, IT utility, and automated delivery service. Other researchers contend that cloud computing is another iteration of IT outsourcing, which delivers applications and infrastructure services over the Internet, and introduces complexities to system integration and security vulnerabilities. Miller's [10] definition of cloud computing as the delivery of computational services on demand is consistent with previous definitions that highlight changes in IT delivery model that includes dynamic on demand provisioning of services as opposed to traditional non agile client server architecture delivery of applications that requires weeks of planning.The genius of cloud computing is that it combines utility computing, distributed computing and centralized data centers to deliver on demand service[11].The business case for cloud computing is its inherent ability to allow cloud providers to build out excess capacity for aggregate demand over scalable networking infrastructure. The ability of cloud computing to provide distributed systems consisting of virtualized resources, for dynamic provisioning based on user requirements on demand is arguably the main reason for its mainstream acceptance[12]. This ability enables an alignment between IT and business strategies for effective budget and resource allocation that leads to efficient support.

2. METHODOLOGY

The research design was non-experimental; however, the approach was quantitative exploratory. The instrument for the study survey was modeled after previously validated study instruments with five parts consisting of demographic information, management's perception, security, cost effectiveness, and IT compliance[13].Exploratory factor analysis was used to explain the existence of dependency among perceptions of cloud adoption, cloud security, cost effectiveness, and IT compliance variables being measured by the survey instrument. Factor analysis reveals the structure of variables, and reduces independent variables to a manageable size by determining their relationship to the dependent variable, which relationship is the perception of cloud adoption in this study, while leaving the original design intact to test for negative correlation[14]. Negative Cronbach's alpha can be realized as a resultof a reverse phrase in an item or rewording of a question, and is used to reduce response bias.

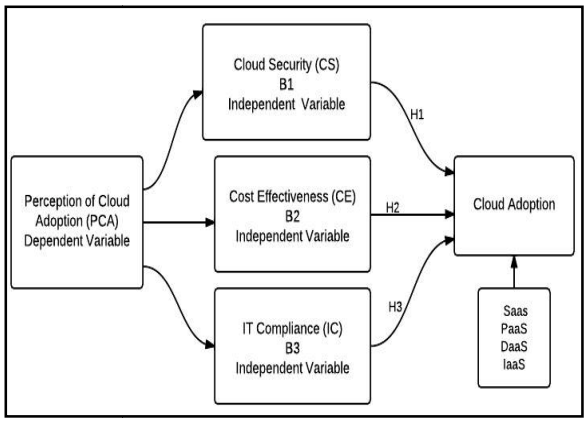

Table 1: Variable Name

Variable Name	Variable Type	Variable Code	Data Type
Perception of Cloud Adoption	Dependent	PCA	Ordinal
Cloud Security	Independent	CS	Ordinal
Cost Effectiveness	Independent	CE	Ordinal
IT Compliance	Independent	IC	Ordinal
Demographic	Independent		Ordinal/Interval

A. Population and Sample

The population for this study included chief information officers (CIO), IT managers, IT directors, operational managers, and other managers who are responsible both for technology acquisition and policy decisions for enterprise companies within the U.S. This study used a probability systematic sampling method. A sample is a representative selection of a small group for the purposes of studying the larger population.

A sample size of 268 [15]was deemed acceptable for achieving reliability as long as it is representative of the entire population; however, the researcher received 282 completed surveys, thereby increasing the validity and reliability of the results. In multiple regression analysis, the sample size is dependent on the desired power of the study, the number of independent variables used in the instrument, and the effect size, which is the relationship between independent and dependent variables.

B. Instrument and Measures

The instrument for the study questionnaire was adapted from the previous study scale developed by Davis with five parts consisting of demographic information, management's perceptions, security, cost effectiveness, and IT compliance[16].The technology adoption instrument used was

validated using discriminant, convergent, construct and face validity based on a multitrait-multimethod (MMT) analysis of validity consistent with the TAM studies. The test for validity showed that there was a high, statistically significant inter-correlation between items ($p < .005$) based on the original study on adoption and technology acceptance byVenkatesh[17].

The instrument employed a five-point semantic differential Likert scale with values ranging from 1 Strongly Disagree to 5 for Strongly Agree. The Likert scales were used to measure managers' perceptions of or attitudes towards factors influencing cloud adoption. Likert scales are used in surveys for measuring attitudes, opinions, and dispositions by asking a user to make value judgments, which is relevant in studying factors influencing cloud adoption by IT managers. Data was analyzed using a multiple linear regression data analysis predicated on PCA = a + b1 + b2 + b3+e, where "a" is the constant, "b" are the regression coefficients, and "e" is the amount of error not explained by the model. In order to test all three hypotheses, only one regression model was necessary.

Data was also examined for normality with skewness and kurtosis statistics[18].In SPSS version 19.0, Skewness and Kurtosis values between -2 and +2 are considered to approximate normal distributions. A power analysis was conducted using G Power 3.1. Validity in quantitative research describes the degree to which assumptions and constructs being measured are accurately presented. The test for validity was required to measure consistency and reliability of results as a prerequisite for the studies replication in order to get the exact same results[18].To assess the reliability of the data analysis, the researcher used Cronbach's alpha to explain the means versus medians and ranks. The reliability of the scales tested by Cronbach's alpha is considered to show a strong reliability with 0.788 for alpha. The reliability coefficient ranges from zero to one (0-1), and a statistical value of .70 or better meets reliability requirements based on Cronbach's alpha[19].

3. CLOUD COMPUTING ADOPTION MODELS

The term "adoption" is used here to define the initial decision regarding whether or not to use a technology service. IT adoption continues to fascinate many researchers, especially those interested in understanding factors that influence organizational leaders' decisions to adopt technology. Adoption theory is relevant in this research because it examines individual's or business leaders' decisions to adopt or not to adopt cloud computing for integration into the organization[20].IT researchers use the terms adoption, acceptance, and diffusion of technology interchangeably to identify positive decisions to implement new technologies, but adoption is most prevalent in empirical studies[21]. According to Davis, the reasons why individuals accept or reject technology has challenged information system researchers for some time, but recent adoption studies have achieved notable success in coming to understand the relevant factors.

The objective of adoption theory is to provide technology adopters with sufficient data to predict whether the systems will in fact enhance IT delivery and improve business processes[25]. Rogers argued that technology acceptance is related to users'perception that is relevant to understand and predict adoption [26]. Nguyen suggested that IT adoption in many organizations happens without proper planning and, as a result, produces a low percentage of successful integrations.

There are three types of cloud-based solutions providing various services: public, private, and hybrid cloud. Public clouds are network infrastructures designed to provide software access through web based portals. Private clouds mimic an internal network with encryption and security measures to restrict access to only authorized customers. Private clouds are proprietary

infrastructures that are wholly operated for an organization to offer secure computing services either on the organization's premises, or they are operated by third party vendor offsite. Cloud computing allows for computing resources to be distributed across regional locations for seamless access as federated private cloud. The hybrid cloud is a combination of private, community, and public delivery of IT services[27].

Cloud computing introduces an on-demand model of software and application delivery which integrates IT with business strategies. The cloud model integrates effective use of shared multi-tenant resources, software packing, on-demand provisioning, and flexible pricing by leveraging the Internet as a platform. The cloud computing model changes the way data is stored and shared, using virtualization to increase availability. Cloud computing solves the problem of limited access to data resources, and lack of agility in client-server data delivery architecture.

In a study on parallel computing, it was found that the cloud model allows for allocation of resources in minutes as opposed to the hours or days that traditional provisioning of applications could consume by virtue of its reliance on queue-based job scheduling. The cloud model provides benefits such as reduced costs of operation to users, and economies of scale to the cloud providers. Also, a study on the type of operating systems that enable cloud delivery concluded that virtualization of computer resources for multi-tenancy delivery is flexible, and that it meets economy of scale requirements for cloud providers, while at the same time remaining cost effective for cloud adopters[28].The cloud platform model is a set of operating systems that runs on the cloud to provide software as a service, platform as a service, infrastructure as a service, and capabilities for scaling up for peak service delivery to millions of users.The three common cloud adoption models are SaaS, PaaS and IaaS.

Software as a service is an application delivery concept that provides pay-as-you go pricing structure for software licenses and access for users instead of either the traditional local install on computers or a delivery through client server network model. In the software as a service model, cloud vendor service providers supply the hardware, network architecture and applications. Providers connect to the customer through a web portal or third party middleware. This model, therefore, excludes customers from installing and running applications on local computers, which in turn reduces the cost burden of licensing, application maintenance and purchases by on-demand pricing.

Software as a service promises to increase flexibility of application installations and to reduce cost by eliminating license fees, hardware cost and maintenance cost associated with traditional client-server software deployment. The software as a service model introduces leasing application through the Internet to users as a service. These include services such as those offered by Salesforce.com, Google Docs and Yahoo's use of Apache Hadoop to provide thousands of users' access to data. The SaaSphenomenon, however, has created security distrust in organizations due to unintended consequences of putting all the organization's applications in the care of external rather than internal resources.

Platform as a service is an application development solution offered by cloud providers that includes operating systems and development tools. These tools can be accessed to manage infrastructure applications such as Microsoft's Windows Azure, Cisco WebEx Connect and Intuit's partner platform for financial services. Also, platform as a service offers ready to use application components that can be dynamically assembled by users into a complete application

on demand such as Google Apps and Cisco's WebEx connect. This feature,because of the underlying application infrastructure components, which includes application servers, middleware, and application frameworks, reduces the time it takes organizations to develop new applications. The service providers for platform as a service gain competitive advantage based on their range of applications, the efficiency of developing such applications, and the size of third party developers.

Infrastructure as a service provides compute and resource access on demand for customers. A computational service consists of CPUs, hypervisors and utilities. Resource allocation includes effective delivery of virtualized environments. The cloud infrastructure includes storage area networks, virtualized services for computing power, data center networks, disaster recovery services, and the required staff to keep the services operational.Infrastructure as a service, therefore, is the commoditization of IT infrastructure resources as an on demand service to organizations. The infrastructure resources constitute a centralized remote virtualized data center that can be accessed by organizations on demand, based on need. The use of cloud infrastructure enables organizations to re-direct resources to long-term strategic business goals while outsourcing the day to day IT functions, such as archiving and business continuity to cloud providers. The most noticeable infrastructure as a service example is Google's App Engine that allows customers to subscribe to an on demand infrastructure with defined hardware, software, applications and data access configurations.

A. Cost-Effectiveness and Economies of Scale

The economics of cloud service delivery reflects a paradigm shift in the ways IT has been delivered, from a product to a service orientation based on customer need. The availability of on demand IT services through shared resources creates economies of scale to cloud service providers that allows for delivery solutions which otherwise would not be feasible for most organizations. The paradigm shift in organizations' IT assets from commodity to services allows for cataloging application dependencies for delivery as a service. The adoption of cloud resources can save companies millions of dollars, and organizations are adopting cloud services because of such differentials. This study reinforces that idea that cloud adoption has benefits more far reaching than just cost effectiveness. Cloud services have the potential to revolutionize the way in which IT is delivered, and to create new business sectors in the same manner as did the Internet in its formative years.

The cost-benefit paradigm has been used in previous IT research to correlate adoption and ease of use, and, thereby, to explain how decision makers alter their adoption strategies based on cost. It can be argued that cloud computing adoption leads to both cost savings and risk mitigation, since there is no need for hardware acquisition and, thus, no need to place capital expenditures at risk in large infrastructure deployments.

Two of the known economic benefits of cloud computing are its ability to eliminate infrastructure acquisition costs, and to improve operational efficiencies. The cost effectiveness of the cloud, however, lies in the pool of shared resources that allows for lowered cost of delivery since one server can host hundreds of customers. The sharing of computational resources allows users to amortize the costs of software and hardware. The cloud service providers, however, must be able to develop computational resources of sufficient size to be able to realize the benefits of economies of scale.

The value proposition of cloud lies in the absence of required upfront cost for hardware, software, networks, staff, training and other traditional network infrastructure needs. Cloud computing provides economies of scale for cloud service providers by creating on demand computing instances at lower costs because neither hardware purchase nor installations are necessary. The cloud providers can invest in large IT hardware acquisitions to the extent of $500 million per data center. The providers use multi-tenancy on limited resources to keep down the cost of hardware while the cloud users benefit from cheap and quick access to these resources.

The current economic decline has led to institutional and corporate budget reductions. The fact that cloud computing's adoption can be accomplished with little, if any, upfront capital allows organizations to procure cloud's unique services. These services include the opportunity for the user to add or remove IT infrastructure services during peak hours while only paying for used capacity.

B. Security factors

Information security attacks on vulnerable systems began in the 1980s with boot viruses transferred through infected floppy diskettes[30]. The attacks were limited in scope with no service impact to the systems, and with limited repair costs compared to the prohibitive repair costs of today's network attacks, which can paralyze entireinfrastructures. The time has long since passed when such attacks were nuisances created by computer technicians showing off their programming skills. Attacks have now evolved into criminal enterprises and cyber warfare causing destruction and impacting audiences on a world-wide scale.

An information security standard and process for enterprise organizations consists of rules for confidentiality, integrity and availability. Information security is always associated with prevention and detection of unauthorized activities in the networks or systems, and requires business to institute relevant strategic policies[29].Effective information security management correlates decisions with business processes within the organization to determine risks, mitigation measures, and relevant enterprise business strategies.

The complexity and anonymity of cloud network access over the Internet poses the gravest risk to IT infrastructure because vulnerabilities in virtualization and multi-tenant features can inflict maximum interruption to network resources when such interruptions are least expected. Security in the cloud, therefore, requires the correctness and effectiveness of multiple network components working together in a multi-tenant infrastructure shared with unknown third parties. The traditional network security delivery requires rigid capacity planning, thereby limiting the ability to offer on-demand software management and related IT services [30].The cloud-computing model improves IT delivery service, but adds complexity to security management and IT compliance integration within an organization's procedures.

The migration of data from standard network architectures to cloud supported solutions, though gaining acceptance in the marketplace, exposes data to many vulnerabilities such as data ownership and protection roles. The dispersion of data across multiple data centers allows cost savings and performance enhancements, but opens the door for exploitation in countries that lack privacy laws[31].The flexibility of cloud's pay per service is a cost motivation for adoption, but the movement of applications from one network to another endangers security and trust in the confidentiality and integrity of data. This is because cloud computing uses virtualization to share resources on one host to multiple customers, which introduces new security weaknesses.

Information security within the cloud model requires understanding of the organizational data privacy needs in order to assign correct physical, procedural, hardware, software, and personnel countermeasures. Cloud computing encompasses multiple technologies, including networks, databases, operating systems, and virtualization. Related security issues within the context of a complexintegration of these technologies. Information security involves an effective process of managing technology, frameworks, protocols, applications, physical environments and users to foster effective measures of system security[32].The security process includes risk identification, technical solutions, governance and user awareness training. The increase in attacks and economic risks associated with the exploitation of vulnerability has led to the creation of security governance as part of the organizational structure.

According to Drugescu and Etges[35], it is vital for an organization to build an information security portfolio, and to identify those areas of a business that, if compromised, pose the greatest risk to the business. The evaluation process identifies threats in an organization, existing vulnerabilities, the likelihood of attack, and the effectiveness of the existing control mechanisms. Based on the findings, an information security program can be designed to secure sensitive and critical data. Information security involves more than processes, technical solutions (firewall, intrusion detection systems, biometrics, firewalls), and people. It also involves an enterprise-wide security strategy to orchestrate these various elements.

The biggest challenge with security in the cloud is the delegation of confidentiality, integrity, and availability of data to third party vendors. The security of the cloud is complicated because of the multi-tenancy of the virtualized resources. Some providers restrict privileged access to hardware to vital parts of the infrastructure, but the fact that the administrator may still have unlimited access to multiple customer's VM-machines will continue to expose users to security vulnerabilities[33].

According to Furht and Escalante, the fact that virtual machines contain critical applications and sensitive data in a shared environment is the single source of security vulnerability that cloud customers fear most. The lack of traditional perimeter firewalls, demilitarized zones, network segmentation, and standard network monitoring tools increase the security vulnerability. Cloud computing security risks are evident in the collocation of multiple virtual machines on the same server, running the same operating systems and managing multiple servers. The exploitation of a known weakness on such an operating system risks all client data.

Studies suggest that security deterrence for cloud adoption at the enterprise level of organization lies with confidentiality and integrity of data at the cloud service provider's network. However, an argument exists that a trusted computing platform can be used to provide closed box execution by guaranteeing the security of the service before the commencement of operation. One study of cloud security by Letaifa determined that the use of a trusted computing platform increases security and confidentiality of virtual machines, but cloud customer will have to manage the security of their own networks[35].

Cloud computing, by definition, is a multi-tenant occupancy, with other users on the same hardware resources. Such a design necessarily introduces the risk of exposing sensitive information to unauthorized users. The shared components, such as central processing unit, caches, and storage that make up the underlying infrastructure as a service fabric are not suitable

by design to offer security isolation for multi-tenancy. Some studies argue that a virtualization hypervisor addresses the security gap by mediating access between guest operating systems and the physical computing resources. The use of virtual machines also affects the generation of cryptographic keys between the host and guest operating systems on the shared host. The cloud's use of small key sizes for encryption reduces the strength of the cryptographic operations performed in the cloud environment, thereby increasing the risk of exposure by cryptanalysis and decryption.

Information owners do not control the hardware resources used to operate on their information, and must rely on the virtualization to provide the security needed to protect this information [34]. According to Gill, the adoption of cloud computing enhances IT performance delivery, but adversely impacts information security. Hackers and cyber based attacks gravitate more towards the large targets of opportunity that cloud service providers seem to make available. It is, therefore, necessary to take security precautions when designing cloud deployments. Enterprise organizations cede control to cloud providers, thereby creating a gap in security defenses. Cloud providers limit application portability and the customer's right to migrate from one provider to another. Most cloud providers host multiple customers' data, which creates risks of guest-hopping attacks on memory, storage and routing between two tenants.

C. IT Compliance

IT compliance consists of organizational policies and procedures to meet regulatory requirements for the violation of which there arepenalties. Sentencing guidelines for violation vary but may range from fine to imprisonment, or both. Compliance regulatory organizations enforce such policiesby regular audits to encourage organizations to act responsibly. IT compliance for cloud-enabled networks includes (1) internal IT processes, such as system logging, log analysis, authentication, authorization, and (2) archiving, back-up, data life cycle, data retention, archival and physical security of servers in the cloud.

Compliance risks associated with IT have been prevalent in outsourced services. The recent increase in the number of data security breaches and system failures on Amazon EC2, for example, has made compliance requirements a priority consideration for cloud adoption. The shared resources nature of cloud computing hinders compliance processes because multiple customers use the same resource to access their data. In cloud computing, the compliance assurance process is not clear when data ownership and storage locations are not under the control of the enterprise organization.

The success of cloud computing also introduces privacy and confidentiality risks to users of cloud computing resources; such risks have led to data protection legislation with civil and criminal sanctions. Cloud services consumers are concerned about data security and privacy since service providers use multi-vendor tenancy on individual resources. Cloud solutions provide ease of access to data from any computer using the Internet without expensive upfront cost in acquiring hardware. Precisely these virtues, makes it easy for organizations to violate data privacy laws and regulations that affect IT compliance requirements for regulations, such as the Health Insurance Portability and Accountability Act and Sarbanes-Oxley.

Customers expect cloud computing service providers to abide by the laws and regulations of specific countries to protect data privacy from unauthorized disclosures. Cloud computing, however, is still in its infancy stages, and lacks coherent policy on privacy and compliance. Thus, every cloud service provider has its own individual compliance white papers to present to potential customers. In order for cloud service providers to meet regulatory requirements, internal IT processes such as system logging, log analysis, authentication, authorization, and archiving, back-up and physical security of servers in the cloud have to be maintained.

4. STUDY RESULTS

The rationale for this research was to determine the influence of the three constructs security, cost effectiveness, and IT compliance on managers' decision to adopt cloud computing using a quantitative exploratory research method. The results of the study are presented below.

There were a total of 282 participants for this study; 54.3% (N = 153) males and 45.7% (N = 129) females. Regarding age group, 28.4% (N = 80) were 18-35; 37.9% (N = 107) were 36-49; and 33.7% (N = 95) were 50-65 years of age. Concerning educational attainment, 49.3% (N = 139) had bachelor degrees; 24.8% (N = 70) had master degrees; and 8.2% (N = 23) had high school diplomas. Highest level of education completed.The results of demographic analysis shows that the largest group of IT professionals who participants in the survey included IT/IS Managers (44.7%, N = 126); IT/IS Professionals (19.9%, N = 56); IT/IS Team Leader (16.0%, N = 45); and "Other" (8.2%, N = 23), which consisted of business managers, analysts, computer technicians, etc. Approximately 35% (N = 98) of respondents had at least two years of experience in implementing cloud-computing technologies; 12.1% (N = 34) had 2-5 years; and 16.7% (N = 47) had 5-10 years. Approximately 31% (N = 87) of respondents' organizations support less than 500 users; 12.4% (N = 35) support 501-1000 users; and 22.3% (N = 63) support 1001 to 5000 users.

Table Ii: Occupational Title

Occupational Title	*N*	%
Chief Information Officer	4	1.4
Chief Security Officer	1	.4
Director of IT/IS	18	6.4
IT/IS Manager	126	44.7
IT/IS Professional	56	19.9
IT/IS Team Leader/Supervisor	45	16.0
Solutions Architect	2	.7
Vice President of IT	7	2.5
Other, please specify	23	8.2
Total	282	100.0

Note.Other = business managers, operation managers;*IT* = information technology.

The largest primary business or industry of respondents' organizations included IT-Services (21.3%, N = 60), followed by "Other" (18.4%, N = 52). Education (9.9%, N = 28) and Services/Banking (9.6%, N = 27) were approximately equal. Other businesses or industries were categorized as manufacturing, retail, insurance, and aerospace.

Table Iii: Primary Business Or Industry Of Organization

Business or Industry	*N*	%
Construction	6	2.1
Education	28	9.9
Energy/Utilities	8	2.8
Financial Services/Banking	27	9.6
Government	25	8.9
Health Care Services	24	8.5
IT – Manufacturing	15	5.3
IT-Services	60	21.3
Manufacturing (Auto)	4	1.4
Professional Business Services (Non-IT)	17	6.0
Telecommunications	15	5.3
Travel/Leisure/Hospitality	1	.4
Other, please specify	52	18.4
Total	282	100.0

Note. Other = manufacturing, retail, insurance, aerospace; IT = information technology

The descriptive statistics for variables thatwere addressed in study are grouped by subscales. In order to compute the scores on the survey instrument, item 10 was reverse-scored. Then, the subscale scores were computed by summing the corresponding items. Scores ranged from 4-20 on all four subscales.

Table Iv: Descriptive Statistics

Subscales	*N*	*Minimum*	*Maximum*	*M*	*SD*
Cloud Security	282	4.00	20.00	11.52	2.70
Cost Effectiveness	282	4.00	20.00	13.69	2.72
IT Compliance	282	4.00	20.00	12.64	2.99
Perception of Cloud Computing Adoption	282	4.00	20.00	13.48	3.19

Note. IT = information technology

A. Reliability and Coefficients

The data were screened for normality with Skewness and Kurtosis statistics to determine a frequency distribution. Skewness values ranged from -.451 to -.158 whereas Kurtosis values ranged from .471 to 1.86. Skewness and kurtosis values between -2 and +2 are considered to approximate normality; therefore, the data were normally distributed.

Table V: Skewness And Kurtosis Statistics

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
Cloud Security	282	-.270	.145	.471	.289
Cost Effectiveness	282	-.451	.145	1.86	.289
IT Compliance	282	-.158	.145	.735	.289
Perception of Cloud Computing Adoption	282	-.395	.145	.479	.289

Note. IT = information technology

Reliability coefficients on the survey instrument ranged from .701 for cloud security to .896 for IT compliance with an overall reliability of .937. The CIO/IT managers' perceptions of security, cost-effectiveness, and IT compliance were significantly related to his or her decision to adopt cloud computing, $F(3, 278) = 197.60$, $p < .001$; $R2 = .681$. The achieved power for the regression analysis is 100%. To address each research questions the following hypotheses were tested.

Table Vi: Reliability Of Coefficients

Scale	*N* of Items	Cronbach's alpha
Cloud Security	4	.701
Cost Effectiveness	4	.881
IT Compliance	4	.896
Perception of Cloud Computing Adoption	4	.882
All Items	16	.937

Note. *N* = number of times

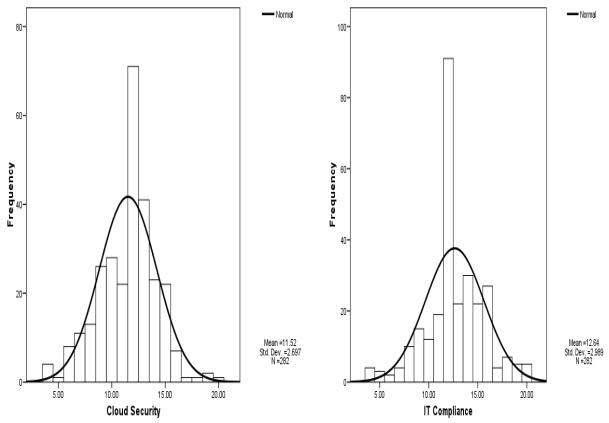

Figure 2. Histogram of cloud security and IT compliance.

B. Research Question and Hypothesis Testing

Three research questions and corresponding hypotheses were adapted from existing studies for this examination. The Pearson Product Moment Correlation (Pearson r) examined the hypotheses. Correlation does not indicate causality since no variables are controlled. Therefore, multiple regression investigated the research questions as it controlled for other variables. The research questions were as follows:

1. Do the CIO/IT managers' perceptions of security affect their decisions to adopt cloud computing?
2. Do the CIO/IT managers' perceptions of cost-effectiveness affect their decisions to adopt cloud computing?
3. Do CIO/IT managers' perceptions of IT compliance affect their decision to adopt cloud computing?

Based on the research questions, the following hypotheses were tested:

Hypothesis 1

H01: There is no correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding cloud security. There was a moderate, positive correlation between CIO/IT managers' decisions to adopt cloud computing and their perception regarding cloud security, $r = .672$, $N = 282$, $p < .001$, two-tails. Therefore, the null hypothesis is rejected. As CIO/IT managers' decisions to adopt cloud computing increased, there was a corresponding increase in their perceptions of cloud security.

Ha1: There is a correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding cloud security. There was a moderate, positive, significant correlation between CIO/IT managers' decision to adopt cloud computing and their perceptionsregarding cloud security, $r = .672$, $N = 282$, $p < .001$, two-tails. Therefore, H01 is rejected.

Hypothesis 2

H02: There is no correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptions of its expected cost effectiveness. There was a significant, strong, positive correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptions regarding its expected cost effectiveness, $r = .704$, $N = 282$, $p < .001$, two-tails. Therefore, the null hypothesis is rejected. As CIO/IT managers' decisions to adopt cloud computing increased, there was a corresponding increase in their perceptions of its expected cost effectiveness.

Ha2: There is a correlation between CIO/IT managers' decisions to adopt cloud computing and their perception regarding its expected cost effectiveness. There was a significant, strong, positive correlation between a CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding its expected cost effectiveness, $r = .704$, $N = 282$, $p < .001$, two-tails. Therefore, H02 is rejected.

Hypothesis 3

H03: There is no correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding IT compliance. There was a significant, strong, positive relationship between CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding IT compliance, r = .756, N = 282, p< .001, two-tails. Therefore, the null hypothesis is rejected. As CIO/IT managers' decisions to adopt cloud computing increased, there was a corresponding increase in their perception regarding IT compliance.

Ha3: There is a correlation between CIO/IT managers' decisions to adopt cloud computing and their perceptionsregarding IT compliance. There was a significant, strong, positive relationship between CIO/IT managers' decisions to adoptcloud computing and their perceptionsregarding IT compliance, r = .756, N = 282, p< .001, two-tails. Therefore, H03 is rejected.

Regression Analysis

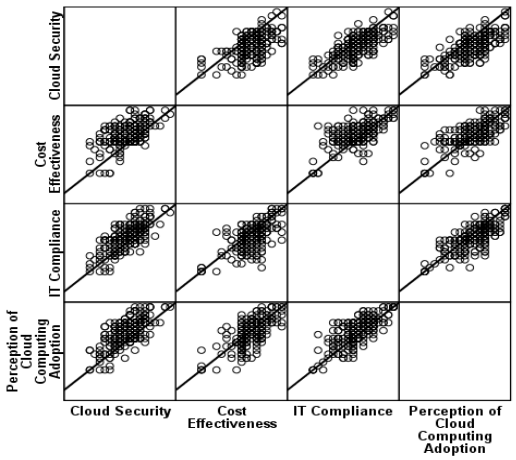

Figure 4: Scatterplot of variables.

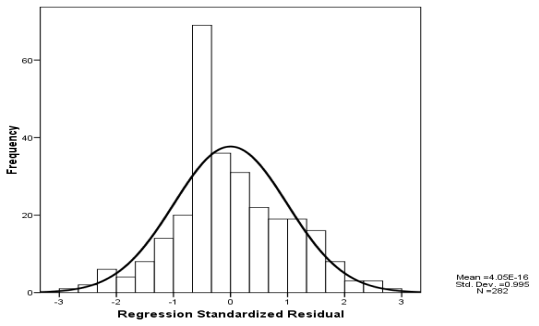

Figure 5. Histogram of regression

The three research questions were investigated with regression analysis predicated on PCA = a + b1(CS) + b2(CE) + b3(IC)+e, where "a" is the constant, b are the regression coefficient, and "e" is the amount of error not explained by the model. One regression model examined the

relationship. Prior to the analysis, the data were checked to determine whether it met the assumptions of multiple regression analysis. For example, linear multiple regression assumes that relationships between the independent and dependent variables are linear. The linearity of the relationships was examined with a scatterplot.

A second assumption of regression analysis is that the residuals are normally distributed. A residual is the difference between the observed and model-predicted values of the dependent variable. A histogram examined the normality of the residuals. As indicated in Figure 8, the residuals were normally distributed.

The ANOVA for the model was statistically significant, F(3, 278) = 197.60, p < .001; R2 = .681. The CIO/IT managers' perceptions of security, cost-effectiveness, and IT compliance were significantly related to their decisions to adopt cloud computing.

Table Vii: Regression Coefficients

Predictor Variable	***R***	***R*²**	**Adj. *R*²**	***B***	**SE *B***	**β**	***t***	***p***
	.825	.681	.677***					
Cloud Security				.270	.057	.228	4.71	.000***
Cost Effectiveness				.413	.052	.352	7.97	.000***
IT Compliance				.395	.058	.370	6.87	.000***

Note. *Dependent variable* = perception of cloud computing adoption. ****p*< .001.

A summary of the hypotheses shows that the three null hypotheses were rejected.

TABLE VIII: Summary of Hypothesis

Hypothesis	**Significance**	**Null Accepted or Rejected**
$H_0$1: There is no correlation between a CIO/IT manager's decision to adopt cloud computing and his/her perception cloud security.	*p*< .001	Null rejected
$H_0$2: There is no correlation between a CIO/IT manager's decision to adopt cloud computing and his/her perception of its expected cost effectiveness.	*p* < .001	Null rejected
$H_0$3: There is no correlation between a CIO/IT manager's decision to adopt cloud computing and his/her perception of IT compliance.	*p*< .001	Null rejected

A post hoc power analysis was conducted on the regression analysis. With the number of predictors (n = 3), the sample size (N = 282), and the adjusted R2 of .677, the achieved power is 100%.

5. CONCLUSION

The study determined that management's perceptions of security, cost-effectiveness, and IT compliance factors significantly influence the decisions whether to adopt cloud computing which is consistent with finding in prior research. Also, the regression testing showed that cost-effectiveness had a greater correlation with the decision to adopt cloud computing than did security[35]. The cost-effectiveness paradigm has been used in previous IT research to correlate adoption and ease of use and, thereby, to explain how decision makers alter their adoption strategies based on cost.The results of this study indicate that cost-effectiveness has a strong positive correlation to managements' decision to adopt cloud computing, which is consistent with previous studies on technology adoption[36]. In a similar study on adoption of cloud computing for radio frequency identifier support found that integration with cloud infrastructure leads to cost reduction for now familiar reasons, namely, cloud computing introduces access on demand while eliminating upfront costs. The flexibility of cloud's pay per service is a cost motivation for adoption, but the movement of application from one network to another endangers security and trust in the confidentiality and integrity of data. This researcher argues that the reason for the significant correlation is due to perception of expected cost savings as a result of cloud adoption.

The decision to adopt cloud computing is based on the characteristics of technology such as security, cost effectiveness, ease of use, usefulness and the need for such technology. A study on the type of operating systems that enable cloud delivery concluded that virtualization of computer resources for multi-tenancy delivery is flexible and meets economy of scale requirements for cloud providers, while at the same time remaining cost effective for cloud adopters.

The implication of this research finding is that IT managers are more likely to adopt cloud computing if they expect it to be to be secure, cost-effective and responsive IT compliance requirements. Cloud service providers should consider the evaluating factors that influence adoption of cloud computing, especially the expected cost-effectiveness benefits, security, and IT compliance organizations. This finding should also assistin the decision-making process for managers considering adoption of cloud technologies. The results also highlight risks and benefits associated with cloud adoption, providing additional information that can be useful to IT management and cloud providers in strategic planning. In sum, the study providesempirical evidence of the extent to which cloud security, cost-effectiveness, and compliance influence management decisions to adopt cloud computing.

6. REFERENCES

[1] F. Lombardi and R. Di Pierto, "Secure virtualization for cloud computing," J. of Network and Comput. Applicat., vol. 34, no. 4, pp.1113-1122, Mar. 2011.
[2] M. Armbrust et al., "A View of Cloud Computing," Commun. of the ACM, vol. 53, no. 4, Nov. 2010.
[3] J.E. Anderson and H.P. Schwager, "SME adoption of wireless LAN technology: Applying the UTAUT model," in7th Annu. Conf. of the Southern Assoc. for Inform. Syst., New York, NY 2004.
[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. of Network and Comput. Applic., vol. 34, pp.1-11, Jan. 2011.
[5] C. Davidson, "Cloud control," Risk, vol. 23, no. 10, pp. 70-78, Mar. 2010.
[6] H. Katzan, "Identity and privacy services," J. of Service Sci., vol. 3, no. 2, pp. 1-13, Feb. 2010.

[7] W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing,. NIST, vol. 800, no. 144, pp. 1-60, Nov. 2011.
[8] H. Du and Y. Cong, “Cloud computing, accounting, auditing, and beyond certified public accountant," The CPA J., vol.8, no. 10, pp. 66-70, Jan. 2010.
[9] A. Ahmed, “Using COBIT to manage the benefits, risks and security of outsourcing cloud computing,”COBIT Focus, vol. 2011, no. 2, pp.1-9, Jun. 2011.
[10] H. Miller and J. Veiga, (2009). « Cloud computing: Will commodity services benefit users long term? » IEE Comput. Soc., vol.1520-9202, no. 9, pp. 57-64, Apr. 2009.
[11] K. Kushida, J. Murray and J. Zysman, “Diffusing the cloud: Cloud computing and implications for public policy,”J. Ind. Compet. Trade, vol 5, no. 5, 1-30. Jul. 2010.
[12] Y. Dwivedi and N. Mustafee, “It's unwritten in the cloud: The technology enablers for realising the promise of cloud computing,”J. of Enterprise Inform. Manage., vol. 23, no. 6, pp. 673-679, Jan. 2010.
[13] A.R. Swanson and F.E. Holton, Research in organizations: Foundations and methods of inquiry. San Francisco, CA: Berrett-Koehler Publications, Inc., 2005.
[14] P.W. Vogt, Quantitative research methods for professionals. Boston, MA: Pearson Education, Inc., 2010.
[15] J.C. De Winter, D. Dodou and A.P. Wieringa, “Exploratory factor analysis with small sample sizes,”Multivariate Behavioral Research, vol. 44, pp.147-181, Mar. 2009.
[16] D.F. Davis, P.R. Bagozzi and R.P. Warshaw, “User acceptance of information technology, system characteristics, user perceptions and behavioral impacts,”Int. J. of Man–Machine Stud., vol. 38, no. 3, pp. 475–487, Aug. 1993.
[17]V. Venkatesh and H. Bala, “Technology acceptance model 3 and a research agenda on interventions,”Decision Sciences, vol. 39, no. 2, pp. 273-315, Sep. 2008.
[18] F. Faul et al., “ G*Power 3: A flexible statistical power analysis for the social, behavioral, and biomedical sciences ,”Behavior Research Methods, vol. 39, no. 1, pp.175-191, Nov. 2007.
[19] L. Cronbach, “ Coefficient alpha and the internal structure of tests,”Psychometrika, vol.16, no. 3, pp. 297-334, May 1957.
[20] A. Wikman, “Reliability, validity and true values in surveys,”Social Indicators Research,vol. 78, no.1, pp. 85-110, May 2006.
[21] M.D. Williams et al., “Contemporary trends and issues in IT adoption and diffusion research,”J. of Inform. Tech., vol. 2009, no.24, pp. 1-10, Jan. 2009.
[22] Tram Truong-Huu; Chen-Khong Tham, "A Novel Model for Competition and Cooperation among Cloud Providers," Cloud Computing, IEEE Transactions on , vol.2, no.3, pp.251,265, July-Sept. 1 2014
[23] Jamshidi, P.; Ahmad, A.; Pahl, C., "Cloud Migration Research: A Systematic Review," Cloud Computing, IEEE Transactions on , vol.1, no.2, pp.142,157, July-December 2013
[24] Kailasam, S.; Dhawalia, P.; Balaji, S.J.; Iyer, G.; Dharanipragada, J., "Extending MapReduce across Clouds with BStream," Cloud Computing, IEEE Transactions on , vol.2, no.3, pp.362,376, July-Sept. 1 2014
[25]D.F Davis, P.R. Bagozzi and R.P. Warshaw, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,”MIS Quart.,vol.13, no. 3, pp. 319-339, Dec. 1989.
[26] M.E. Rogers, Diffusion of Innovation,5th ed. New York, Free Press, 2003.
[27] H.T. Nguyen, “Information technology adoption in SMEs: an integrated framework,”Int. J. of Entrepreneurial Behaviour & Research Tech. Manage.,vol. 15, no. 2, 162-186, Jan. 2009.
[28] M.A. Sharif, “It's written in the cloud: The hype and promise of cloud computing,”J. of Enterprise Inform. Manage., vol. 23, no. 2, pp.131-134, May 2010. Available: doi: 10.1108/17410391011019732
[29] H. Katzan, “Identity and privacy services,”J. of Service Sci., vol. 3, no. 2, 1-13, May 2010.
[30] S. Keller et al., “Information security threats and practices in small businesses,” Inform. Syst. Manage.,vol. 22, no. 2, pp.7-19, Jul. 2005.
[31] S. Edson et al.” Ontologies for information security management and governance,”Inform. Manage.& Comput. Security, vol. 16, no. 2, pp. 150-165, Jul. 2008.

[32] F. Lombardi and R. Di Pierto, R. (2011). Secure virtualization for cloud computing. J. of Network and Comput. Applicat., vol. 34, no. 4, pp. 1113-1122, Oct. 2011.
[33] S. Mustafee, "Exploiting grid computing, desktop grids and cloud computing for e-science,"Transforming Government: People, Process and Policy, vol. 4, no. 4, pp. 288-298, May 2010.
[34] E. Straub, "Understanding technology adoption: Theory and future directions for informal learning,"Review of Educational Research, vol. 79, no. 2, pp. 625-730, Feb. 2009.
[35] C. Drugescu and R. Etges, "Maximizing the return on innvestment of information security programs: Program governance and Metrics,"Inform. Syst. Security,vol. 15, no. 6, pp. 30-40, Mar. 2009.
[36] B. Furht and A. Escalante, "Handbook of cloud computing," J. of Inform. Syst., vol. 3, Nov. 2010.
[37] A. Letaifa et al., "State of the art and research challenges of new services architecture technologies: Virtualization, SOA and cloud computing,"Int. J. of Grid & Distributed Computing, vol. 3, no. 4,pp. 69-87, May 2010.
[38] R. Gill, "Why cloud computing matters to finance,"Strategic Finance, vol. 92, no. 7, pp. 43-67, Jun. 2011.
[39] H. Demirkan, R.R. Harmon and M. Goul, "A service-oriented web application framework,"IT Professional Mag., vol. 13, no. 5, pp. 15-21, Jul. 2011.
[40] D. Owunwanne and R. Goel,"Radio frequency identification (RFID) technology: Gaining a competitive value through cloud computing,"Int. J. of Manage. and Inform. Syst., vol. 14, no. 5, pp.157-164, Apr. 2010.
[41] Opala, John, Omondi; Rahman, Shawon and Alelaiwi, Abdulhameed ; "An Analysis on the Factors Influencing Managers' Decision to Adopt of Cloud Computing"; Invited book chapters in titled " Handbook of Research on Architectural Trends in Service-Driven Computing" IGI Global, 2014
[42] Opala, John, Omondi and Rahman, Syed (Shawon);"Corporate Role in Protecting Consumers from the Risk of Identify theft "; International Journal of Computer Networks & Communications (IJCNC), Vol.5, No.5, September 2013

ACKNOWLEDGMENT

The authors extend their appreciation to theDeanship of Scientific Research at King SaudUniversity, Riyadh, Saudi Arabia for funding thiswork through the research group project No RGP-VPP- 318

AUTHORS BIO

Dr. Omondi John Opala is an Associate Professor at the Department of Information Technology at Devry University's Keller Graduate School and Technical Lead at Cisco Systems, North Carolina, USA. Omondi's research interests include Systems Architecture, Cloud computing, Information Assurance, Security Governance, Big Data, and Software-defined Networks (SDN).

Dr. Shawon (Syed) M. Rahman is an Associate Professor in the Department of Computer Science and Engineering at the University of Hawaii-Hilo, Hawaii, USA, and a visiting professor at the King Saud University, Riyadh, KSA. Shawon's research interests include Software Engineering education, Software Testing & QA, Information Assurance and Security, Cloud Computing, Mobile Application Development, and Web Accessibility. He has published over 100 peer-reviewed articles and is a member of many professional organizations including IEEE, ACM, ASEE, ASQ, ISACA, and UPE.

Dr. Abdulhameed Alelaiwi is a vice dean for technical affairs, Scientific Research Deanship, King Saud University (KSU) and a faculty member in Software Engineering Department, College of Computer and Information Sciences, KSU. He holds a Ph.D. in the field of Software Engineering from the department of software engineering, Florida Tech Univ., USA, 2002. Before joining King Saud University, he worked in the industry around 7 years. He continues to consult with local corporations in the areas of Software Engineering, E- Government, and Information security.