THE STUDY OF CLOUD COMPUTING ADOPTION RELUCTANCE AMONG SMALL FINANCIAL, HEALTHCARE, AND LEISURE INDUSTRIES IN THE UNITED STATES

Doctoral Dissertation Research

Submitted to the
Faculty of Argosy University, Chicago Campus
College of Business

In Partial Fulfillment of
the Requirements for the Degree of
Doctor of Business Administration

By

Jamal A. Shaban

November, 2014

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

THE STUDY OF CLOUD COMPUTING ADOPTION RELUCTANCE AMONG SMALL FINANCIAL, HEALTHCARE, AND LEISURE INDUSTRIES IN THE UNITED STATES

THE STUDY OF CLOUD COMPUTING ADOPTION RELUCTANCE AMONG SMALL FINANCIAL, HEALTHCARE, AND LEISURE INDUSTRIES IN THE UNITED STATES

Abstract of Doctoral Dissertation Research

Submitted to the
Faculty of Argosy University, Chicago Campus
College of Business

In Partial Fulfillment of
the Requirements for the Degree of

Doctor of Business Administration

by

Jamal A. Shahan

Argosy University

November 2014

Ayman Talib, DBA

Elias Demetriades, Ph.D.

Department: College of Business

ABSTRACT

As the Internet momentum started to wind down, a new wave of computing power was on the rise. Cloud computing is a new approach in using computing resources, which is made available to clients on demand as a pay-per-use service. Cloud computing has been gaining popularity in the past few years. Organizations of all types have considered moving their operations to the Cloud to cope with frequent market changes, reduced administrative cost, and the burden of constantly upgrading hardware and software. However, recent research shows that small organizations are still reluctant to adopt Cloud computing as it still faces challenges such as data security, business continuity and disaster recover, contract lock-in, service level agreement and compliance.

The focus of this study was to investigate factors that would persuade or hinder small firms from adopting Cloud computing. The study looked at small organizations only in the fields of financial, health and leisure services, and applicable laws and regulations that they had to abide with when considering the Cloud. These regulations are: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and Financial Industry Regulatory Authority (FINRA). These laws/regulations are elaborated on in the body of the dissertation. The main outcome of this study contributes to the body of knowledge by providing empirical evidence on some of the factors that inhibit small organizations' decision to adopt Cloud computing. Further, the study will enlighten Cloud service providers to improve their services and to provide the tools to meet client's expectations.

Key Words: Cloud Computing, FINRA, HIPPA, PCI DSS, Data Security, Business Continuity, Contract lock-in, SLA, Compliance

ACKNOWLEDGEMENTS

I would like to thank Dr. Ayman Talib and Dr. Elias Demetriades for their help during the dissertation phase of my doctoral study. They have been very helpful in guiding me to complete the dissertation, especially Dr. Talib for his continuous guidance, inspiration, and recommendations during the dissertation work. I also wish to thank many other people who were instrumental to my success by giving advice, encouragement, statistics, and editing assistance. These people include, but are not limited to, Dr. A. Alshboul for his support and encouragement, and Dr. A. Weaver for dissertation editing and fellow Argosy University students.

DEDICATION

I would like to give all of my praises and gratefulness that are due first and foremost to the All-Mighty God, for giving me the willpower to complete this stage of my life. I would also like to dedicate this dissertation to my parents. I wish that they were here to witness this accomplishment. To my family, to my wife, Aya Shaban, who has been at my side and encouraging me in making this possible. Also, to my children, Sammy, Ra'ed, Sa'ed, Hala, and Layan, who have been patient with me and have added joy to my life along the way. Last but not least, to my brothers, sisters, and friends for their support and encouragements. I love you all!

TABLE OF CONTENTS

Page

TABLE OF TABLES

Table **Page**

TABLE OF FIGURES

Figure **Page**

CHAPTER ONE: INTRODUCTION

Digital computing has dramatically changed the way organizations conduct business with its efficiency and powerful computations. Many organizations have invested heavily in their information technology (IT) and its infrastructure. Corporate capital expenditure spending rose from five percent in the late 1960s to over 50% in recent years (Carr, 2003). However, with the recent global economic and market slowdown, organizations were forced to pursue new avenues to control cost, increase efficiency, and enhance productivity (Misra & Mondal, 2011; Sultan, 2009). To cope with the unexpected changes, organization's IT departments are now required to have dynamic systems and strategies to accommodate demands. Business agility is now becoming a strategic necessity. Ross, Weill, and Robertson (2006) noted that "Greater globalization, increasing regulation, and faster cycle times all demand an ability to quickly change organizational processes" (p. 12). Some organizations are outsourcing their IT services, while others are considering adopting Cloud computing to reduce costs and sustain a competitive advantage (Gill, 2011).

Cloud computing is based on the idea of virtualization so that servers that host applications or store data are shared among many organizations. Hence, multiple data centers are linked together for scalability and to accommodate customer's requirements. Cloud computing is a technological innovation that is operation efficient, cost cutting, and deployment flexible. It also has been gaining popularity in the past few years. Organizations of all types, including financial, health, and leisure services firms, have considered moving their operations to the Cloud to cope with frequent market changes, reduced administrative costs, and the burden of constantly upgrading hardware and

software. According to Bittman (2006), "As the world becomes more connected…the ability to react with speed and flexibility is growing in importance." Early adopters are pursuing the Cloud adaptation cautiously due to data security, legal and regulatory concerns with their data being at stake, or losing full visibility of how data becomes available. Recent studies have focused on the benefit of the Cloud, but minimal research, if any, examined Cloud service provider's (CSP) regulatory obedience with industry and government regulations. Gartner's survey revealed that different CSP have different levels of security as well as regulatory and standard audits (Leong & MacDonald, 2011). Some CSP are required to issue a statement of Audit Standards No. 70 (SAS70), but this is not evidence of security or regulatory compliance (Himmel, 2012). However, recent surveys indicate that organizations are tentative in considering the Cloud solution due to various concerns and the obvious is regulatory compliance solutions that CSP might lack to support or comply with. Wang and Shih (2009) suggested that Cloud providers should assume responsibility as much as the client in meeting compliance, which in turn will motivate Cloud adaptation (Wang & Shih, 2009). Therefore, uncertainty of CSP credibility plays a major role in accepting or rejecting Cloud adoption. Currently, CSP has mainstream level of control over the Cloud service as presented in Figure 1.

Background

Cloud computing consists of a collection of computing resources, such as software and hardware, made available over the Internet without limitations of usage. Cloud operations can scale over thousands of servers instantaneously to make resources available to meet requester demands. The Cloud uses distributed computing so that clients can process multiple tasks simultaneously. This computing power is known as

utility computing, which is made available to clients as pay-per-use. Therefore, clients can scale up or down based on their necessities.

Cloud services consist of three layers of different services commonly referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS; Vaquero, Rodero-Merino, Caceres, & Lindner, 2008). With the Infrastructure as a Service layer (IaaS), the firm outsources its hardware used to support operations, including servers, storage, and networking components. The PaaS is the ability to rent these virtualized services to run existing applications or develop new applications. The SaaS provides customers with typical software that runs over the Internet, such as Google docs program (Hayes, 2008). The three layers or services can be used individually or combined based on the business's needs.

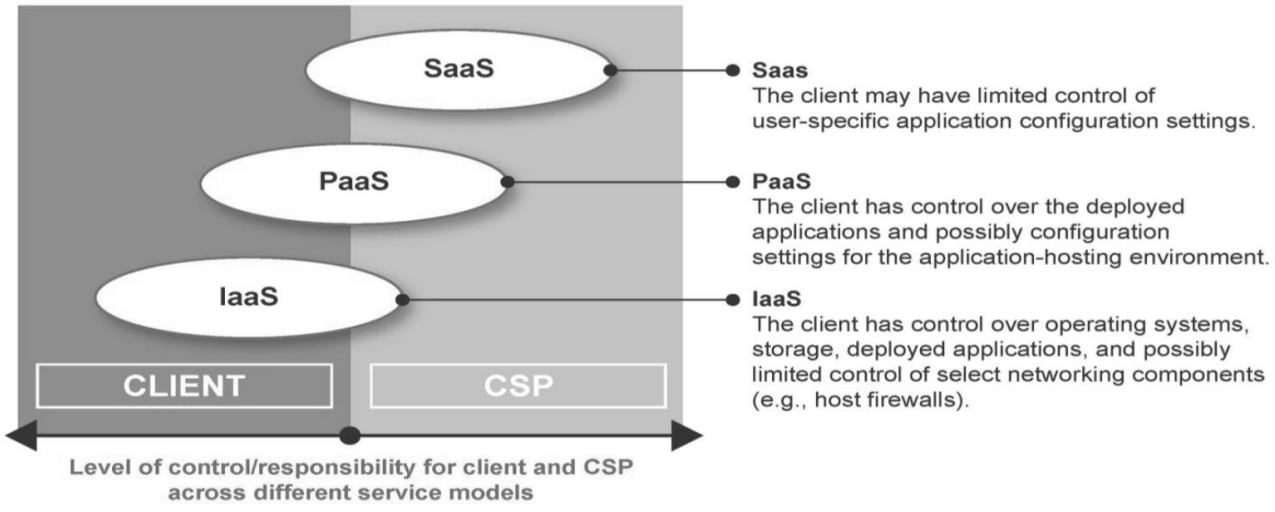


Figure 1. Level of control/responsibility for client and CSP across different service models.

The use of Cloud computing has been growing dramatically among individuals and small to mid-sized businesses. A poll conducted in 2011 by CDW, an Illinois-based

computer hardware and software supplier, confirmed that nearly 28% of U.S. small businesses are using the Cloud computing model in their daily operation. Two years later the firm conducted a similar survey and found small business Cloud adoption increased to 46%. This is an indication that Cloud computing is evolving, but still faces resistance.

Statement of the Problem

Global economic downturn and business uncertainty have become an economic threat for community and government interests (Bates, 2005). According to the government, small business administration and small size organizations account for 67% of net job creation in the United States (SBA, 1979). Therefore, permanence and strength of small organizations is critical to economic growth as well as gratification to personal freedoms (Anderson, 2009; Michael & Pearce, 2009; Shackelford, 2009). The economic slump and ambiguity has forced organizations to look to venues to cut down on spending while maintaining competitiveness. To sustain business operations and profitability, organizations are turning to technology to address these concerns. According to Gartner, organizations' Chief Information Officers (CIO) are forced to cut down on business expenditures and many are reducing IT spending to reconcile (Leong & MacDonald, 2011). To mitigate the increased IT business operation, numerous organizations outsourced their IT operation overseas, while others pursued available technology.

Cloud computing, a new technological paradigm that offers computing scalability and flexibility, is gaining momentum among organizations as a pay-per-use solution to the augment of data processing and reduction in business IT operating costs. Recent studies find small organizations are reluctant to move their operations to the Cloud because of profound concerns about data security, business continuity and service

availability, contract lock-in, service delivery agreement (SLA), and compliance as identified by Armbrust et al. (2010). In this study, the researcher analyzed hindrances identified as data security, business continuity, contract lock-in, and SLA, and one obstruct regulatory compliance as a factor that cultivates small organization's reluctance from adopting the Cloud. The goal of this study was to provide information perceived by firms who currently utilize or are considering Cloud technology and to provide Cloud service provider's credible data about factors that persuade or hinder small firms from adopting the Cloud. This study also contributes to the body of knowledge by providing empirical evidence on compliance as being a major concern to organization's considering Cloud adoption.

Purpose of the Study

The purpose of this quantitative study was to achieve a better understanding of factors that cultivate small organization's reluctance to adopt Cloud computing through the use of the extended technology acceptance model (TAM). The study investigated external factors that influence small organization's acceptance or rejection of Cloud adoption, which could be consistent with other factors as identified in the studies of Davis, Bagozzi, and Warshaw (1989), Amoroso, Spencer, and Redfield (2004), and Opitz, Langkau, Schmidt, and Kolbe (2012).

In the study, the researcher carefully examined regulatory compliance laws applicable to three industries identified as financial services, healthcare services, and leisure services, to find determinants that influence their decision in adopting or rejecting the Cloud services. To further clarify the conception of CC, articles and white papers were collected from vendors and practitioners and creditable sources published on the

Internet, as well as scientific publications such as IEEE with a focus on CC adoption and factors that influence the adoption rate. The study used the extended technology acceptance model (TAM), which included five obstructs: 1) data security, 2) business continuity, 3) contract lock-in, 4) service level agreement (SLA), and 5) regulatory compliance in addition to perceived ease of use and the perceived usefulness from the TAM model as a predictor to adopting Cloud computing.

Significance of the Study

The focus of this study was to examine which of the external factors cultivate small finance, health and leisure services organizations' decision in adopting or rejecting Cloud computing. The study examined industry and government regulations FINRA, HIPAA, and PCI DSS that are applicable to these industries. Further, the study will contribute to the body of knowledge by measuring and publishing empirical evidence of determinants to Cloud adoption lagging among small organizations.

Rationale

The rationale for this research was to determine the effect of the five hindrances: 1) data security, 2) business continuity and service availability, 3) contract lock-in, 4) service delivery agreement (SLA), and 5) compliance on Cloud technology adoption among small organizations using a quantitative exploratory research method.

Research Questions

Regardless of the increase in Cloud computing adaptation and reported benefits, studies show that organizations are hesitant to adopt the Cloud (Amirkhani, Salehahmadi, Hajialiasgari, & Nikafkar, 2011; Udoh, 2012). The main problem investigated in this study was determinants that contribute to small organizations' reluctance in adopting the

emerging Cloud computing technology. These factors are identified as security and privacy of information, business continuity and disaster recovery, contract lock-in, SLA, and regulatory compliance (Armbrust et al., 2010).

The high level question of this study was:

What cultivates small size organization's reluctance to adopt Cloud computing?

This study investigated the following underlying research questions:

RQ1: Are there differences between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing?

RQ2: Are there differences between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing?

RQ3: Are there differences between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

RQ4: Are there differences between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing?

RQ5: Are there differences between cloud users and non-users in regards to the effect of government regulations concerns on small organizations decision to adopt Cloud computing?

RQ6: Are there differences between cloud users and non-users in regards to the effect of technology perceived ease of use (PEoU) on small organizations decision to adopt Cloud computing?

RQ7: Are there differences between cloud users and non-users in regards to the effect of technology perceived usefulness (PU) on small organizations decision to adopt Cloud computing?

Using the quantitative approach, we assessed the relationship between dependent and independent variables. The sub-questions also identified as the external factors (e.g., data security, business continuity and disaster recover, contact lock-in, SLA, and compliance) were examined to determine which will mostly influence small organizations' decision to adopt or reject Cloud computing. Cloud adoption is the dependent variable and was measured by responses to questions presented in the survey.

Hypotheses

The underlying research question was addressed through the testing of seven hypotheses. All seven hypotheses, which were constructed on the basis of the survey questionnaire, are presented below. The participants' responses were also used to address the underlying research question through inductive analysis of the results.

Hypothesis 1

H_0: There is no statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

H_1: There is statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

Hypothesis 2

H_{02}: There is no statistically significant difference between cloud users and non-users in regards to the effect of business continuity concerns on small organizations decision to adopt Cloud computing.

H_{a2}: There is statistically significant difference between cloud users and non-users in regards to the effect of business continuity concerns on small organizations decision to adopt Cloud computing.

Hypothesis 3

H_{03}: There is no statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

H_{a3}: There is statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing.

Hypothesis 4

H_{04}: There is no statistically significant difference between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing.

H_{a4}: There is statistically significant difference between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing.

Hypothesis 5

H_{05}: There is no statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

H_{a5}: There is statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

Hypothesis 6

H_{06}: There is no statistically significant difference between cloud users and non-users in regards to the effect of perceived ease of using technology on small organizations decision to adopt Cloud computing.

H_{a6}: There is statistically significant difference between cloud users and non-users in regards to the effect of ease of using technology on small organizations decision to adopt Cloud computing.

Hypothesis 7

H_{07}: There is no statistically significant difference between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing.

H_{a7}: There is statistically significant difference between cloud users and non-users in regards to the effect of technology usefulness on small organizations decision to adopt Cloud computing.

Using the quantitative approach, the study assessed the relationship between dependent and independent variables. The sub-questions, also identified as the external factors, are the independent variables and were examined to determine which will mostly influence small organizations' decision to adopt Cloud computing. Cloud adoption is the dependent variable and was measured by responses to questions presented in the survey.

Definition of Terms

Application programmable interface (API): This is a set of procedures, protocols, and different implementations used to build software applications (Ali, Younis, Zamli, & Ismail, 2010).

Broker-dealer: A term used in financial services regulations. In general, it is a natural person, a company, or other organization that engages in the business of trading securities for its own account or on behalf of its customers. Broker-dealers are at the heart of the securities and derivatives trading process.

Business associate (BA): A person or entity that performs certain functions or activities that involves the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Cloud computing (CC): Cloud computing as defined by Mirzaei (2008) is a computing model that was built on decades of research which utilizes virtualization, distributed computing, utility computing, and networking.

Cloud customer, client, or tenant: The entity including merchants, payment processors, and service providers who subscribe to utilize Cloud services.

Cloud service provider (CSP): The entity providing the Cloud service. The CSP acquires and manages the infrastructure required for providing the services, runs the Cloud software that provides the services, and delivers the Cloud services through network access (NIST, 2012).

Community Cloud: A Cloud infrastructure and service shared between multiple organizations with a common tie.

Distributed computing: Computer's process with the ability to run multiple tasks simultaneously.

Electronic discovery (e-Discovery): The California e-Discovery Act (AB5) was signed into law in 2009. "This act requires disaster recovery data, a.k.a. backup tapes, to be treated as a standard source of search and discovery efforts" (ABA Technology eReport, 2011). E-Discovery is the process of searching, locating, and securing electronic data on any local or networked computer in an organization with the intention of using the data as evidence in a civil or criminal legal case. E-Discovery can be performed offline or online, on a standalone computer, or a networked computer. Once a computer is identified, it is decommissioned and secured until all data is collected and evidence presented to court.

Financial Industry Regulatory Authority (FINRA): FINRA is the largest independent watchdog for all financial firms conducting business in the United States. FINRA's mission is to protect investors by making sure financial institutions operate fairly and honestly. FINRA issued regulatory notice 10-06 in 2010 that addressed

enterprise social networks including communications traffic over blogs, wikis, discussion forums, bookmarks, social media, and unified communications. These simple electronic communications of any organization are subject to discovery should the firm face legal action.

Granular policy control: Define corporate governance policies at the global, local, group, or user level that prevent access to specific websites and the ability to download applications.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA was passed by the United State Congress and signed by President Bill Clinton in 19996. HIPAA has two titles, Title I is to protect health insurance coverage to employees and their families in the event of job loss or job change. Title II, which is addressed in this study, is the Administrative Simplification (AS) provision, which tackles the standard for protecting sensitive patient data. Title II mandates that any company that deals with individual's health information (HI) must protect the information and ensure all required physical safeguards, technical safeguards and policies, and network and security measures are in place and followed. A supplemental act to HIPAA called The Health Information Technology for Economic and Clinical Health (HITECH) was passed in 2009 to address new technological developments in the health industry and the increased usage, storage, and transmittal of electronic health records over the web.

Hybrid Cloud: Using a Hybrid approach, companies can maintain control of an internally managed private Cloud while relying on the public Cloud as needed.

Identity management: This requires the firm to implement a solution that provides content filtering for messages posted to a wide range of real-time

communication tools, social networking sites (e.g., blogs, wiki, and communities), and webmail (e.g., Gmail) to ensure all messages are appropriate.

Infrastructure as a Service (IaaS): Hardware used to support business operations including servers, storage, and networking components.

Log conversation and content: Captures post-content and log conversations made to social media sites and exports to e-Discovery or enterprise content management platforms.

Network, data transmission, and security: This mandates the CSP to have a secure network and communication channels to protect against unauthorized public access of ePHI. These concern all methods of data transmission even over a private network whether it is instant messaging, social networking, email, or Internet.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS regulations are widely accepted policies and procedures created in 2004 with the goal to optimize the security of cardholder information and transactions. The four major credit card companies Visa, MasterCard, Discover, and American Express created PCI DSS jointly to protect cardholder data against theft and misuse. PCI DSS consists of six key goals with more than 300 sub-requirements that address every domain of information security and mandates CSP to implement within the cardholder data environment. These goals are:

- Access control: This requires the protection of cardholder data physically and electronically. Access to system information and operations should be restricted to intended individuals only. These individual should have unique credentials assigned to access such systems. It also requires a proper

mechanism for shredded documents disposal and procedures to prevent document duplications.

- Data storage: Cardholder's personal information such as Social Security number, date of birth, phone number, and mailing address should be stored in a secure repository against hacking. Furthermore, strong encryption algorithm are applied to data in transit over public networks and e-commerce transactions over the web.
- Network and system monitoring: This requires CSP to track and monitor all access to network resources and cardholder data. Perform a regular scan of all network resources, systems, and applications to make sure security measures and processes are in place, functioning properly, and up to date.
- Secure network: This involves having a network protected by robust firewalls for LAN and Wireless LAN that withstand any malicious attacks. Furthermore, authentication to network resources must be limited to pre-identified personnel. Network configuration and data flow diagram or a listing of all systems that store, process, or transmit cardholder data that should be stored and secured with restrict access.
- Security policy: CSP should maintain a policy that addresses information security that includes system access, password policy, and change management. Enforcement measures such as audits and regular testing of controls to ensure its effectiveness.
- Vulnerability management: This requires anti-virus software, anti-spyware programs, and other anti-malware solutions installed and frequently updated

on all systems within the network. In addition, all applications should be free of bugs and vulnerabilities. Operating system (OS) patches should be tested and installed on all systems once released by the vender to prevent any back door attacks that target cardholder data.

Physical safeguard: The physical safeguard requires the CSP to maintain a secure data-centre where data resides with limited facility access and control to those who are authorized. Companies that are required to be HIPAA compliant must have policies and procedures for use with site visitors and employees and predetermine who can access computer equipment and electronic media. This includes transferring, removing, disposing, and re-using electronic media and electronic protected health information (ePHI).

Platform as a Service (PaaS): Network resources such as hardware, VM's, storage, and software made available to customers as pay-per-use to run existing applications or develop new ones.

Private Cloud: Private Clouds are data center architectures owned by a single company that provides flexibility, scalability, provisioning, automation, and monitoring.

Public Cloud: According to NIST, with public Clouds, 'The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling Cloud services' (NIST, 2012).

Software as a Service (SaaS): The software that runs over the Internet such as Google docs program (Hayes, 2008).

Technical policies: Technical policies are procedures that include a set of controls that CSP test frequently to ensure their effectiveness and to confirm the integrity

of ePHI and to make sure it has not been altered or destroyed. Moreover, an Information Technology (IT) disaster recovery plan and off site backups for patients (HI) is critical to business continuity. In a recent study that was conducted by the Gartner Group, it was reported that 40% of businesses that lose their data in a disaster go out of business within five years. Hence, the company's survival after a disaster depends greatly on the continuity of data protection and the accessibility and credibility of the recovery plan.

Technical safeguard: The technical safeguard is a set of documentation maintained by CSP that explains procedures on how the protected health data is accessed and who has access. Commonly, access to such information is strictly limited to pre-authorized individuals with unique credentials such as user-ID and a password. The HI must be encrypted and only intended users can decrypt its contents. Furthermore, a record of activity logs of system access and tracking records of hardware and software changes are retained for audits. Lastly, an emergency procedure should be kept in a safe place as a reference should security violations or unintended activities occur.

Utility computing: Term used for any of the three services offered by the Cloud provider, Saas, PaaS, and IaaS to purchase individually or as a package as needed and pay-per-use.

Virtual machine (VM): The software program that runs on a machine that exhibits the behavior of a separate computer. Multiple VM machines can exist within a single computer.

Virtualization Cloud computing: Consists of a collection of computing resources such as software and hardware made available over the Internet without

limitations of usage. The Cloud can scale over thousands of servers instantaneously to make resources available to meet requester demands.

Table 1

Variable's Name

Variable Name	Variable Type	Data Type
Cloud Adoption	Dependent	Ordinal
Data Security	Independent	Ordinal
Business Continuity and Disaster Recovery	Independent	Ordinal
Contract Lock-in	Independent	Ordinal
Service Level Agreement (SLA)	Independent	Ordinal
Compliance	Independent	Ordinal

Organization of the Remainder of the Study

Chapter Two contains an analysis of the existing literature associated with Cloud computing adoption, data security, business continuity and disaster recover, contract lock-in, SLA, and compliance. The articles cited for the study are from peer reviewed journalism, industry practitioners, and technology market research sites. Chapter Three contains the methodological approach as well as the conceptual and theoretical model of the study. It also includes research questions, hypotheses, variables, and measurements of the constructs through statistical analysis. The chapter consists of data collection plan, survey instrument, data analysis techniques, validity and reliability, assumptions and limitations, and ethical considerations of the study.

Chapter Four contains the finding of collected data illustrated in tables and figures representing the factors that cultivate small organizations' reluctance in adopting Cloud computing. Chapter Five provides an overview of the study results with a discussion of data analysis and how to apply the study findings to hypotheses, research questions, and

the implication of the results to organizations in the U.S. planning to pursue Cloud computing adoption. Lastly, the study provides recommendations for further research for Cloud adoption.

CHAPTER TWO: LITERATURE REVIEW

The constant evolution of technology composes challenges for organizations to keep up with the latest changes. For example, the birth of the Internet and related technologies revolutionized the way organizations planned and conducted business. It took a few years for organizations to adopt the Internet and begin using it, and even longer to make websites and introduce E-commerce (Gaspay, Dardan, & Legorreta, 2008). Some small and midsize organizations took advantage of the Internet and E-commerce to vastly extend their operation globally and compete with larger corporations. Studies show that organizations who adopted the Internet first improved communication, reduced costs, and saved time to market their goods (Chwelos, Benbasat, & Dexter, 2001; Walczuch, Van Braven, & Lundgren, 2000).

As the Internet momentum started to wind down, a new wave of technology was on the rise. Cloud computing (CC) or computing as a utility initiated a new delivery model of information technology service. Cloud computing providers have infinite on demand computing resources offered on a pay-per-use basis. The firm can employ these resources as needed and pay for what is used. The flexibility of scaling up or down improves the firm's IT economics by reducing hardware/software and labor costs.

Still, this new wave got researchers busy investigating the pros and cons of this new era. Many saw great opportunities in CC, but were skeptical about its growth and adaptation. They have identified 10 Cloud computing obstacles (five barriers to its adaptation and five hindrances in growth). These barriers are identified as: (a) data security, (b) business continuity and service availability, (c) contract lock-in, (d) service delivery agreement (SLA), and (e) compliance. Growth obstacles are identified as (a)

performance unpredictability, (b) data transfer bottlenecks, (c) scalable storage, (d) bugs in large-scale distributed systems, and (e) reputation fate sharing (Armbrust et al., 2010).

This research focused on small organizations' reluctance to CC adoption, specifically compliance as a contributing factor to slow CC adoption. Nevertheless, a wealth of research was conducted on obstructions identified as data security, business continuity and service availability, contract lock-in, and service level agreement. These were not ignored and were briefly discussed and included in the data analysis as well.

Data Security

Many organizations still believe that data managed internally is protected more than being externally managed (e.g., Cloud provider). According to Herrmann (2008), "Security is one of the core competencies of the Cloud provider" (as cited in Staten, Yates, Gillett, Saleh, & Dines, 2008). Some statistics show that one-third of data breaches are caused by lost or stolen laptops or other devices containing company information or employees exposing data on the Internet, and 16% are caused by internal theft (Mills, 2009). Since Cloud service providers are equally subjected to these requirements, many do not accept responsibility for the data stored in their infrastructure. They relinquish their responsibility of any risk (Cloud Security Alliance, 2009). Loss of data control is not the only security concern. Data-in transit, data-at-rest, processing of data, including multi-tenancy, data lineage, data provenance, and data reminisce (magnetization) are also other security concerns to account for (Mather, Kumaraswamy, & Latif, 2009). Many firms, mainly financial institutions, are expected to adapt their information security policies, standards, and practices to incorporate the activities related to a Cloud service provider. Nevertheless, a recent survey found that security concerns,

integration, and data location remain the top challenges in adopting the public Cloud among large organizations.

Business Continuity and Service Availability

System reliability and data availability are crucial factors for an enterprise's business operation. Reliability measures how frequently the system fails whereas availability measures the percentage of time the system is in its operational state. Data storage and I/O performance is another concern to many adopters (Kim, Lim, Leong, Jo, & Lee, 2009). According to Abadi (2009), "Clouds are typically built on top of cheap commodity hardware, for which failure is not uncommon. Consequently, the probability of a failure occurring during a long-running data analysis task is relatively high" (Abadi, 2009, p. 6). However, Cloud service providers (CSP) have the technology and capacity, but outages or latency in accessing data are inevitable. Nonetheless, having one CC provider is a single point of failure (Armbrust et al., 2010), regardless of having multiple data centers. CSP outages were witnessed in recent years, which caused loss of production and, most importantly, affected customer's experiences. For example, salesforce.com experienced an outage on February 12, 2008 that left customers without services for six hours (Leavitt, 2009). During the same time period, it was reported that Amazon EC2 (Elastic Compute Cloud) suffered a three hour outage. It took some time to recover and regain customer trust. In 2007, the online storage service MediaMax went out of business because of a lack of policy control. Their network administrator executed a faulty script that caused the deletion of customer data (Bowers, Juels, & Oprea, 2009). Moreover, Amazon Web Service (AWS), a service used by many start-up Internet companies as well as large enterprises including Netflix and NAS, had an outage that was

reported by USA Today. The report noted that, "When AWS goes down; it can disrupt a notable portion of Internet activity, sometimes for hours at a time" (Barr, 2013).

In Gartner's survey, many organizations believed that having control over their own IT infrastructure can mitigate risks more effectively but downtime is imminent in any environment, whether the application is hosted on the Cloud or in-house (Leong & MacDonald, 2011). Cloud computing providers continue to build data centers to ensure reliability, availability, and flexibility of data. In a survey released in December, 2010 by the 1105 Government Information Group, significant cost reduction, reliability, and availability of data are the top three reasons federal agencies are moving to the Cloud.

Contract Lock-In

Contract lock-in is crucial to Cloud customers due to two main reasons. First, contract lock-in is attractive to Cloud computing providers. Viega (2009) noted that one motivating factor for lock-in is in the vendor's interest to increase their prices. Tenants are susceptible to price increases, to reliability problems, and even to providers going out of business (Sultan, 2009). Secondly, CSP offers tenants three different platform services, with SaaS as the most challenging. Using SaaS, the customers have to develop their own application programmable interface (API) to interface with the CSP platform to access their data. These API's are not interchangeable between Cloud providers.

In general, the more proprietary a Cloud service or platform is, the harder it will be to move away from it (van Ommeren & van de Berg, 2011). For instance, when the tenant decides to move their software operation to a new CSP due to price increase or violation for promised services, they will have to rewrite their APIs to abide by new CSP platform requirements. These interfaces hinder consumers to move from one provider to

another (Buyya, Yeo, & Venugopal, 2008). According to Armbrust et al. (2010), "concern about the difficulty of extracting data from the Cloud is preventing some organizations from adopting Cloud computing" (p. 15).

Service Delivery Agreement (SLA)

A service level of agreement is a document that describes the service level expected by the customer along with technical details like daily backups and recovery time objectives. The agreement includes metrics the service will be measured on and penalties that will happen if not achieved (Greiner & Paul, 2007). Microsoft Windows Azure, for example, guarantees 99.5% of external Internet connectivity to customer's instance role. For storage they guarantee 99.9% for role instance not running and initiate a corrective action and 99% for properly formatted requests to add, update, and delete data (Windows Azure SLA, 2014). This 99.9% of network up-time translates mathematically into four minutes (Table 2) in down-time per month. This might not sound like a lot, but since network operations are the core function of many businesses, the four minutes of down time on the Cloud means more revenue loss for a business.

There are different SLA metrics included in an SLA contract and they are dependent on the service purchased from the CSP. These metrics may include:

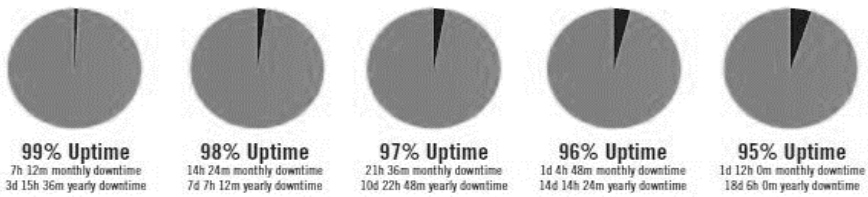
1. Service availability during peak business hours and E-commerce that generates revenue 24/7.
2. Defect rate such as incomplete backups and coding errors.
3. Technical quality of the service provider support team, which includes escalation and RTS (return to service).

According to the ENISA survey, 15% of clients received availability reports from CSP and only 7% receive penetration test reports (Dekker & Hogben, 2011). Therefore, these metrics should be well identified in a contract and reviewed by a legal firm or in-house counsel for content and to determine responsibility and to protect the customer from third-party litigation resulting from service level breaches.

Gartner's study found that major Cloud providers, Amazon and HP, have the worst SLA and they described it as "practically useless" (Leong & MacDonald, 2011). Since the Cloud utilizes virtualization, Amazon and HP include VM machine up time in their SLA contract, but left off storage. Gartner wrote, "If the storage isn't available, it doesn't matter if the virtual machine is happily up and running — it can't do anything useful" (Leong & MacDonald, 2011). Network resource up-time is critical to business operations, especially companies with online services (e.g., E-commerce). The availability of resources could transfer into an expensive SLA contract 99.999% of the time. Nevertheless, it is yet to be ascertained if the customers receive adequate compensation to lost business due to CSP outages.

Table 2

Percent Uptime-to-Day Conversion



Uptime	Downtime per month	Downtime per year
100%	0m	0m
99.999%	0.4m	5m
99.99%	4m	52m
99.9%	43m	8h 46m
99.8%	1h 26m	17h 31m
99.7%	2h 10m	1d 2h 17m
99.6%	2h 53m	1d 11h 2m
99.5%	3h 36m	1d 19h 48m
99.4%	4h 19m	2d 4h 34m
99.3%	5h 2m	2d 13h 19m
99.2%	5h 46m	2d 22h 5m
99.1%	6h 29m	3d 6h 50m
99.0%	7h 12m	3d 15h 36m
98.9%	7h 55m	4d 0h 22m
98.8%	8h 38m	4d 9h 7m
98.7%	9h 22m	4d 17h 53m
98.6%	10h 5m	5d 2h 38m
98.5%	10h 48m	5d 11h 24m
98.4%	11h 31m	5d 20h 10m
98.3%	12h 14m	6d 4h 55m
98.2%	12h 58m	6d 13h 41m
98.1%	13h 41m	6d 22h 26m
98.0%	14h 24m	7d 7h 12m

Uptime	Downtime per month	Downtime per year
97.9%	15h 7m	7d 15h 58m
97.8%	15h 50m	8d 0h 43m
97.7%	16h 34m	8d 9h 29m
97.6%	17h 17m	8d 18h 14m
97.5%	18h 0m	9d 3h 0m
97.4%	18h 43m	9d 11h 46m
97.3%	19h 26m	9d 20h 31m
97.2%	20h 10m	10d 5h 17m
97.1%	20h 53m	10d 14h 2m
97.0%	21h 36m	10d 22h 48m
96.9%	22h 19m	11d 7h 34m
96.8%	23h 2m	11d 16h 19m
96.7%	23h 46m	12d 1h 5m
96.6%	1d 0h 29m	12d 9h 50m
96.5%	1d 1h 12m	12d 18h 36m
96.4%	1d 1h 55m	13d 3h 22m
96.3%	1d 2h 38m	13d 12h 7m
96.2%	1d 3h 22m	13d 20h 53m
96.1%	1d 4h 5m	14d 5h 38m
96.0%	1d 4h 48m	14d 14h 24m
95.9%	1d 5h 31m	14d 23h 10m
95.8%	1d 6h 14m	15d 7h 55m
95.7%	1d 6h 58m	15d 16h 41m
95.6%	1d 7h 41m	16d 1h 26m
95.5%	1d 8h 24m	16d 10h 12m
95.4%	1d 9h 7m	16d 18h 58m
95.3%	1d 9h 50m	17d 3h 43m
95.2%	1d 10h 34m	17d 12h 29m
95.1%	1d 11h 17m	17d 21h 14m
95.0%	1d 12h 0m	18d 6h 0m

A note on "the nines": When discussing reliability, one often talks about "five nines" (99.999%), "four nines" (99.99%), "three nines" (99.9%), etc.

A note on maintenance: Many service providers do not count downtime caused by planned maintenance into their uptime numbers.

In the table above, a month is 30 days and a year is 365 days.

You can learn more about the Pingdom uptime monitoring service at www.pingdom.com, or read our blog at royal.pingdom.com.

Compliance

Various types of industry and government privacy laws and regulations exist at the national, state, and local levels, making compliance a potentially complicated issue for Cloud computing (Jansen & Grance, 2011). CSP should be proactive in providing safeguards to customer's sensitive data and information, but to accept liability to their

services has yet to be seen. Government and industry-association requirements, such as e-Discovery, FINRA, HIPAA, SOX, and PCI DSS require the CSP to provide secure networks and physical locations and have the necessary policies to protect data from potential risks and vulnerability. In this study, the researcher examined three regulatory compliances specific to the financial, health care, and leisure services, identified as FINRA, HIPAA, and PCIDSS.

Financial Industry Regulatory Authority (FINRA)

In general, FINRA's mission was to protect investors by making sure financial institutions operate fairly and honestly. Financial institutions use a wide range of communication and collaboration tools, therefore they are required to implement a solution that provides content filtering for messages posted to a wide range of real-time communication tools, social networking sites (e.g., blogs, wiki, and communities), and webmail. Further, you can post content and log conversations made to social media sites and export to e-Discovery or enterprise content management platforms. The consequences for not binding with FINRA can be hefty. For example, in 2010, FINRA fined Piper Jaffray $700,000 for failure to retain approximately 4.3 million emails from November, 2002 through December, 2008 (FaceTime, 2014).

Some companies do not fully state they are compliant, but appear to have the standards in place to be compliant. However, many do not specify if they are or are not Securities and Exchange Commission (SEC) compliant and lay the responsibility on the tenant. The tenant must do their due diligence to determine if the CSP offers such services. Currently, Google, Microsoft, SugarSync, and Yandex are not SEC compliant.

On outsourcing in financial services, Michael Macchiaroli reminded the broker-dealer community that in order to comply with SEC Rule 17a-4, the electronic records used in transactions must be non-erasable and non-rewritable. He also warned that the service provider that does not grant data storage in facilities outside the United States may be unsuitable in accessing the records. Furthermore, inability to access such records due to broker-dealer nonpayment to the third party hosting such records is also unacceptable. He advised that Cloud service providers must deliver SAS 70 audit letters to broker-dealers (Loeb & Loeb, 2013).

SEC/FINRA Rule 17a is a set of rules governing the archiving and security of broker-dealer records which was created in 1997 by the SEC in order to ensure brokers follow correct procedures in handling financial information. The most relatable of rules to Cloud storage companies is 17a-4(f), which introduces a third party and is intended to ensure broker-dealers have a backup to their backup of files.

Health Insurance Portability and Accountability Act (HIPAA)

Healthcare has had some serious deficiencies throughout the years and it is a prime target for identity theft. The risk is not the actual healthcare information, but financial fraud according to U.S. Department of Health and Human Services. HIPAA title II mandates companies that deal with individual's health information (HI) to protect the information and ensure that all required physical safeguards, technical safeguards and policies, and network and security measures are in place and followed. A supplemental act to HIPAA, called the Health Information Technology for Economic and Clinical Health (HITECH), was passed in 2009 to address new technological developments in the

health industry and the increased usage, storage, and transmission of electronic health records over the web (U.S. Department of Health & Human Services, 2003).

To strengthen the privacy and security protection of individual's health information, the U.S. Department of Health and Human Services (HHS) and the Office for Civil Rights released the Omnibus New Rule on Sept. 23, 2013 to ensure patient's privacy is protected regardless of where their information is stored, including the Cloud. The rule ensures the protection of any covered entity that deals with the electronic transmission of patient records despite its size. Therefore, this rule applies to any health care service provider (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, who is engaged in electronic transmission of individual's information such as billing, benefits, or claims and should follow rules set forth by the HHS office.

Moving patient health information (PHI) records to the Cloud requires the party housing that data to secure its integrity and privacy. CSPs are required by law to sign a business associate agreement (BAA) indicating how they will handle and respond to data breaches, even if caused by the provider's sub-contractors. Nevertheless, moving the data to the Cloud creates some concerns regarding the potential violation of compliance and privacy laws. According to Softlater (2009), due to compliance and data privacy laws in various countries, locality of data is very important in most enterprise's architecture. Cloud computing is based on virtualization; therefore, data can span multiple data centers in multiple locations over multiple countries. The data then falls under that country's jurisdiction and its local laws. As many health providers are shifting

toward information digitization, Kumekawa (2005) noted that this will represent a great challenge to patient privacy, confidentiality, and security. He argued that information in digital format can be easily searched, manipulated, and shared among millions by a strike of a computer key.

Another area of concern is the health care staff's knowledge and the type of training they received in handling PHI data. McGee (2013) wrote about two recent data breaches at the Oregon Health and Science University when the staff inappropriately stored decrypted patient data in the Cloud. The Cloud provider, Google, had a strong password policy to access Google drive but they did not provide a BA. According to David Boltzman from the Office of Civil Rights, "If you use a Cloud service, it should be your Business Associate. If they refuse to sign a Business Associate Agreement, don't use the Cloud service."

PCI Data Security Standard (PCI DSS)

Organizational success results from customer loyalty and trust. Customer's sensitive information such as date of birth, social security number, and financial details must be kept in a trustful place. According to McNulty (2007), there are conflicting choices that business decision makers face in the event of a data breach. These conflicting approaches highlighted the challenges of maintaining consumer trust and compliance while abiding by different and conflicting disclosure laws (Allen, 2012).

Maintaining sensitive data is a responsibility shared between the tenant and the CSP. If customer's sensitive data are processed or stored in the Cloud environment, then PCI DSS will be relevant to that environment and it requires the validation of CSP infrastructure and the tenant usage of that environment (PCI, 2013). PCI DSS has six

major objectives that an organization must maintain in order to be in compliance. First, a secure network must be maintained in which transactions can be conducted. Second, cardholder information must be protected wherever it is stored. Third, systems should be protected against the activities of malicious hackers. Fourth, access to system information and operations should be restricted and controlled. Fifth, networks must be constantly monitored and regularly tested to ensure proper function. Sixth, a formal information security policy must be defined, maintained, and followed at all times (PCI, 2010).

A violation in any of these objectives results in noncompliance. Cloud computing is based on the idea of virtualization, which means that data does not exist on a physical machine used in communication. Furthermore, virtual networks are in their infancy stage and do not yet have the tools to monitor and capture information required for compliance audits.

Summary

Cloud computing adoption has been on the rise and many firms report measurable business benefits and performance gains. All types of organizations have been adopting Cloud computing technology to achieve performance gains (Ekanayake, Qui, Gunarathne, Beason, & Fox, 2010), but its dynamic provisioning demand is arguably the main reason for its mainstream acceptance (Dwivedi & Mustafee, 2010). The literature review suggested that many small organizations are dawdling in adopting Cloud computing regardless of its benefits. In this study, the researchers will investigate factors that cultivate small organization's reluctance to adopt Cloud computing through the use of the extended technology acceptance model (TAM) which included five obstructs: 1)

data security, 2) business continuity, 3) contract lock-in, 4) service level agreement (SLA), and 5) regulatory compliance in addition to perceived ease of use and the perceived usefulness from the TAM model as a predictor to adopting Cloud computing.

CHAPTER THREE: METHODOLOGY

Introduction

Small organizations are lacking in adopting Cloud computing as found in the research and industry surveys. These studies revealed that lack of security and regulations in Cloud computing is a major drawback. Meanwhile, researchers focused on factors that hinder organizations from adopting Cloud computing, but did not profoundly examine legality as being a major drawback. Government and the industry are currently playing the catch-up game in declaring new regulations for gaps not being addressed by the Cloud service provider. As a result, the Cloud service provider has to assume more responsibility, which in turn encourages more organizations to adopt the Cloud. This has not been the case thus far, as mentioned in the previous chapter. Therefore, the focus of this quantitative study was to evaluate factors that are considered a major impediment to Cloud service adoption. The factors examined in this study were data security, business continuity and disaster recovery, contract lock-in, SLA, and regulatory compliance; with the latter being the focal point to three small organizations identified as finance, health, and leisure services. The term *adoption* is used here to define the initial decision regarding whether or not to use a technology service (Thong et al., 2011).

This chapter contains a detailed description of the research process, design, and methodology. The first section of this chapter outlines the aim of this study. The second section of this chapter describes the method used in the research to collect data for analysis and sampling. The third section of this chapter represents the research design and the steps taken throughout the research process.

Study Aim

The study aimed to accomplish the following:

1. To add to the body of research on factors that prompt small organizations in the health, financial, and leisure services to adopt or reject Cloud computing.
2. To examine if compliance with government and industry regulations applicable to these industries is integrated in the Cloud computing solution.

Conceptual Model

Scholars and practitioners are still evaluating factors that influence technology acceptance or dismissal. Over two decades of research, theories, and models were developed and extended for the purpose of identifying technology adopting factors (Agarwal & Prasad, 1999; Davis et al., 1989; Venkatesh & Davis, 2000; Taylor & Hunsinger, 2011; Ochieng, Waema, & Onsomu, 2012; Venkatesh, Morris, Davis, & Davis, 2003; Wang & Shih, 2009).

The *Technology Acceptance Model* (TAM) is a widely used theory in information systems which helps explain the factors that influence technology acceptance (Arbuckle, 1996). The model, according to Davis et al. (1989), has two important factors that influence individuals in their decision about how and when they will use technology.

The factors are Perceived usefulness (PU) and Perceived ease-of-use (PEoU).

1. Perceived usefulness (PU): "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis et al., 1989).
2. Perceived ease-of-use (PEoU): "the degree to which a person believes that using a particular system would be free from effort" (Davis et al., 1989).

TAM, as cited in most research that dealt with user acceptance of technology, stated that researchers claim it attracted more quick research and gave less attention to the real problem (Lee, Kozar, & Larsen, 2003). They encourage others to explore if the PU and PEoU factors in TAM are the mediators of external variable effect, and, if so, which external variables are important (Venkatesh, 2000; Venkatesh & Brown, 2001).

In general, the TAM model explains between 30% and 40% of system usage (Burton-Jones & Hubona, 2006; Legris, Ingham, & Collerette, 2003). Further, perceived usefulness is often found to be the strongest determinant in the model (Burton-Jones & Hubona, 2006; King & He, 2006; Legris et al., 2003; McFarland & Hamilton, 2006). A numerous amount of research had extended the TAM model to enhance the knowledge of technology acceptance and adoption (Wixom & Todd, 2005).

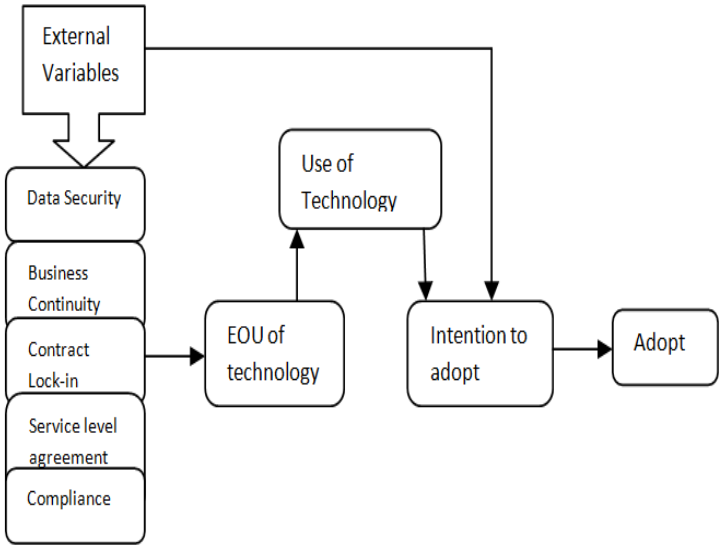


Figure 2. Projected TAM model.

Prior studies excluded compliance as a relevant factor in explaining adoption barriers to Cloud computing among small organizations. In this study, the researcher will

extend the TAM model (Figure 2) to include external variables (data security, business continuity, contract lock-in, SLA, and compliance) with the focus on compliance as a key, which may influence the organization's perception in adopting a new technology.

Framework

TAM is derived from the Theory of Reasoned Action (TRA), which offers a powerful explanation for user acceptance and usage behavior of information technology. TAM is relevant to the study of Cloud computing because it explains the determinants of user acceptance of a wide range of end-user computing technologies (Davis et al., 1989). TAM theorizes that using technological innovation is perceived usefulness as achieving better performance, and perceived ease of use as using the system is effortless, which persuades the individual to use the innovation. Davis et al. (1989) defined perceived ease of use as "the degree to which a person believes that using a particular system would be free from effort" and perceived usefulness as "the degree to which a person believes that using a particular system would enhance his or her job performance." Perceived ease of use also affects the perceived usefulness. The intention to use affects real usage behavior. Between these two, perceived ease of use has a direct effect on both perceived usefulness and technology usage (Adams, Nelson, & Todd, 1992; Davis et al., 1989).

Instrumentation

Selection of Subjects

This study focused on small organizations within the United States. The participants were comprised of individuals from three industries: financial services, health services, and leisure services in the context of small organizations in the United States. Participants included blue and white collar employees, IT Management, CTOs,

and small business owners. These various individuals are extremely diverse and across many demographic variables, therefore they provided a good population to study. Such a diverse population is in the thousands and being so diverse makes it appropriate in both size and scope.

Instrumentation and Survey Questionnaire

A quantitative research method was used in this research which allowed making generalizations on the basis of the data collected from the sample (Charles & Mertler, 2002). In this research, a web-based survey was used to collect the data for this study. The survey questionnaire was assembled by the researcher to help in drawing a conclusion about small organizations' behavior in evaluating the Cloud. Furthermore, the survey was presented to practitioners in the three fields targeted in this study to get their criticism and recommendations. They proposed to specifically ask a question to measure individual's knowledge with Cloud computing, and if the firm had experienced any security threats or failed to meet regulatory compliance.

The reason for their recommendation was that not many decision makers of small firms are familiar with Cloud computing, hence they might reject the idea because of lack of knowledge. Secondly, firms that experienced security threats to their internally controlled network will more than likely decline to have somebody else housing their data.

These questionnaires provided a descriptive analysis and were collected from a variety of participants in a minimal amount of time to quantify the results (Nesbary, 2000; Sue & Ritter, 2007). The goal was to assess the importance of external factors (as mentioned previously) in adopting technological innovation, such as Cloud computing

among participants, and to identify additional factors that organizations encounter when adopting an innovation. Participant responses were measured on Likert-scale of 5, with 1 being strongly disagree, 2 is disagree, 3 being neutral, 4 is agree, and 5 is strongly agree. Further, the survey included open-ended questions and the answers to these were carefully examined to determine the legitimacy of participant's responses.

Survey Questions Outline

Questions 1, 2, 3, and 12 are the participant's demographic information. Questions 7, 8, 9, and 10 are in regards to applicable regulatory compliance and to determine if the firm is currently in compliance with theses regulation. Questions 5, 6, 13, 14, and 15 target participants who utilize or are currently evaluating the Cloud. Questions 17, 18, 19, and 20 are to measure participant interest in adopting the Cloud considering what the provider offers.

The participation request letter asked the potential participants to voluntarily participate in the survey, which remained open for a 30-day period and took approximately 30 minutes to complete. Accessing the survey link redirected the participants to the survey landing page (the consent page) on SurveyMonkey's website to read, agree, and print the consent form. Once the participant consented they were presented with the survey questionnaire. The participants remained anonymous and any and all conditions specific to their organization were strictly adhered to. A survey questionnaire consisting of 21 questions was used to measure the individual's perception of the effect of external variables and how they influence the adoption of Cloud computing.

Limitations and Implications

One limitation of this study was that a participant may not answer truthfully, even though the participant's identity was anonymous, for fear that their incorrect behavior may be discovered and that they may be reprimanded. Therefore, they may have known copyright laws and answered the survey with the appropriate response, but still violated the law in their normal practice of the workplace. This may have caused the results to be skewed. An additional limitation may have been that the participant may have tried to quickly research the question to obtain the correct answer prior to responding. Another potential limitation is the bias response to the survey questionnaire. As Han describes, self-reporting bias occurs when a participant's experience, self-perception, and work environment influence their survey responses.

Another limitation may be that not all invited participants actually participated. Although this may be the case, those that did participate should make a sufficient sample as to how the population as a whole would have responded. This is due to the fact that the participants selected were extremely diverse across many demographic variables.

Procedures

The researcher has secured the necessary institutional approval for the study from a third party survey service SurveyMonkey. All participants were selected from the SurveyMonkey database, a professionally administered third party survey service. SurveyMonkey recruited individuals from their database that met the requirements for this research study. This third party survey service targeted audiences from small organizations engaged in the financial, healthcare, and leisure services industries and emailed them the invitation to take the survey. Further, any response from individuals

outside of these industries was rejected and not included in the data analysis. The participation request letter was sent via email, using the blind copy function, to each of the invited individuals asking for their voluntary participation. The survey remained open for a 30-day period and took approximately 30 minutes to complete. An invitation to participate in a survey, as well as the consent letter, was sent via email to the audience. Once the participant consented, they were provided with the survey questionnaire, which was the instrument used for this study.

Data Analysis

Subsequent to the survey being available for a 30-day period, the data from SurveyMonkey was collected and entered in the Statistical Package for the Social Sciences (SPSS) database and Excel, which was the software used to tabulate the data for analysis. The data was then statistically analyzed and a conclusion was produced. If appropriate, any possible recommendations were then provided. The analysis included descriptive statistics, as well as *t*-test and chi-square tests for significance of differences in the means. Whenever possible, correlation analysis was used.

The study used statistical analysis in relation to the research question using descriptive statistics, group comparisons with t-tests and ANOVA tests, and correlation matrices. These were employed to measure and confirm the seven adoption obstacles; group comparison t-test analyses was used to evaluate the relationship between the independent variables and the dependent variable. The survey questionnaire has been attached to this document as Appendix A.

Ethical Considerations

A written consent to conduct this study was obtained from the Argosy University Institutional Review Board (IRB) with no identifiable conflict of interest. There were minimal risks to potential participants in filling out this survey. The participants were provided with a consent form before accessing the survey on SurveyMonkey.com. The study did not collect sensitive data nor identify individual participants, which upholds the requirement of respect of persons and thus meets the criteria specified in the Belmont Report by the National Institute of Health (1979). Upon completion of the study, data were downloaded to the researcher's computer and subsequently deleted from Survey Monkey's web server. The data were copied to a CD ROM and will be kept in a safe for at least seven years after which time it will be destroyed.

CHAPTER FOUR: RESULTS

This chapter presents results in six sections. Section 1 restates the purpose and main research questions. Section 2 describes screening the data and presents reliability checks of survey data with Cronbach's alpha. Section 3 presents respondent demographics. Section 4 presents the inferential results of testing the research questions about participants' degree of satisfaction with Cloud technology. Section 5 presents descriptive and inferential statistics on participants' degree of agreement with a range of Cloud technology benefits. Section 6 addresses specific motivations to adopt Cloud technology.

Restatement of Purpose and Research Questions

Purpose of the Study

Although Cloud computing technology (hereafter Cloud technology) provides a number of benefits, organizations are hesitant to adopt it (Amirkhani et al., 2011; Udoh, 2012). The main goal in this study was to identify the factors that contribute to the reluctance of small organizations to adopt the emerging Cloud computing technology. The factors examined in this study were perspectives about the Cloud technology with respect to maintaining data security and privacy of information as well as promoting business continuity and disaster recovery. Factors also included perceptions about Cloud technology contract lock-in, service level agreements (SLA), and the extent to which Cloud technology secures regulatory compliance.

This study tested seven research questions, which are listed below. Corresponding hypotheses are presented along with results of hypothesis testing in Section 4.

Research Questions

RQ1: Are there differences between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing?

RQ2: Are there differences between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing?

RQ3: Are there differences between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

RQ4: Are there differences between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing?

RQ5: Are there differences between cloud users and non-users in regards to the effect of government regulations concerns on small organizations decision to adopt Cloud computing?

RQ6: Are there differences between cloud users and non-users in regards to the effect of technology perceived ease of use (PEoU) on small organizations decision to adopt Cloud computing?

RQ7: Are there differences between cloud users and non-users in regards to the effect of technology perceived usefulness (PU) on small organizations decision to adopt Cloud computing?

Screening the Data and Reliability Checks of Variables

Screening the Data

Data were collected from an online survey comprised of demographic and perception questions. Demographic data were categorical. Likert-scaled data were continuous. Continuous variables rated perceptions by level of agreement (strongly disagree = 1, disagree = 2, neutral = 3, agree = 4 and strongly agree = 5) and satisfaction (dissatisfied = 1, somewhat dissatisfied = 2, neutral = 3, satisfied = 4, and very satisfied = 5).

All data were screened for entry errors. A total of 81 participants agreed to take the survey. However, numerous participants failed to answer many or all of the survey questions. Consequently, there were 35 or 36 participants for most questions. Missing data did not show any systematic pattern.

Likert-scaled variables were screened for normality, linearity, outliers, and homoscedasticity. The data did not show any substantial departures from statistical normality and thus met the assumptions of parametric inferential tests. Independent *t*-tests were used to compare perceptions between Cloud technology users and non-users. Significance was set at $p = .05$. Percentages were rounded off to whole numbers and thus do not necessarily add to 100%.

Reliability Checks of Variables

The survey used in the current study was developed by the principal investigator and was not formally validated psychometrically. Instead, the data's internal consistency or reliability was evaluated by generating Cronbach's alpha statistics (Table 3) for conceptually-related survey statements. Cronbach's alpha was used because 1) the

survey was designed with a number of conceptually-related statements, 2) conceptually-related statements presented a Likert-scaled array of responses (rather than providing dichotomously-scored statements), and 3) the survey was only administrated once (Gliner, Morgan, & Leech, 2000). Cronbach's alpha is a commonly employed test of internal consistency for Likert-scaled data that views each statement within each set of conceptually-related statements as a "retest" of another item. In essence, Cronbach's formula generates all possible test-retest pairs of correlations and provides the mean as the reliability index *alpha* (Cronbach's alpha is not synonymous with the significance level for hypothesis testing, which is also called alpha). Cronbach's alpha ranges in value from 0 to 1. The closer Cronbach's alpha is to 1, the greater the internal consistency or reliability of the database. Indices of .70 or higher reflect an adequately reliable database.

Results of Reliability Checks

Table 3 shows the reliability statistics for conceptually-related survey statements. Reliability statistics indicated that the data were reliable.

Table 3

Cronbach's Alpha Internal Consistency (Reliability) Statistics on Cloud Technology Data

Data from Conceptually-related Survey Statements	Number of Cases	Cronbach's Alpha
Level of Satisfaction with TAM Model Satisfaction with Usefulness of Cloud Technology Satisfaction with Ease of Cloud Technology Use	35	.84
Level of Agreement with* Flexibility and Business Agility Data Backup and Disaster Recovery Reduces Upfront Cost	33	.83

Integration with Existing Infrastructure Legality and Compliance Contractual Agreement		
Level of Satisfaction with Data Availability and Data Security Vendor Contractual Agreement Business Continuity and Service Availability Service Level Agreement (SLA) Vendor Compliance Fulfillment	36	.89

Note. *Cronbach's calculations excluded three conceptually-related items because only seven participants provided answers, cf Table 7.

Participants Demographics

A total of 81 participants initially agreed to take the survey. However, over half of them failed to answer most of the survey questions. The result was a total of 36-45 participants for most questions.

Personal Participants Demographics

The principal investigator made an effort to balance the participants by gender. Figure 3 shows that of the $n = 36$ participants who supplied gender and age information, an approximately equal number of men and women fell into each age category. About a quarter of both male and female participants fell in the 35-49 year-old category (male participants, 26%; female participants, 27%) and the 50-65 year-old category (male participants, 26%; female participants, 23%). Fewer participants were in the 18-24 year-old category (male participants, 17%; female participants, 18%) and correspondingly more were in the 25-34 year-old category (male participants, 30%; female participants, 32%).

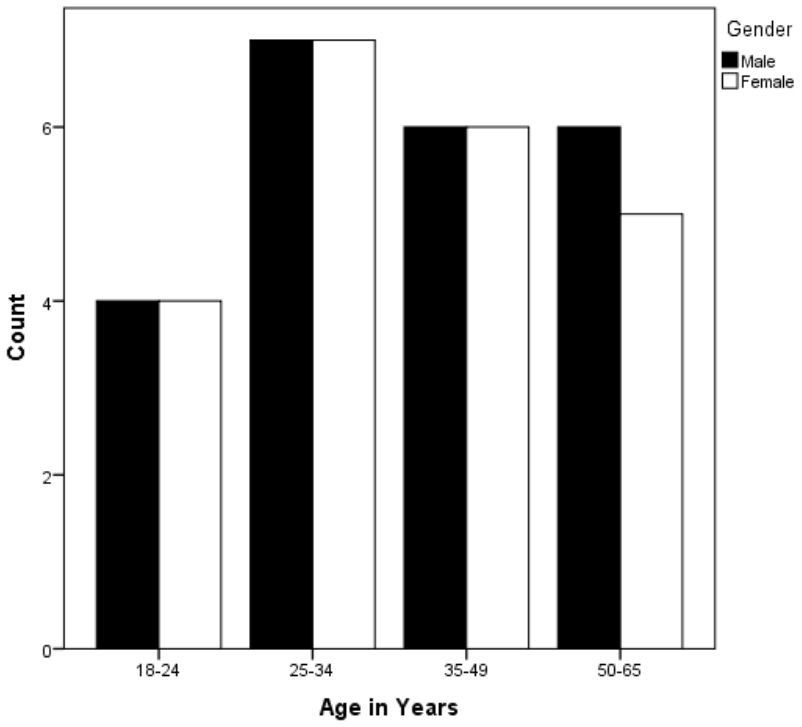


Figure 3. Cross-tabulation of gender and age class, $N = 45$ participants.

Only $n = 14$ participants (17%) provided information on both education and household income. Figure 4 shows that the majority of participants fell in the $25000-$50000 income range (50%). These were followed by an equal proportion (14%) in the $0-$25000, $100000-150000, and $150000+ income categories.

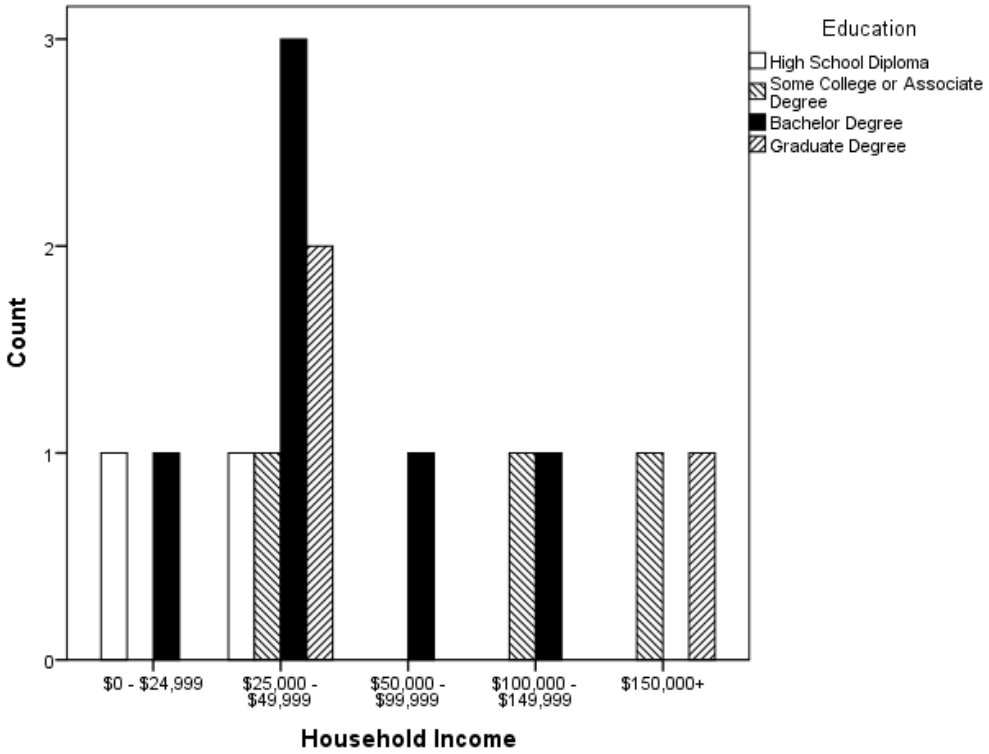


Figure 4. Cross-tabulation of educational level by household income, $N = 14$ participants.

Figure 5 shows the distribution of participants by region of residence. A third of the participants resided in the Mountain states (30%), followed by a slightly smaller percent of participants from the South Atlantic and Pacific regions (20%, respectively). Ten percent were from the East North Central states. A small number of remaining participants were from a range of regions.

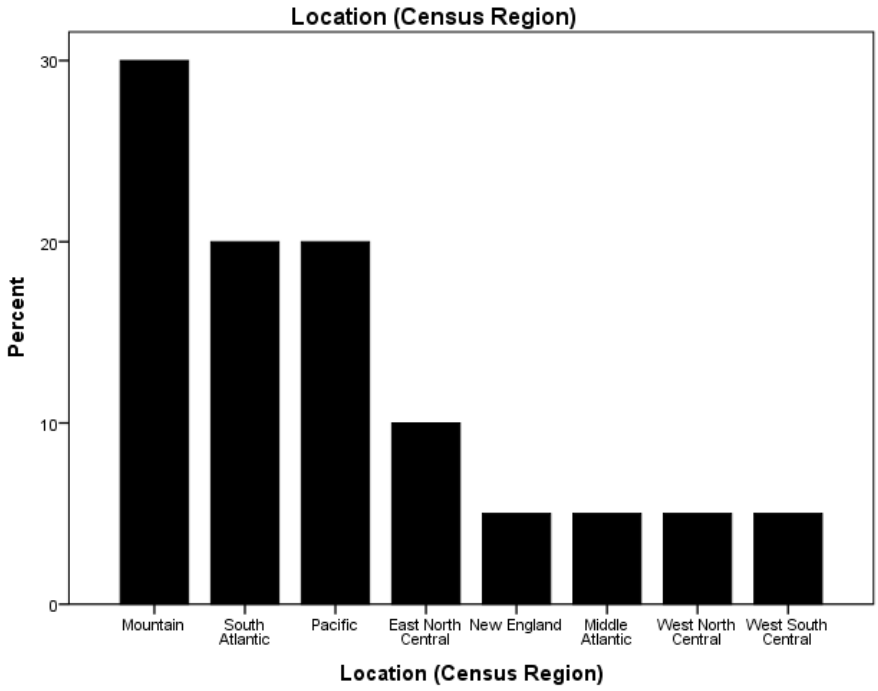


Figure 5. Distribution of participants by region of residence, $N = 20$ participants.

Professional and Business Demographics

The survey originally asked participants to select from 18 different job categories. These 18 different job categories were collapsed into two categories. One category was comprised of participants from financial, health, and leisure services industries because these industries were of primary interest to the current study. The other category was comprised of participants from all other industries. A total on $N = 45$ participants provided information on their titles and industry. Figure 6 shows the distribution of titles by industry of the participants: 40% of participants selected Other Professions and 60% selected Financial, Health, or Leisure Services. About one third, 31%, chose the other category among job titles on the survey, 29% were IT staff, 20% were IT management, and 11% were business owners.

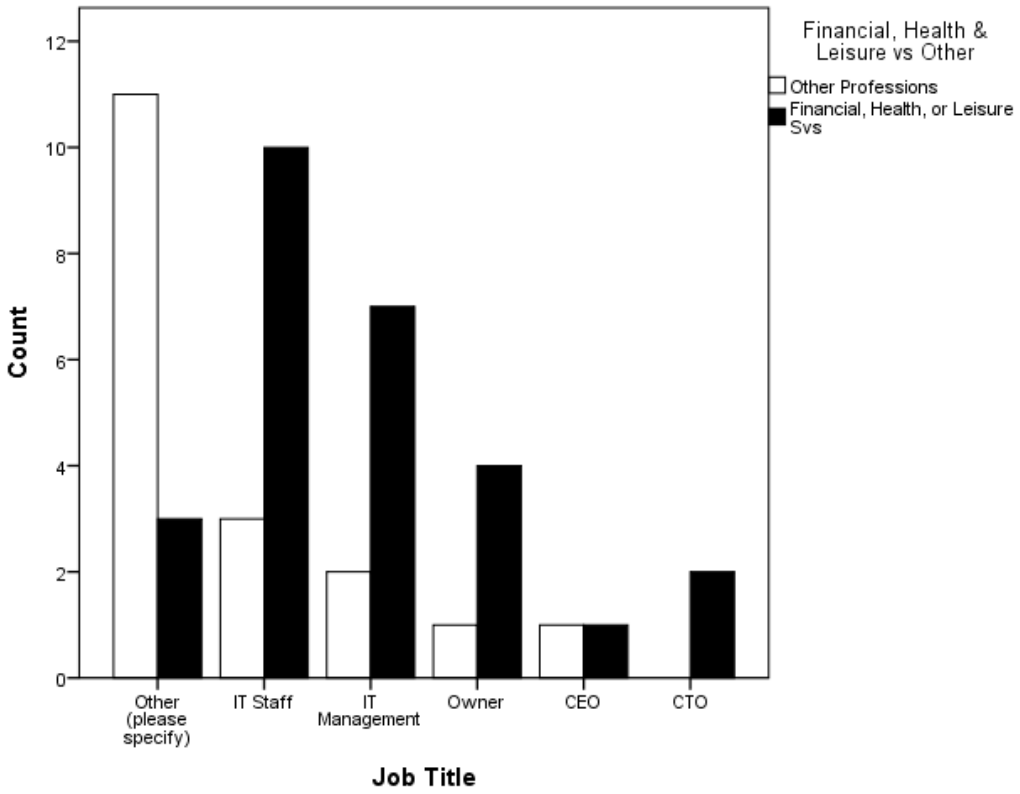


Figure 6. Distribution of participants by job title and profession, $N = 45$ participants.

Figure 7 shows the distribution of firm size represented by the participants. A little over half, 52%, worked for small firms with 1-99 employees. Another approximate fifth had 100-250 employees, 20%, and 500+ employees, 22%. Just four percent of the participants worked for firms that had 250-499 employees.

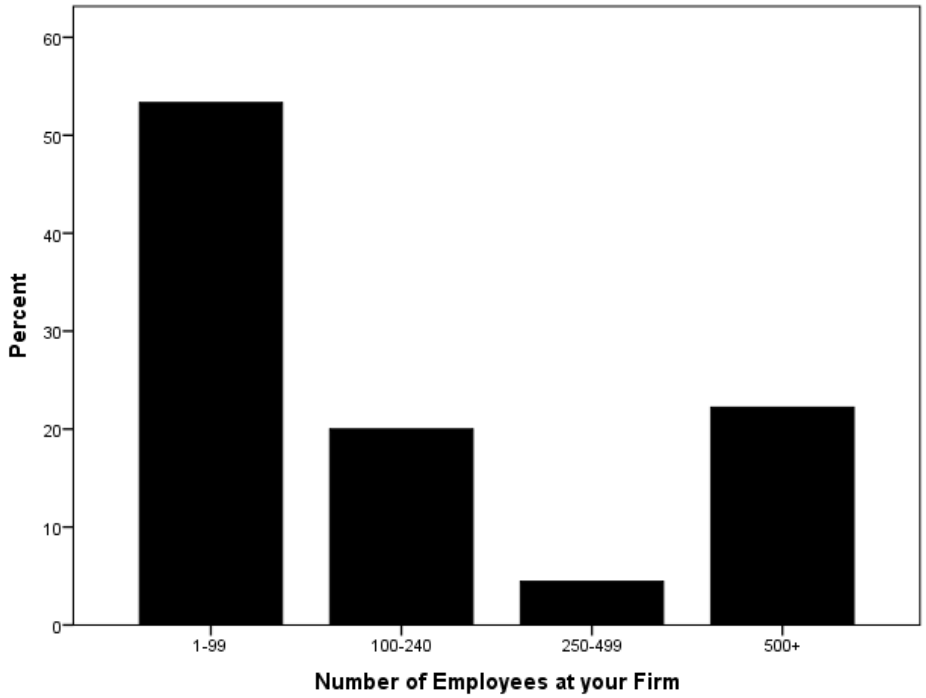


Figure 7. Distribution of firm size, $N = 45$ participants.

Participant Familiarity with and Use of Cloud Technology

Participants were asked four questions about Cloud technology. Questions included their current knowledge about Cloud computing, their firm's current Cloud status, the Cloud services that their firm or employer currently used or was evaluating, and Cloud models that their firm or employer currently used or was evaluating.

Figure 8 shows that just under half (48%) of the participants were fairly new to Cloud technology. Eighteen percent had heard about Cloud technology and 30% had beginning knowledge about it. Another third of the participants, 32%, reported intermediate knowledge about Cloud technology. A quarter of the participants, 25%, reported advanced knowledge about Cloud technology.

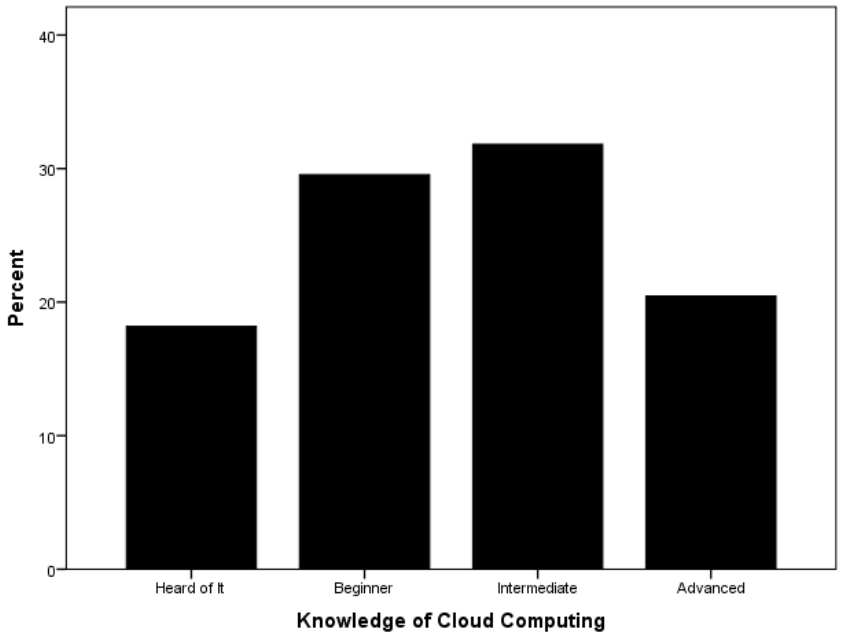


Figure 8. Distribution of the level of knowledge about Cloud technology, $N = 44$ participants.

Participants were asked to choose between three options to report their firm or employer's status with respect to Cloud technology. Figure 9 show that 20% currently used one or more Cloud technology services. Just under half, 42%, were currently evaluating Cloud technology and 39% were not currently evaluating Cloud technology for their business at the time they took the survey.

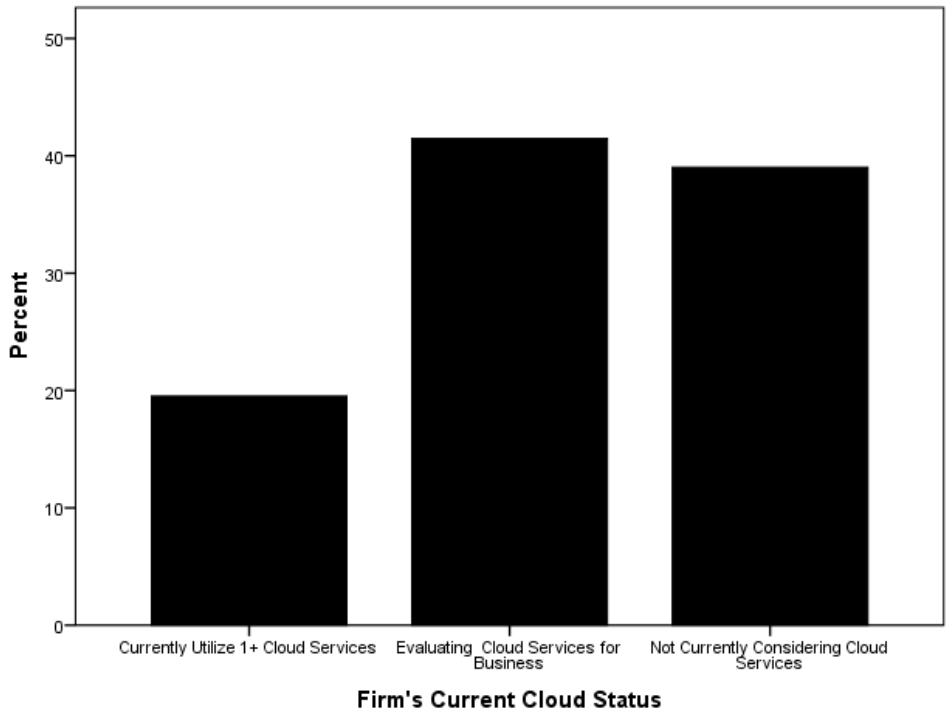


Figure 9. Distribution of firm or employer's status regarding Cloud technology, $N = 36$ participants.

Participants were asked to report how their firm or employer used Cloud technology from a list of three options: as software or SaaS, as infrastructure or IaaS, and as a computer platform or PaaS. Figure 10 shows that the most frequent use of Cloud technology was using its software (SaaS, 50%, Figure 10), followed by as infrastructure (IaaS, 17%) and as a platform (PaaS, 14%). Small percentages of participants reported using two of the three Cloud technology services (11%) and only eight percent reported using all three services.

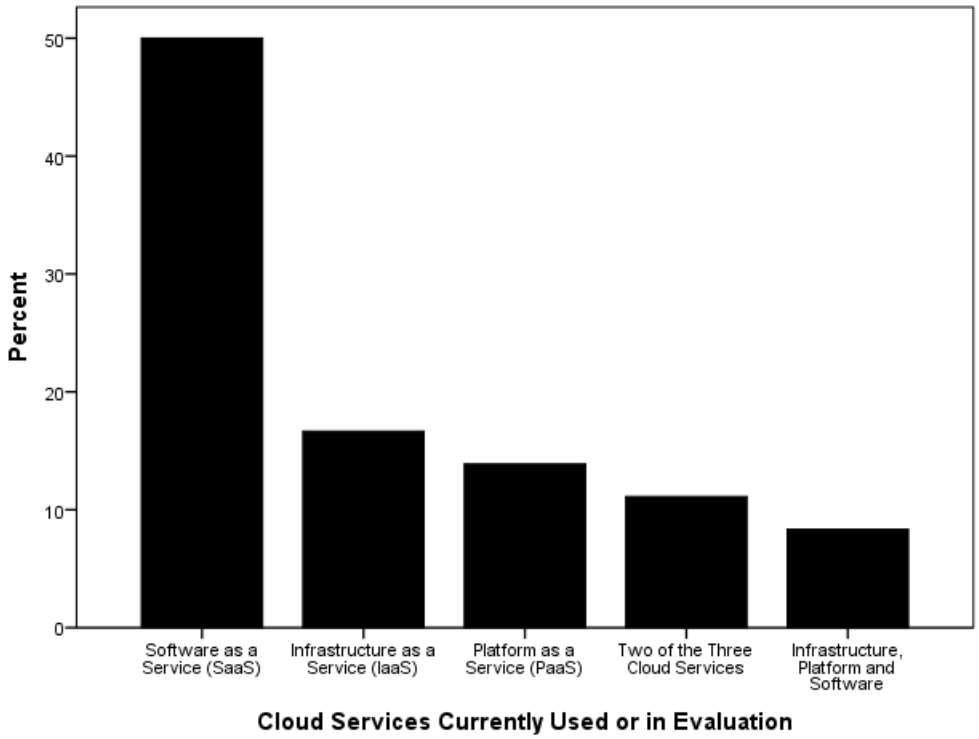


Figure 10. Distribution of Cloud technology services currently in use or being considered for use, $N = 36$ participants.

There are several options for Cloud technology models, including public, private, hybrid, and community models. Figure 11 shows that three-quarters of the participants reported using private Cloud (42%) or public Cloud (31%). A much smaller but equal proportion reported hybrid Cloud (14%) or community Cloud use (14%).

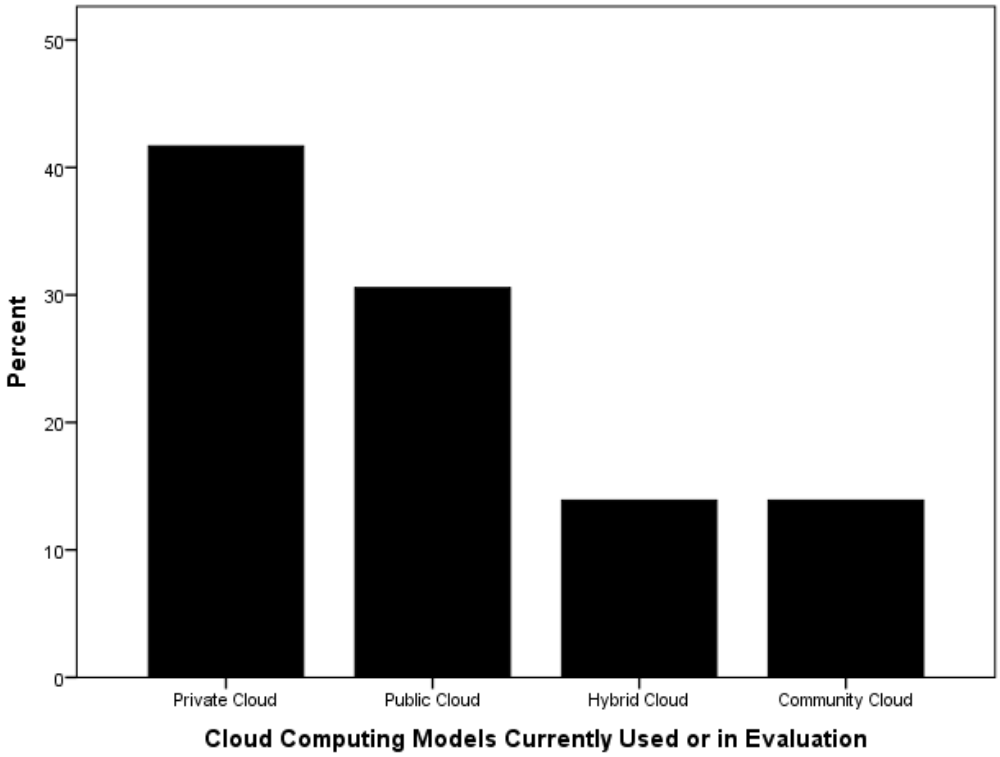


Figure 11. Distribution of Cloud technology models currently in use or under evaluation.

Inferential Results of Testing Research question

This section presents the results of testing the research questions. It begins with some descriptive statistics to show how participants responded to the elements of Cloud services addressed in each of the seven research questions. Then it presents results for each research question individually. Data were level of satisfaction on a 5-point Likert scale (dissatisfied = 1, somewhat dissatisfied = 2, neutral = 3, satisfied = 4, and very satisfied = 5). The higher the data point, the greater the satisfaction with the Cloud technology service indicated.

Descriptive Statistics of Satisfaction with Cloud Technology Services

Table 3 presents descriptive statistics for the satisfaction ratings with Cloud technology services in order from most satisfied with to least satisfied with. The TAM

model of usefulness and ease of Cloud technology use showed the highest satisfaction ratings, which reflected ratings close to satisfied with both the ease and usefulness of Cloud technology. The mean for usefulness was further supported by the mode, which indicated that the most frequent rating of Cloud technology usefulness was very satisfied. On average, participants were least satisfied with vendor compliance fulfillment.

Table 4

Descriptive Statistics of Levels of Satisfaction with Cloud Technology Services, N = 26

Cloud Technology Elements	Mean	Median	Mode	SD	Skew	Kurtosis
Usefulness of Cloud Technology (TAM)	3.85	4	5	1.08	-0.69	0.19
Ease of Use of Cloud Technology (TAM)	3.84	4	3	0.90	-0.04	-1.06
Data Availability and Data Security	3.31	3	3	0.62	0.82	1.11
Business Continuity and Service Availability	3.27	3	3	0.78	-0.53	2.23
Service Level Agreement (SLA)	3.19	3	3	0.63	0.86	1.93
Vendor Contractual Agreement	3.15	3	3	0.61	1.05	2.82
Vendor Compliance Fulfillment	3.04	3	3	0.72	-0.06	3.60

Note. SD = standard deviation. SEM = standard error of the mean. SEM of Skew = 0. 46. SEM of kurtosis = 0.89.

Correlations among satisfaction with Cloud technology services ratings are shown in Table 4. Satisfaction with Cloud-based data availability and data security, and vendor contractual agreement, correlated strongly and positively with satisfaction ratings for all of the other services. Satisfaction ratings for business continuity and service availability also correlated strongly and positively with SLA and vendor compliance fulfillment.

However, note that satisfaction ratings with TAM measures of the ease of and general usefulness of Cloud technology did not correlate with all of the other services across the board. Instead, both ease and usefulness only correlated with satisfaction with

data availability and data security, and with vendor contractual agreement. Usefulness correlated significantly with vendor compliance fulfillment whereas ease did not. Ease and use correlated strongly and positively with each other.

Table 5

Pearson's Correlation Matrix of Cloud Technology Services, N = 26 Participants

	V1	V2	V3	V4	V5	V6	V7
V1 Data Availability and Data Security	1	***.82*** **	***.49*** *	***.56*** **	***.51*** **	***.43*** *	***.46*** *
V2 Vendor Contractual Agreement	-	1	***.50*** **	***.54*** **	***.71*** **	***.46*** *	***.50*** *
V3 Business Continuity and Service Availability	-	-	1	***.87*** **	***.62*** **	.38	.30
V4 Service Level Agreement (SLA)	-	-	-	1	***.60*** **	.28	.20
V5 Vendor Compliance Fulfillment	-	-	-	-	1	***.47*** *	.39
V6 Usefulness of Cloud Technology (TAM)	-	-	-	-	-	1	***.85*** **
V7 Ease of Use of Cloud Technology (TAM)	-	-	-	-	-	-	1

Note. Statistically significant correlations are shown in bold italics for ease of viewing. *Correlation is significant at the 0.05 level (2-tailed). **Correlation is significant at the 0.01 level (2-tailed).

Results of Testing Research Questions

The following section shows the results of testing the research questions. Each research question asked if there are differences between cloud users and non-users in regards to the effect of Cloud technology service named in the question concerns on small organizations decision to adopt Cloud computing. These questions were tested with independent *t*-tests by comparing mean satisfaction with the Cloud technology service named in the question between two groups. The two groups were created by collapsing the data for the Cloud status variable shown in Figure 9 into two categories. One category included participants who were currently using or evaluating Cloud technology for use. For simplicity, the group was called Users. The other category included the

remaining participants who were not currently using Cloud technology and were not currently evaluating it for use. For simplicity, the group was called Non-users.

The expectation was that Users would be significantly more satisfied with the specific Cloud service named in the research question than were Non-users. Thus, one-tailed hypotheses were tested.

Table 6 shows the means that were compared for statistical significance in the t-tests. All of the means in Table 6 range within the point value of 3, which, on the Likert satisfaction scale used in this study, represented a "neutral" perspective. Note also that the standard deviations (SD) on Table 6 show that there was greater variability in the answers among Non-users compared to Users. Moreover, in many cases Non-users variability was as much as twice as Users.

Table 6

*Mean Satisfaction Ratings for t-Tests about Cloud Technology Services, n = 21 Users, n = 15 Non-users**

Cloud Technology Services	Current Cloud Status	Mean	SD	SEM
Data Availability and Data Security	Users	3.05	0.50	0.11
	Non-users	3.60	0.74	0.19
Business Continuity and Service Availability	Users	3.29	0.46	0.10
	Non-users	3.33	0.98	0.25
Vendor Contractual Agreement	Users	3.00	0.32	0.07
	Non-users	3.53	0.74	0.19
Service Level Agreement (SLA)	Users	3.24	0.44	0.10
	Non-users	3.27	0.80	0.21
Vendor Compliance Fulfillment	Users	3.05	0.38	0.08
	Non-users	3.27	0.96	0.25
Usefulness of Cloud Technology (TAM)	Users	3.76	0.94	0.21
	Non-users	3.87	1.06	0.27
Ease of Use of Cloud Technology (TAM)	Users	3.77	0.77	0.17
	Non-users	3.57	1.16	0.31

Note. *Ease of use of Cloud technology (TAM), *n* = 14 Non-users. SD = standard deviation. SEM = standard error of the mean.

Table 7 shows the results of independent *t*-tests. Significant differences are presented in bold italics for ease of recognition.

Table 7

Independent Samples t-Tests Results for Research Questions 1 – 7

	Levene's		t-test for Equality of Means						
	F	*p*	*t*	*df*	*p*	Mean Diff	SE Diff	95% CI Diff Lower	95% CI Diff Upper
Data Availability and Data Security*	6.47	.02	***-2.52***	***22.91***	***.01***	***-0.55***	***0.22***	***-1.01***	***-0.10***
Business Continuity*	6.46	.02	-0.18	18.53	.43	-0.05	0.27	-0.62	0.52
Vendor Contractual Agreement*	23.94	.00	***-2.62***	***17.65***	***.01***	***-0.53***	***0.20***	***-0.97***	***-0.10***
Service Level Agreement (SLA)*	4.80	.03	-0.13	19.97	.45	-0.03	0.23	-0.50	0.45
Vendor Compliance Fulfillment*	11.63	.01	-0.84	17.22	.20	-0.22	0.26	-0.77	0.33
Usefulness of Cloud Technology (TAM)	0.22	.64	-0.31	34	.38	-0.10	0.34	-0.79	0.58
Ease of Use of Cloud Technology (TAM)	2.30	.14	0.59	33	.28	0.19	0.32	-0.47	0.85

Note. *Variances are unequal so the corrected t-test results are shown. Business Continuity = Business Continuity and Service Availability. *P* = *p*-value. Levene's = Levene's Test for Equality of Variances. Mean diff = Mean Difference between means. SE Diff = standard error of the difference between means. 95% CI Diff = 95% Confidence Interval of the Difference between Means. Significant differences are shown in bold italics for ease of viewing.

RQ1: Are there differences between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing?

H_0: There is no statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

H_1: There is statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

Table 7 shows that there was sufficient evidence to reject the null hypothesis and to conclude that was a statistically significant difference in satisfaction with Cloud data security between Cloud Users and Non-users. However, the result went opposite to the predicted direction that Users would be more satisfied. That is, Figure 12 illustrates the mean and SEM from Table 6, which revealed that Non-users were more satisfied with Cloud technology data security than were Users. The effect of [lack of] exposure to Cloud technology was strong, Cohen's d = 0.84.

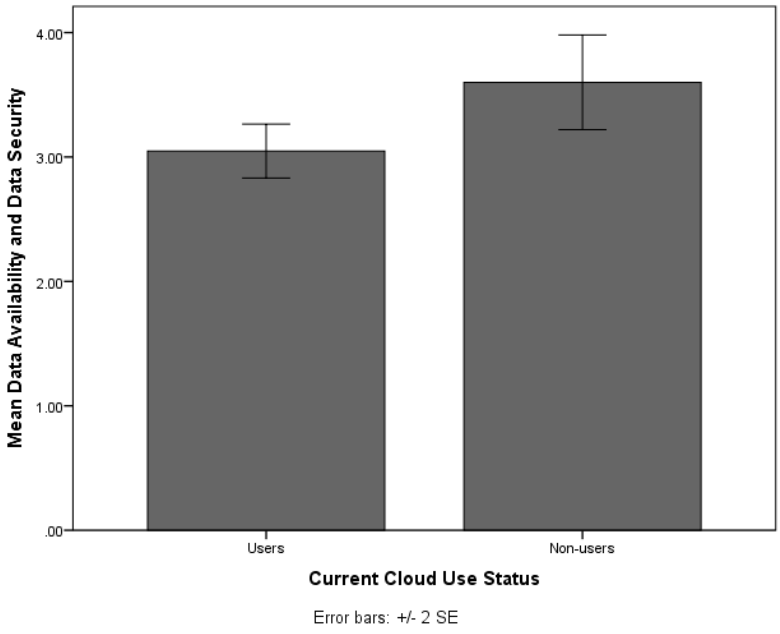


Figure 12. Mean satisfaction with Cloud technology data security in Users and Non-users.

RQ2: Are there differences between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing?

H_{02}: There is no statistically significant difference between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing.

H_{a2}: There is statistically significant difference between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing.

Table 7 shows that there was a non-significant difference between the average satisfaction ratings of business continuity and disaster recovery between Users and Non-users. The null hypothesis was retained. Figure 13 shows that the mean ratings of the two groups were in close agreement.

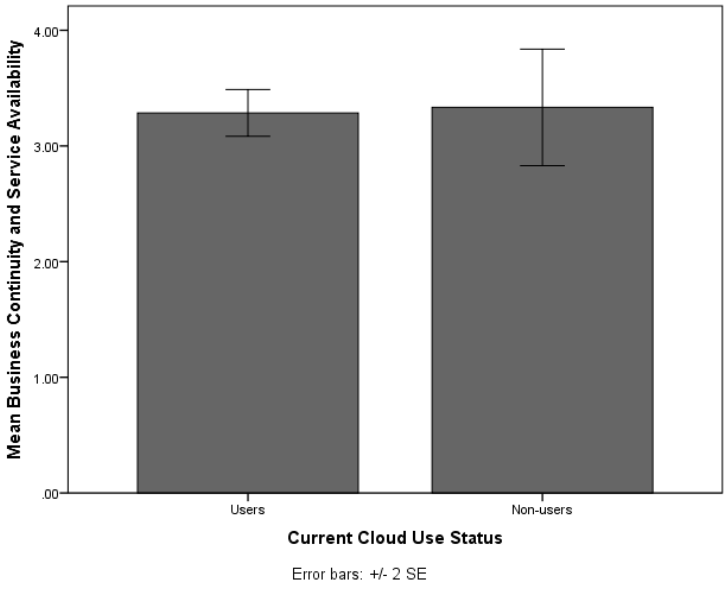


Figure 13. Mean satisfaction with Cloud technology business continuity and disaster recovery in Users and Non-users.

RQ3: Are there differences between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

H_{03}: There is no statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

H_{a3}: There is statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing.

Table 7 shows that there was sufficient evidence to reject the null hypothesis and conclude that was a statistically significant difference in satisfaction with Cloud contract lock-in between Cloud Users and Non-users. However, similar to the results for research question 1, the result went opposite to the predicted direction that Users would be more satisfied. That is, Figure 14 illustrates the mean and SEM from Table 6, which revealed that Non-users were more satisfied with Cloud technology contract lock-in than were Users. The effect of [lack of] exposure to Cloud technology was strong, Cohen's d = 1.00. Figure 14 also shows that Users rated their satisfaction as neutral; the small SEM indicates that most participants gave a neutral answer, that is, they did not have an opinion about Cloud technology contracts.

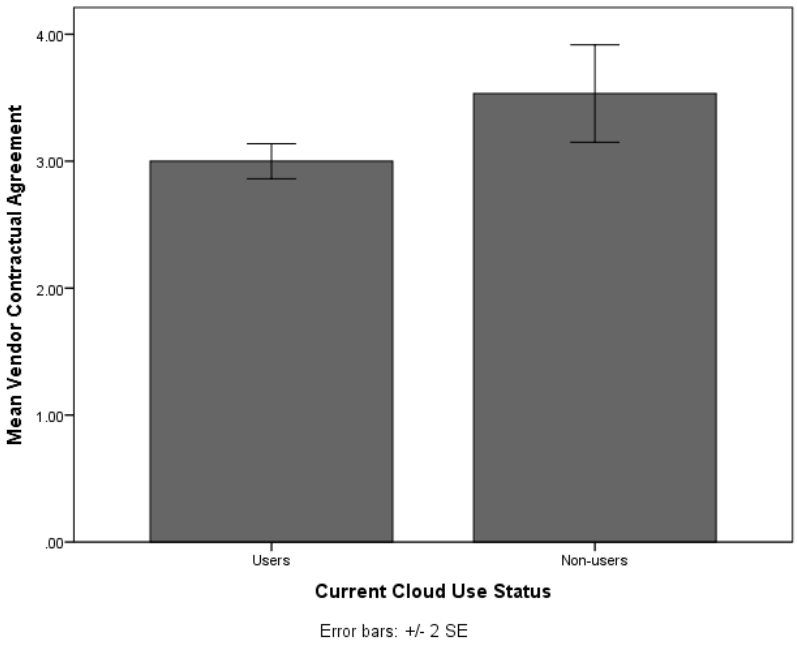


Figure 14. Mean satisfaction with Cloud technology contract lock-in between Users and Non-users.

RQ4: Are there differences between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing?

H_{04}: There is no statistically significant difference between cloud users and non-users in regards to the effect of service level agreement SLA concerns on small organizations decision to adopt Cloud computing.

H_{a4}: There is statistically significant difference between cloud users and non-users in regards to the effect of service level agreement SLA concerns on small organizations decision to adopt Cloud computing.

For research question 4, the null hypothesis was retained. Table 7 shows that there was a non-significant difference between the average satisfaction ratings of business continuity and disaster recovery between Users and Non-users. Figure 15

illustrates that the mean ratings of the two groups were virtually identical, averaging close to neutral satisfaction Cloud service level agreements.

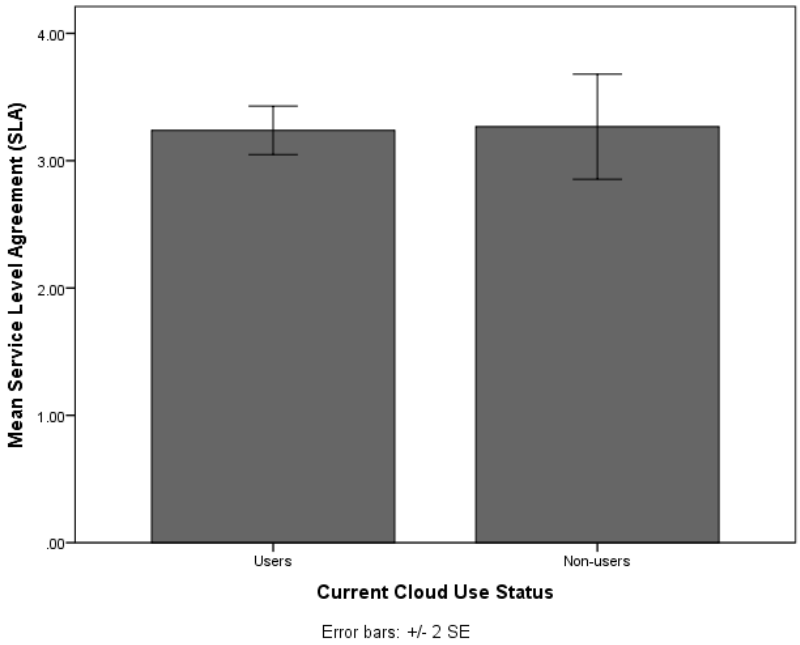


Figure 15. Mean satisfaction with Cloud service level agreements (SLA) in Users and Non-users.

RQ5: Are there differences between cloud users and non-users in regards to the effect of government regulations concerns on small organizations decision to adopt Cloud computing?

H_{05}: There is no statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

H_{a5}: There is statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

For research question 5 about compliance with government regulations, the null hypothesis was retained. Table 7 shows that there was a non-significant difference between the average satisfaction ratings of compliance with government regulations between Users and Non-users. Figure 16 show that the mean rating among Users averaged a neutral rating. Satisfaction of the Non-users was non-significantly higher with respect to Cloud technology mediating compliance with government regulations. Pertinent to this result was the finding that, of $N = 36$ participants, 8% ($n = 3$) had been fined in the last three years for regulation non-compliance compared to 92% ($n = 33$) who had not been fined.

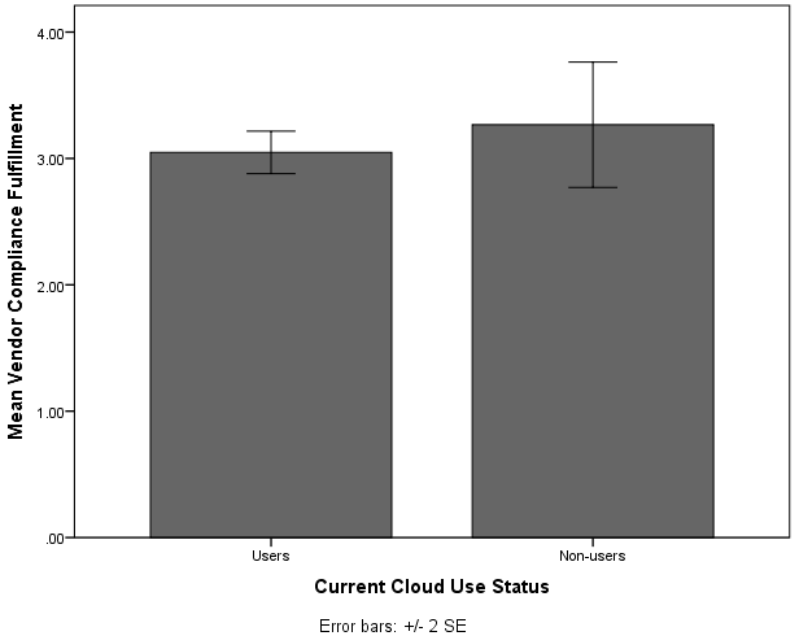


Figure 16. Mean satisfaction with Cloud mediation of compliance with government regulations Users and Non-users.

RQ6: Are there differences between cloud users and non-users in regards to the effect of technology perceived ease of use on small organizations decision to adopt Cloud computing?

H_{06}: There is no statistically significant difference between cloud users and non-users in regards to the effect of perceived ease of using technology on small organizations decision to adopt Cloud computing.

H_{a6}: There is statistically significant difference between cloud users and non-users in regards to the effect of ease of perceived using technology on small organizations decision to adopt Cloud computing.

Table 6 and Figure 17 show that the average satisfaction ratings with Cloud technology services (listed in the research question 1-5) was close to very satisfied among Users, whereas Non-users rated their satisfaction as slightly lower than did Users.

However, the difference in satisfaction was insufficient to reject the null hypothesis (Table 7). The conclusion for this question was that Users and Non-users did not differ in average satisfaction with the ease of using Cloud technology. Figure 17 shows the mean satisfaction ratings, and that Non-users were more variable in their answers.

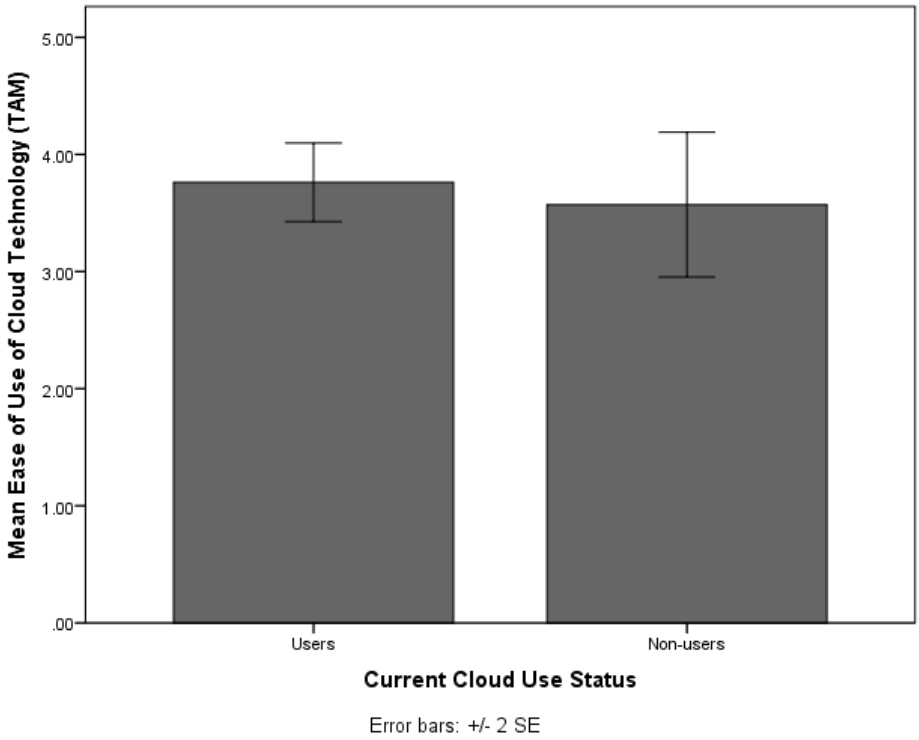


Figure 17. Mean satisfaction with the ease of using Cloud technology between Cloud Users and Non-users.

RQ7: Are there differences between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing?

Table 6 and Figure 18 show that the average satisfaction ratings with Cloud technology services (listed in the research question 1-5) was similar to ratings of the ease of using Cloud technology, in that ratings for both Users and Non-users were close to very satisfied among Users.

H_{07}: There is no statistically significant difference between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing.

H_{a7}: There is statistically significant difference between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing.

Table 7 shows the results of the *t*-test, which indicated that the difference in satisfaction between Users and Non-users was insufficient to reject the null hypothesis. The null hypothesis was retained. Figure 18 shows that the means were very close in value.

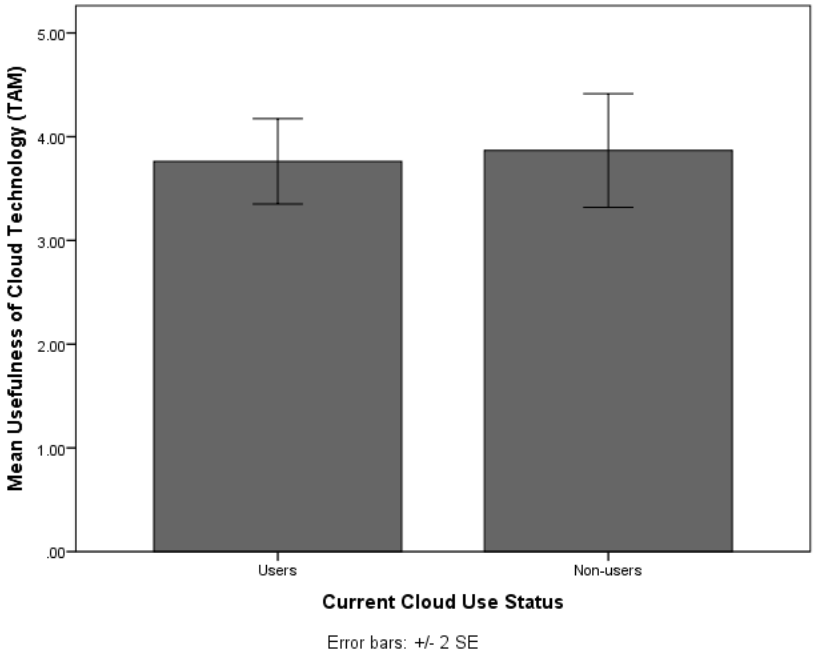


Figure 18. Mean satisfaction with the usefulness of Cloud technology between Cloud Users and Non-users.

Table 8

Summary of Hypotheses

Hypothesis	Significance	Null Rejected or not Rejected
H_{01}: Cloud users in comparison with non-users believed that data security concerns had no effect on small organizations decisions to adopt Cloud computing.	$P = .01$	Null Rejected
H_{02}: Cloud users in comparison with non-users believed that business continuity concerns had no effect on small organizations decisions to adopt Cloud computing.	$P = .43$	Null not Rejected
H_{03}: Cloud users in comparison with non-users believed that contract lock-in concerns had no effect on small organizations decisions to adopt Cloud computing.	$P = .01$	Null Rejected
H_{04}: Cloud users in comparison with non-users believed that Cloud service level agreement (SLA) had no effect on small organizations decisions to adopt Cloud computing.	$P = .45$	Null not Rejected
H_{05}: Cloud users in comparison with non-users believed that Cloud compliance with government regulations had no effect on small organizations decisions to adopt Cloud computing.	$P = .20$	Null not Rejected
H_{06}: Cloud users in comparison with non-users believed that ease of using technology had no effect on small organizations decisions to adopt Cloud computing.	$P = .38$	Null not Rejected
H_{07}: Cloud users in comparison with non-users believed that technology usefulness had no effect on small organizations decisions to adopt Cloud computing.	$P = .28$	Null not Rejected

Benefits of Cloud Technology

A major interest of the current study was a greater understanding the participants' views of the potential benefits of Cloud technology compared to other forms of data storage and retrieval. Specifically, it was of considerable interest to examine a range of Cloud features to see if participants viewed Cloud features as benefits, but also how they prioritized these perceived benefits. Correspondingly, this section provides detailed data on levels of agreement about Cloud technology to present precise information about participant perceptions.

Participants were asked to rate their level of agreement with several statements that the features of Cloud technology were benefits. Level of agreement was measured on a 5-point Likert scale (strongly disagree = 1, disagree = 2, neutral = 3, agree = 4, and strongly agree = 5). The higher the value of the data points in this section, the greater the agreement that the listed feature was beneficial to business. The features are listed in Table 9 in order from greatest to least agreement.

Table 9

Descriptive Statistics of the Level of Agreement with Survey Statements about Cloud Technology Features as Benefits

	N	Mean	Median	Mode	SD	Skew	Kurtosis
Flexibility and Business Agility	36	3.75	4.00	3[a]	0.73	0.43	-0.98
Data Backup and Disaster Recovery	35	3.66	4.00	3	0.88	-0.37	1.10
Reduces Upfront Cost	36	3.64	3.50	3	0.87	0.24	-0.80
Integration with Existing Infrastructure	36	3.39	3.00	3	0.87	-0.05	0.78
Legality and Compliance	35	3.34	3.00	3	0.68	0.02	-0.07
Contractual Agreement	35	3.14	3.00	3	0.65	-0.14	4.26
Data Loss and Privacy	7	3.14	3.00	3	0.69	-0.17	0.34
Loss of Control over Own Data	7	2.86	3.00	3	0.38	-2.66	7.00
Lack of Industry Standards	7	2.57	3.00	3	0.79	-1.76	2.36

Note. Multiple modes exist; the smallest mode is shown.

Flexibility and business agility. Participants rated the flexibility and business agility provided by Cloud technology the highest. A little over half of the participants, 58%, agreed or strongly agreed that Cloud technology provides flexibility and business agility, compared to 42% were rated their agreement as neutral. Figure 19 shows that no one disagreed that flexibility and business agility was a benefit.

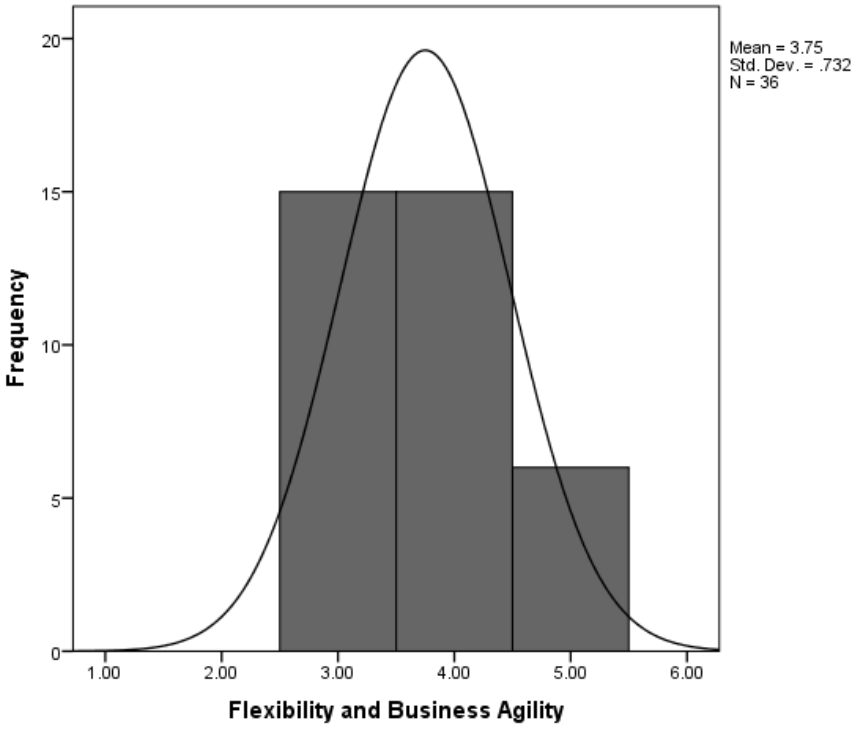


Figure 19. Frequency distribution of levels of agreement with the Cloud technology benefit of flexibility and business agility.

Data backup and disaster recovery. Participants were approximately split on the idea that the Cloud's data backup and disaster recovery feature is a benefit. Figure 20 shows that approximately half were neutral or strongly disagreed, 46%. The other 54% agreed or strongly agreed. Note that 37% agreed rather than strongly agreed.

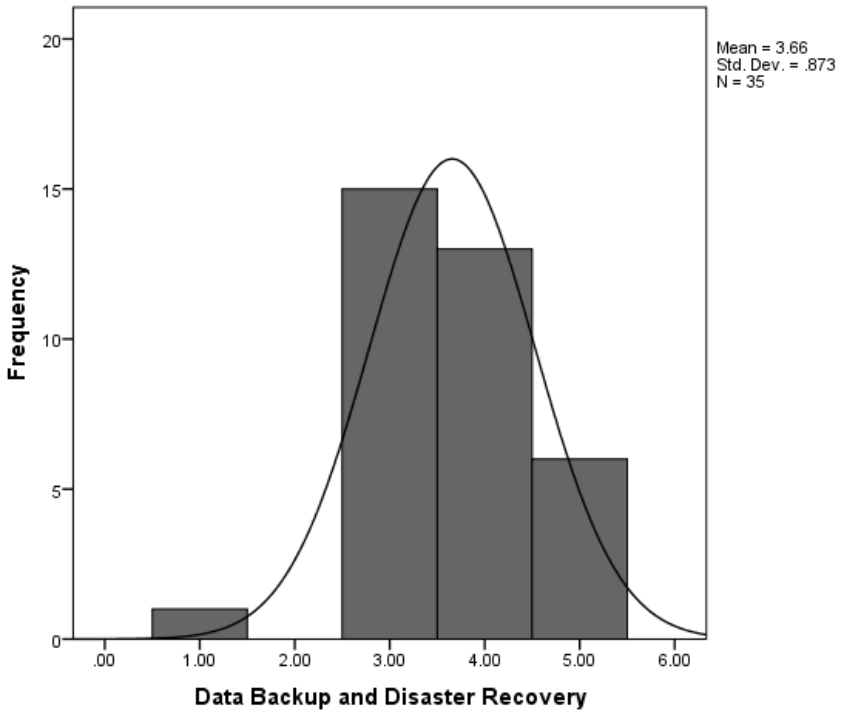


Figure 20. Frequency distribution of levels of agreement with that Cloud technology data backup and disaster recovery is a benefit to business.

Reducing up-front costs. Figure 21 shows that participants were evenly split on the question of whether one of the benefits of Cloud technology is a reduction in upfront costs. Fifty percent of participants disagreed or were neutral.

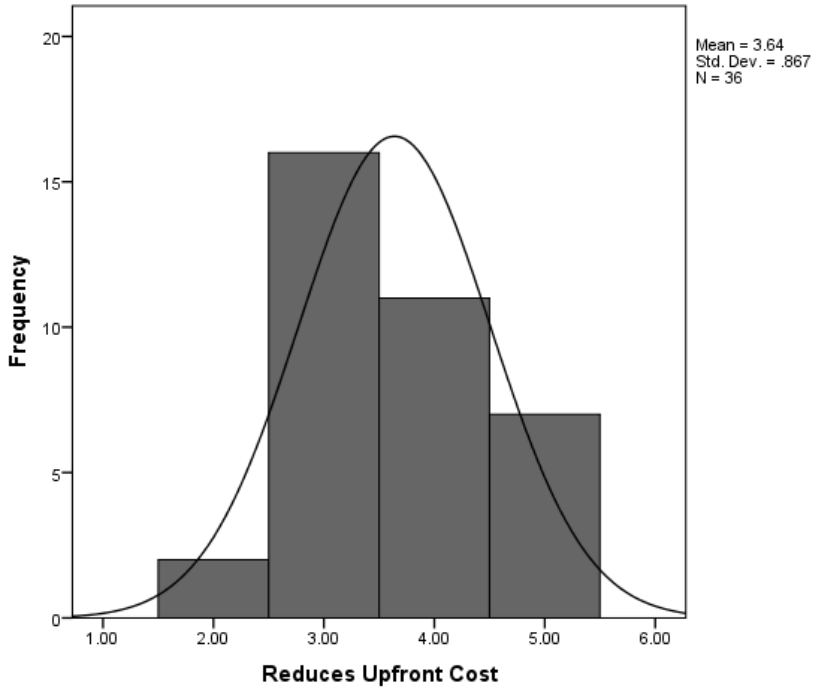


Figure 21. Frequency distribution of levels of agreement with the Cloud technology benefit of reducing upfront costs.

Integration with existing infrastructure. About half of the participants, 53%, rated integration of Cloud technology in the existing infrastructure as neutral. Over a third, 39%, agreed or strongly agreed that integration was a Cloud benefit. A small percent, 8%, disagreed and one person strongly disagreed that integration was a benefit.

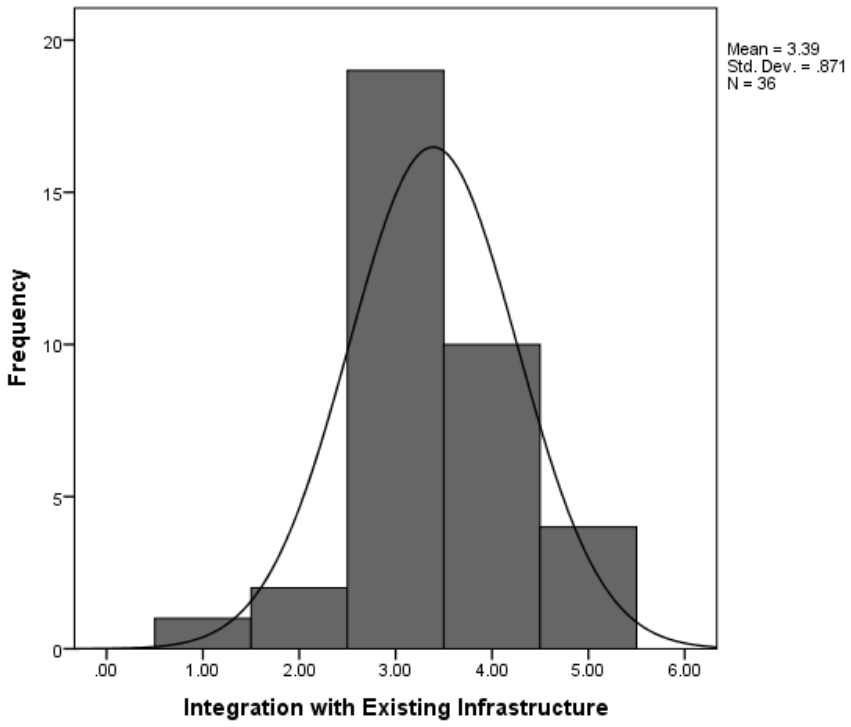


Figure 22. Frequency distribution of levels of agreement with the Cloud technology benefit of integration with existing infrastructure.

Legality and compliance. The extent to which participants agreed that legality and compliance is a Cloud technology benefit (shown in Figure 23) corresponds to the firms' applicable regulations. Table 10 shows that about a quarter of the participants' firms each had to comply with e-Discovery, FINRA, HIPPA and PCI DSS, respectively.

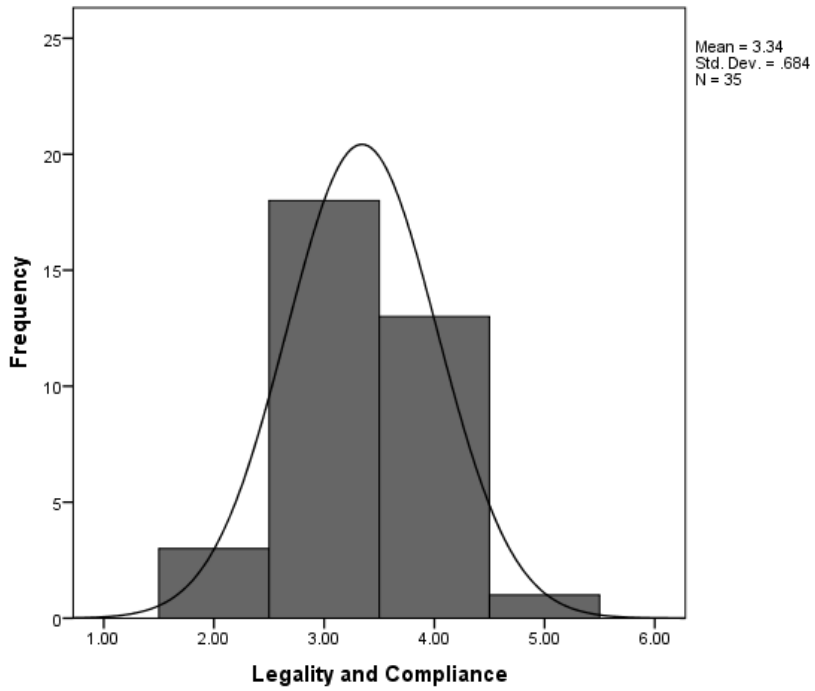


Figure 23. Frequency distribution of levels of agreement with the Cloud technology benefit of legality and compliance.

Table 10

Regulations that Apply to Participant's Firm

	Frequency	Percent	Cumulative Percent
e-Discovery: Electronic Data Discovery	7	19	19
FINRA: Financial Industry Regulatory Authority	11	31	50
Health Insurance Portability and Accountability Act	9	25	75
PCI DSS: Payment Card Industry Data Security Standard	9	25	100
Total	36	100	

There were too many missing data to run a chi-square test of independence to see if there was a statistically significant association between attitudes about legality and compliance, and applicable regulations. Instead, cross-tabulation of the two variables

(legality and compliance x applicable regulations) in Figure 24 shows that that levels of agreement were not the same across the different applicable regulations: e-Discovery: 14% disagreed, 57% were neutral, and 29% agreed; FINRA: 9% disagreed, 82% were neutral, and 9% agreed; HIPPA: 13% disagreed, 13% were neutral, and 75% agreed; PCI DSS: 0% disagreed, 44% were neutral, and 56% agreed.

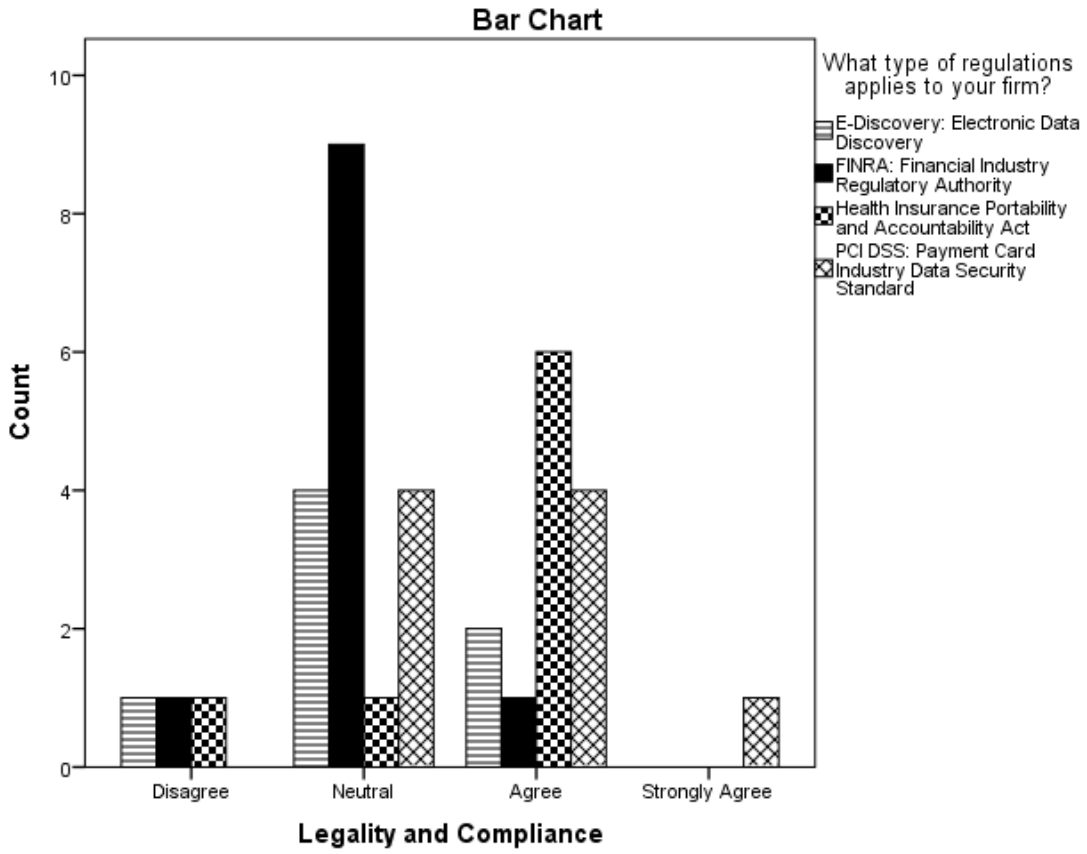


Figure 24. Cross-tabulation between applicable regulations and agreement that Cloud technology legality and compliance features are benefits to business.

Data loss and privacy. The data of levels of agreement in Figure 25 should be viewed with caution because only seven participants answered the question. They suggested that 71% of the participants disagreed or were neutral on data loss and privacy as a benefit.

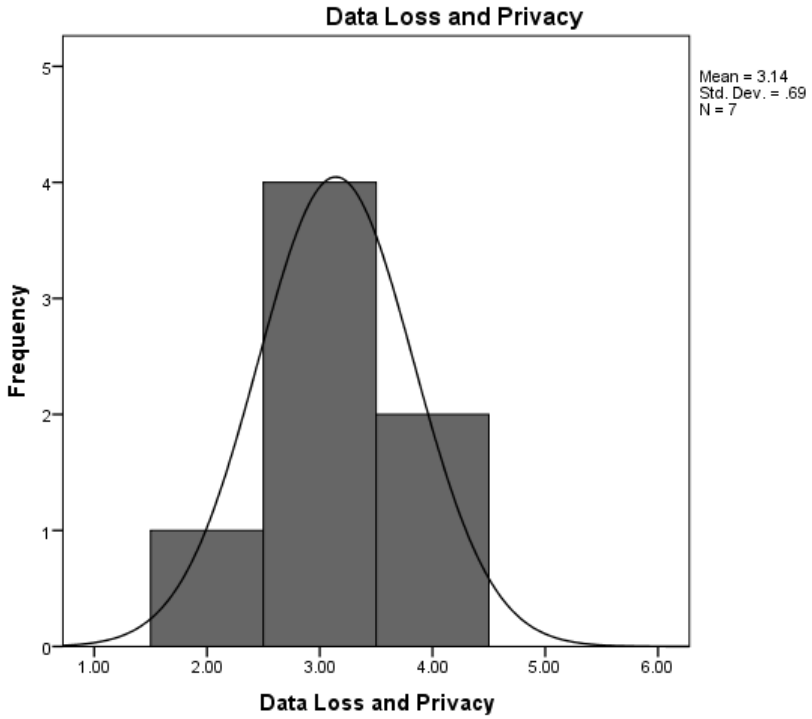


Figure 25. Frequency distribution of levels of agreement that Cloud technology data loss and privacy features are benefits to business.

Contractual agreement. The majority of participants were neutral on the statement that Cloud technology contractual agreements were a benefit to business (Figure 26).

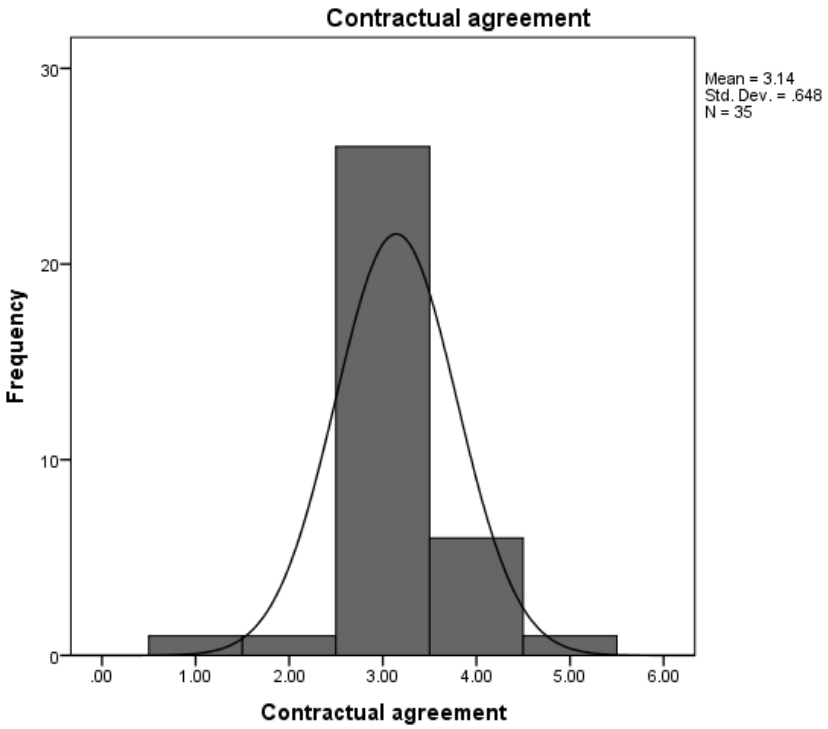


Figure 26. Frequency distribution of levels of agreement that Cloud technology contractual agreement features are benefits to business.

Loss of control over own data. Responses to the statement the Cloud technology's features with respect to loss of control over one's own data were unequivocal among the seven participants who answered this question. The majority response was neutral, 86%. The remaining 14% disagreed.

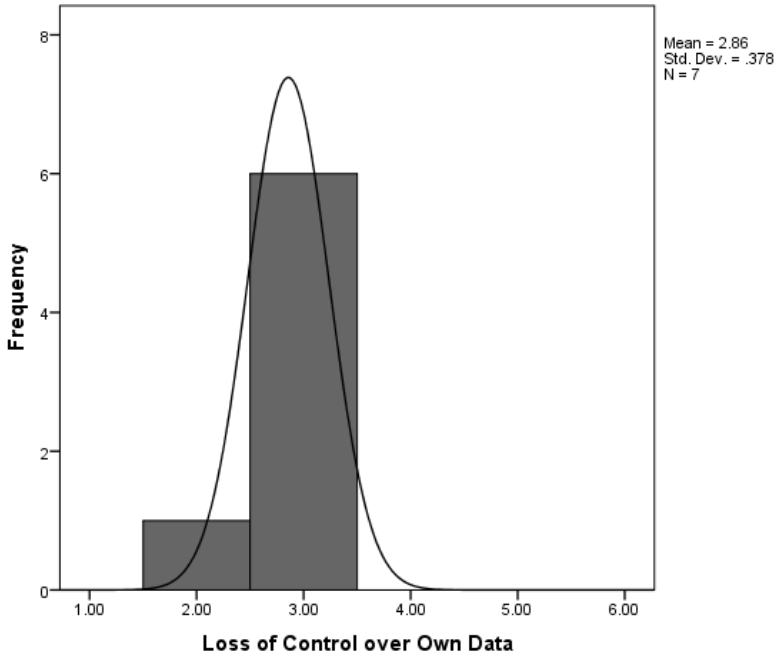


Figure 27. Frequency distribution of levels of agreement that Cloud technology features loss of control over own data are benefits to business.

Lack of industry standards. Only seven participants answered this question.

Most were neutral, 71%. The remaining 29% disagreed.

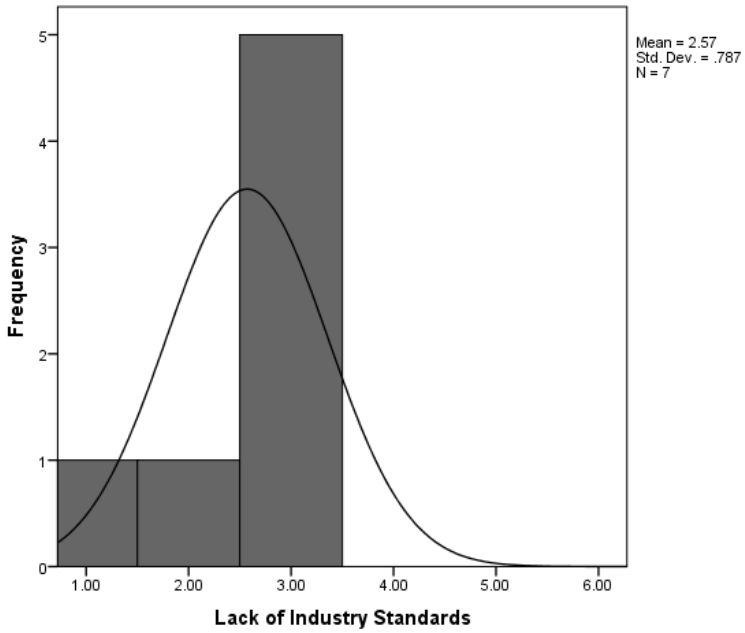


Figure 28. Frequency distribution of levels of agreement that lack of industry standards Cloud technology benefit business.

Motivators to Adopt Cloud Technology

Participants were asked to rate their likelihood of adopting Cloud technology if three services were offered. Table 9 shows that the majority of participants said that they would be motivated to adopt Cloud technology if service providers protected card holder data against misuse. Nearly as many participants said they would be motived if BAA agreements were offered. Only about half were motived by an annual audit letter.

Table 11

Motivators in Adopting Cloud Technology

Motivators to Adopt Cloud Service	Yes	No	N
If it Protected Cardholder Data against Misuse	26 (74%)	9 (26%)	35
If Cloud Service Provider Offered BAA Agreement	24 (69%)	11 (31%)	35
If it Included Annual Audit Letter	20 (57%)	15 (43%)	35

CHAPTER FIVE: DISCUSSION

The purpose of this chapter is to provide a concise summary of the research study of factor and inhibiters that contribute to small size organizations in the financial, healthcare, and leisure service industry reluctance to adopt Cloud computing technology in the United States. This chapter will provide the reader with a concise summary of information already presented in previous chapters, a recapitulation summary of the statistical data, and interpretation of finding presented in Chapter Four. This chapter is organized as follow: summary of the results, discussion of the results, recommendation for future research, and conclusion.

Summary of the Results

Cloud computing is a new approach which offers IT resources as pay-per-use services. At its core, it utilizes a distributed shared pooling of IT services (SaaS, IaaS, and PaaS) as a centralized IT services on demand (Rose et al., 2011). Recent industry surveys showed a significant increase in Cloud technology adoption among big organization but it remains static among small organizations.

The requirement for this study was aimed at participants in the IT field from small firms in the financial, health, and leisure services in the United States. The survey text is listed in Appendix A. All data were screened for entry errors. A total of 81 participants agreed to take the survey. However, numerous participants failed to answer many or all of the survey questions. Consequently, there were 35 or 36 participants for most questions. Missing data did not show any systematic pattern.

The survey questions consisted of 20 questions divided into four categories: 1) participant's demographic information; 2) the firm applicable regulatory compliance to

determine if the firm is currently in compliance with theses regulation; 3) questions to participants who currently utilize the Cloud and their level of satisfaction, and to participants who are evaluating the Cloud to understand their motives; and 4) questions to all participants (including participants who are currently utilizing, evaluating, and not considering the Cloud) to determine the level of acceptance in adopting Cloud technology should the Cloud provider secure the means for these firms to fulfill their regulation obligations.

The survey questionnaire for the study was developed by the researcher who also applied an extended model of the unified theory of acceptance TAM model to test correlation between independent and dependent variables. TAM is widely used to determine the user's intention in using or rejecting the use of technology. However, the external factors, data security and availability, disaster recovery and business continuity, SLA, contract lock-in, and compliance were tested to determine the user's level of acceptance in using the new technology.

The study employed statistical analyses with the SPSS statistical tool to determine positive significant correlation between accepting or rejecting Cloud technology and the five independent variables: 1) data security and availability, 2) disaster recovery and business continuity, 3) SLA, 4) contract lock-in, and 5) compliance. Prior to NRB approval, the researcher presented the survey to practitioner's in the field of IT to obtain their criticism and recommendations on the questions presented to participants. These questionnaires were consistent with prior IT studies on adoption of technologies (Straub, 1989). The Cronbach's alpha (α) was calculated for reliability on the five point Likert-

scale type survey items and yielded (α = .83) indicating consistency and conceptually related statements (Cronbach, 1932).

The survey was hosted by SurveyMonkey website and mailed to random recipients and posted in social media site using SurveyMonkey tools. The survey questions asked about the perception of participants who currently utilize the Cloud and the motivation of participants who are evaluating the Cloud with regards to these factors: 1) data security and availability, 2) disaster recovery and business continuity, 3) SLA, 4) contract lock-in, and 5) compliance. For increased statistical validity, only data from the 36 respondents who met the requirements were used in the data analysis.

Discussion of the Results

The foundation of this research is to determine factors that contribute to small organizations' reluctance in adopting Cloud technology. *N*=36 will be used in the remainder of this section unless *N* is otherwise specified.

Demographics: Gender, Age, and Title

Of the *N* = 36 participants who supplied gender and age information, an approximately equal number of men and women fell into each age category. About a quarter of both male and female participants fell in the 35-49 year-old category (male participants, 26%; female participants, 27%) and the 50-65 year-old category (male participants, 26%; female participants, 23%). Fewer participants were in the 18-24 year-old category (male participants, 17%; female participants, 18%) and correspondingly more were in the 25-34 year-old category (male participants, 30%; female participants, 32%).

A total of 45 participants provided information on their titles and industry. Forty percent of participants selected Other Professions and 60% selected Financial, Health, or Leisure Services. About one third, 31%, chose the other category among job titles on the survey, 29% was IT staff, 20% were IT management, and 11% were business owners.

Cloud Knowledge and Current Status

Participants were asked four questions about Cloud technology. Questions included their current knowledge about Cloud computing, their firm's current Cloud status, the Cloud services that their firm or employer currently used or was evaluating, and Cloud models that their firm or employer currently used or was evaluating. Under half (48%) of the participants were fairly new to Cloud technology, 18% had heard about Cloud technology, and 30% had beginning knowledge about it. Another third of the participants, 32%, reported intermediate knowledge about Cloud technology. A quarter of the participants, 25%, reported advanced knowledge about Cloud technology. Participants were asked to choose between three options to report their firm or employer's status with respect to Cloud technology. Twenty percent reported that they currently use one or more Cloud technology services. Just under half, 42%, were currently evaluating Cloud technology and 39% were not currently evaluating Cloud technology for their business at the time they took the survey.

Using Cloud Services and Models

Participants were asked to report how their firm or employer used Cloud technology from a list of three services options: Software as a Service or SaaS, as infrastructure or IaaS, and computer platform or PaaS. The most frequent use of Cloud technology was using its software (SaaS, 50%), followed by as infrastructure (IaaS,

17%), and as a platform (PaaS, 14%). Small percentages of participants reported using two of the three Cloud technology services (11%) and only 8% reported using all three services. With regards to Cloud technology models such as public, private, hybrid, and community models, three-quarters of the participants reported using private Cloud (42%) or public Cloud (31%). A much smaller but equal proportion reported hybrid Cloud (14%) or community Cloud use (14%).

The results showed that Cloud services are mostly being used with 50% of participant's who responded that currently use SaaS. However, the results are concise with our predictions that small firms do not have the infrastructure and most likely would only use the software offering of the Cloud, which only requires a computer with Internet connection and a browser to connect to the Cloud provider to perform their daily operation. The results further revealed that of the four Cloud technology models, 42% are using the private Cloud, which is an indication that many clients still do not trust the public Cloud and would rather have their own private Cloud.

Participants were presented with a set of questions to determine their acuity of Cloud computing. These questions correlate with the independent variables and revealed the following information.

Flexibility and Business Agility

Participants rated the flexibility and business agility provided by Cloud technology the highest. A little over half of the participants, 58%, agreed or strongly agreed that Cloud technology provides flexibility and business agility, compared to 42% who rated their agreement as neutral.

Data Backup and Disaster Recovery

Participants were approximately split on the idea that the Cloud's data backup and disaster recovery feature is a benefit. Approximately half were neutral or strongly disagreed, 46%. The other 54% agreed or strongly agreed. Note that 37% agreed rather than strongly agreed.

Reducing Up-Front Costs

Participants were evenly split on the question of whether one of the benefits of Cloud technology is a reduction in upfront costs. Fifty percent of participants disagreed or were neutral.

Integration with Existing Infrastructure

About half of the participants, 53%, rated integration of Cloud technology in the existing infrastructure as neutral. Over one third, 39%, agreed or strongly agreed that integration was a Cloud benefit. A small percent, 8%, disagreed. One person strongly disagreed that integration was a benefit.

Legality and Compliance

The extent to which participants agreed that legality and compliance is a Cloud technology benefit corresponds to the firms' applicable regulations. A quarter of the participants' firms had to comply with e-Discovery, FINRA, HIPPA, and PCI DSS, respectively. However, results revealed that participants did not feel that a Cloud provider provides the tools to comply with regulations. The results were e-Discovery: 14% disagreed, 57% were neutral, and 29% agreed; FINRA: 9% disagreed, 82% were neutral, and 9% agreed; HIPPA: 13% disagreed, 13% were neutral, and 75% agreed; PCI DSS: 0% disagreed, 44% were neutral, and 56% agreed.

Data Loss and Privacy

The data of levels of agreement should be viewed with caution because only *N*=7 participants answered the question. They suggested that 71% of the participants disagreed or were neutral on data loss and privacy as a benefit.

Contractual Agreement

The majority of participants were neutral on the statement that Cloud technology contractual agreements were a benefit to business.

Loss of Control Over Own Data

Responses to the statement the Cloud technology's features with respect to loss of control over one's own data were unequivocal among the *N*=7 participants who answered this question. The majority response was neutral, 86%. The remaining 14% disagreed.

Lack of Industry Standards

Only *N*=7 participants answered this question. Most were neutral, 71%. The remaining 29% disagreed. These results indicate that many participants are not familiar with the Cloud industry standards considering being a new innovation.

Motivators to Adopt Cloud Technology

Participants were asked to rate their likelihood of adopting Cloud technology if three services were offered. The majority of participants (*N*=35*)* said that they would be motivated to adopt Cloud technology if service providers protected card holder data against misuse. Nearly as many participants said they would be motivated if BAA agreements were offered. Only about half were motivated by an annual audit letter.

Research Questions and Hypothesis Testing

Seven research questions and corresponding hypotheses were developed for examination. Each research question asked if the Cloud technology service named in the question hindered small organizations from adopting Cloud computing technology. The questions were tested with independent *t*-tests by comparing mean satisfaction with the Cloud technology service named in the question between two groups. The two groups were created by collapsing the data for the Cloud status variable shown in Figure 9 into two categories. One category included participants who were currently using or evaluating Cloud technology for use. For simplicity, the group was called Users. The other category included the remaining participants who were not currently using Cloud technology and were not currently evaluating it for use. For simplicity, the group was called Non-users. The main research question was as follows:

What cultivates Small Size Organization's reluctance to adopt Cloud computing?

Based on the underlying research questions with regards to the independent variables that hinders Cloud adoption: data security and availability, disaster recovery and business continuity, SLA, contract lock-in, and compliance the following hypotheses were tested:

RQ1: Are there differences between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing?

H_0: There is no statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

H_1: There is statistically significant difference between cloud users and non-users in regards to the effect of data security concerns on small organizations decision to adopt Cloud computing.

There was sufficient evidence to reject the null hypothesis ($p = .01$) and to conclude that was a statistically significant difference in satisfaction with Cloud data security between Cloud Users and Non-users. However, the result went opposite of the predicted direction that Users would be more satisfied. The test results revealed that Non-users were more satisfied with Cloud technology data security than were Users. The effect of [lack of] exposure to Cloud technology was strong, Cohen's ($d = 0.84$). However, with Non-users believing that the Cloud provider offers security and data availability, not considering adopting remains questionable but could be that they are not the decision makers within their firm. Moreover, the results found that 39% of participants are not currently considering Cloud technology due their perception to its security

RQ2: Are there differences between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing?

H_{02}: There is no statistically significant difference between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing.

H_{a2}: There is statistically significant difference between cloud users and non-users in regards to the effect of business continuity and disaster recovery concerns on small organizations decision to adopt Cloud computing.

Data analysis showed there was a non-significant difference (p = .43) between the average satisfaction ratings of business continuity and disaster recovery between Users and Non-users. The null hypothesis was retained. The results showed the mean ratings of the two groups were in close agreement.

RQ3: Are there differences between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

H_{03}: There is no statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing?

H_{a3}: There is statistically significant difference between cloud users and non-users in regards to the effect of contract lock-in concerns on small organizations decision to adopt Cloud computing.

Data analysis showed there was sufficient evidence to reject the null hypothesis (p = .01) and conclude that was a statistically significant difference in satisfaction with Cloud contract lock-in between Cloud Users and Non-users. However, similar to the results for research question 1, the result went opposite of the predicted direction that Users would be more satisfied. The effect of [lack of] exposure to Cloud technology was strong, Cohen's (d = 1.00). Users rated their satisfaction as neutral; the small SEM

indicates that most participants gave a neutral answer, that is, they did not have an opinion about Cloud technology provider contracts.

RQ4: Are there differences between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing?

H_{04}: There is no statistically significant difference between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing.

H_{a4}: There is statistically significant difference between cloud users and non-users in regards to the effect of service level agreement (SLA) concerns on small organizations decision to adopt Cloud computing.

For research question 4, the null hypothesis was retained (p = .45). The results showed there was a non-significant difference between the average satisfaction ratings of business continuity and disaster recovery between Users and Non-users. The mean ratings of the two groups were virtually identical, averaging close to neutral satisfaction Cloud service level agreements. These results coordinate with much business's disaster recovery and business continuity plans. These backup plans are stored outside their premises.

RQ5: Are there differences between cloud users and non-users in regards to the effect of government regulations concerns on small organizations decision to adopt Cloud computing?

H_{05}: There is no statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

H_{a5}: There is statistically significant difference between cloud users and non-users in regards to the effect of compliance with government regulations concerns on small organizations decision to adopt Cloud computing.

For research question 5 about compliance with government regulations, the null hypothesis was retained (p = .2). There was a non-significant difference between the average satisfaction ratings of compliance with government regulations between Users and Non-users. The mean rating among Users averaged a neutral rating. Satisfaction of the Non-users was non-significantly higher with respect to Cloud technology mediating compliance with government regulations. Pertinent to this result was the finding that, of N = 36 participants, 8% (n = 3) had been fined in the last three years for regulation non-compliance compared to 92% (n = 33) who had not been fined.

RQ6: Are there differences between cloud users and non-users in regards to the effect of technology perceived ease of use on small organizations decision to adopt Cloud computing?

H_{06}: There is no statistically significant difference between cloud users and non-users in regards to the effect of perceived ease of using technology on small organizations decision to adopt Cloud computing.

H_{a6}: There is statistically significant difference between cloud users and non-users in regards to the effect of ease of perceived using technology on small organizations decision to adopt Cloud computing.

Table 5 and Figure 17 show that the average satisfaction ratings with Cloud technology services (listed in the research question 1-5) was close to very satisfied among Users, whereas Non-users rated their satisfaction as slightly lower than did Users.

However, the difference in satisfaction was insufficient to reject the null hypothesis (Table 7). The conclusion for this question was that Users and Non-users did not differ in average satisfaction with the ease of using Cloud technology. Figure 17 shows the mean satisfaction ratings, and that Non-users were more variable in their answers.

RQ7: Are there differences between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing?

H_{07}: There is no statistically significant difference between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing.

H_{a7}: There is statistically significant difference between cloud users and non-users in regards to the effect of technology perceived usefulness on small organizations decision to adopt Cloud computing.

The average satisfaction ratings with Cloud technology services (listed in the research question 1-5) was similar to ratings of the ease of using Cloud technology, in that ratings for both Users and Non-users were close to very satisfied among Users. Participants who were satisfied with the ease of using Cloud technology were also satisfied with its usefulness; however, participants who were not satisfied with the ease of using Cloud technology were also not satisfied with its usefulness. This may suggest a

"coupling" of the views of the Cloud: if it is easy, it must be useful and vice versa; if it is not easy, it must not be useful. The results of the *t*-test indicated that the difference in satisfaction between Users and Non-users was insufficient to reject the null hypothesis. The null hypothesis was retained as the means were very close in value.

The survey responses showed that participants were neutral in most of their responses, which helps us derive a new knowledge from this study and presume the following: 1) Survey participants who currently adopt Cloud technology are satisfied with the cloud provider services; hence they had no opinion to share. 2) Survey participant lacks the knowledge of cloud computing, therefore education is a key to motivate laggers.

Recommendation for Future Research

The survey results showed that the majority of participant were IT staff or IT managements but did not specifically ask if they were the firm's decision maker.

Therefore, a recommendation of using this survey is to target decision maker within a firm to refine the results and get a better understanding of their perceptions of the Cloud adoption. The survey asks random questions about the level of satisfaction of users who currently use or evaluating the Cloud, while this is a valid question to understand their experience and motives. A valuable approach should separate "currently in use" from "currently being considered" to get a finer-scaled picture of the current uses and attitudes about Cloud technology.

The study targeted individuals from the Financial, Health, and leisure services with the applicable industry laws and regulations. Future research should target other

industries to see if the Cloud provider is willing to secure their compliance. Lastly, future research should investigate if Network Bandwidth is an obstacle since many clients or tenants share one datacenter. This indeed is in line with the suggested future research identified by Armbrust et al. (2010) on Cloud technology growth obstacles which are: Performance Unpredictability, Data Transfer Bottlenecks, Scalable Storage, Bugs in Large- Scale Distributed Systems, and Reputation Fate Sharing.

Conclusion

The purpose of this quantitative study was to evaluate barriers that contribute to Cloud technology adoption reluctance among small organizations in the financial, health, and leisure services industry. Seven research questions and corresponding hypotheses were developed for examination. Each research question asked if there are differences between cloud users and non-users in regards to the effect of cloud technology service named on small organizations decision to adopt Cloud computing. The questions were tested with independent *t*-tests by comparing mean satisfaction with the Cloud technology service named in the question between two groups. The test results of the *t*-distribution with a 95% confidence interval level showed that cloud users and non-users had no statistically significant difference in regards to the effect of data security and contract lock-in agreement concerns on small organizations decision to adopt Cloud. Whereas, the difference between the two groups in regards to business continuity and disaster recovery, service level agreement (SLA), and regulatory compliance had statistically significant concerns in adopting the cloud. Additionally, a significant percentage of participant responded that they would strongly consider adopting the cloud should the cloud provider provide the tools to secure their fulfillment with industry and

government regulations. These results were somewhat concise with finding in the literature review.

The study anticipated to contribute to the body of knowledge by providing empirical evidence on compliance that researchers can use in evaluating other industries when adopting Cloud technology. The research encompasses a survey questionnaire, hypothesis testing which was formulated around an extended model of TAM, and data analysis. The projected TAM model introduced in this study can be utilized in future studies to test other possible external variables.

REFERENCES

ABA Technology eReport. (2011). Retrieved from http://www.americanbar.org /newsletter /publications/technology_e_report_home/2011_mar_issue /technotes.html

Abadi, D. (2009). Data management in the Cloud: Limitations and opportunities. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*. Retrieved from http://cs-www.cs.yale.edu/homes/dna/papers/abadi-Cloud-ieee09.pdf

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly,* 227-247

Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies?. *Decision Sciences*, *30*(2), 361-391.

Ali, M. F., Younis, M. I., Zamli, K. Z., & Ismail, W. (2010). Development of Java based RFID application programmable interface for heterogeneous RFID system. *Journal of Systems and Software*, *83*(11), 2322-2331.

Allen, B. M. (2012). *A Factor Analysis of Noncompliance in the Payment Card Industry* (Doctoral dissertation, Walden University).

Amirkhani, A., Salehahmadi, Z., Hajialiasgari, F., & Nikafkar, N. (2011). A new integrated TBT-TAM model for Mobile Marketing Adoption in Insurance Industry. *Interdisciplinary Journal of Contemporary Research in Business, 3*(3), 855-866.

Amoroso, A., Spencer, D. E., & Redfield, R. R. (2004). Improving on success: What treating the urban poor in America can teach us about improving antiretroviral programs in Africa. *AIDS*, *18*, S39-S43.

Anderson, K. (Ed.). (2009). *Distortions to agricultural incentives: A global perspective, 1955-2007*. World Bank Publications.

Andrés, L., Cuberes, D., Diouf, M., & Serebrisky, T. (2010). The diffusion of the Internet: A cross-country analysis. *Telecommunications Policy, 34*, 323 -340. doi: 10.1016/j.telpol

Arbuckle, J. L. (1996). Full information estimation in the presence of incomplete data. *Advanced structural equation modeling: Issues and techniques*, 243-277.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of Cloud computing. *Communications of the ACM*, *53*(4), 50-58.

Barr, R. (2013). Qualys Inc. How to gain comfort in losing control to the Cloud.

Bates, T. (2005). Analysis of young, small firms that have closed: Delineating successful from unsuccessful closures. *Journal of Business Venturing, 20*, 343-358. doi: 10.1016/j.jbusvent.2004.01.003

Bittman, T. J. (2006). Achieving Agility: The Data Center Is the Foundation Gartner, Inc.

Bowers, K. D., Juels, A., & Oprea, A. (2009, November). HAIL: a high-availability and integrity layer for Cloud storage. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 187-198). ACM.

Burton-Jones, A., & Hubona, G. S. (2006). The mediation of external variables in the technology acceptance model. *Information & Management, 43*, 706-717. doi: 10.1016/j.im.2006.03.007

Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented Cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on* (pp. 5-13). Ieee.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24-38.

Charles, C. M., & Mertler, C. A. (2002). *Introduction to educational research* (4th ed.). Boston, MA: Allyn and Bacon.

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Research report: empirical test of an EDI adoption model. *Information systems research*, *12*(3), 304-321.

Cloud Security Alliance (CSA). (2011). Defined categories of service. Retrieved from https://cloudsecurityyalliance.org/wp-content/uploads/2011/09/SecaasV10.pdf

Creswell, J. W. (2012). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Cronbach, A. (1932). *The Jewish peace book for home and school*. Dept. of Synagogue and school extension of the Union of American Hebrew congregations.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1993). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Dekker, M., & Hogben, G. (2011). Survey and analysis of security parameters in Cloud SLAs across the European public sector. Online abrufbar unter: http://www. enisa. europa. eu/activities/Resilience-and-CIIP/Cloud-computing/survey -and-analysisof-security-parameters-in-Cloud-slas-across-the-european -public-sector.

Dwivedi, Y., & Mustafee, N. (2010). It's unwritten in the Cloud: The technology enablers for realizing the promise of Cloud computing. *Journal of Enterprise Information Management, 23*(6), 673-679. doi: 10.1108/17410391011088583

Ekanayake, J., Qui, X., Gunarathne, T., Beason, S., & Fox, G. (2010). High performance parallel computing with Cloud and Cloud technologies. *Journal of Information Systems, 2*(4), 1-39. doi: 10.1007/978-3-642-12636-9_2

European Network and Information Security Agency (ENISA). (2011). Survey and analysis of security parameters in Cloud SLAs across the European public sector.

FaceTime. (2014). FINRA: Compliance Guide Social Networks, Web 2.0 and Unified Communications. Retrieved from http://docs.bankinfosecurity.com/files /whitepapers /pdf/370_whitepaper_FaceTime_FINRA_SocNet.pdf

Forrester Research. (2009). Is Cloud computing ready for the enterprise? Forrester Research Report, May. Retrieved from http://forrester.com

Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., ...& Stoica, I. (2009). Above the Clouds: A Berkeley view of Cloud computing. *Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Rep. UCB/EECS*, *28*, 13.

Gaspay, A., Dardan, S., & Legorreta, L. (2008). Distance learning through the lens of learning models: New outlets for innovation. *Review of Business Research*, *8*(4).

Gill, R. (2011). Why Cloud computing matters to finance. *Strategic Finance*, *92*(7), 43-47.

Gliner, J. A., Morgan, G. A., & Leech, N. L. (2000). *Research methods in applied settings: An integrated approach to design and analysis*. Psychology Press.

Greiner, L., & Paul, L. G. (2007). SLA definitions and solutions. Retrieved from http://www .cio.com/article/128900/SLA_Definitions_and_Solutions

Hayes, B. (2008). Cloud computing: As software migrates from local PCs to distant Internet servers, users and developers alike go along for the ride. *News Technology*, 9-11. doi: 10.1145/1364782.1364786

Herrmann, W. (2008). Cloud computing – das Buzzword des Jahres? Retrieved from http://informationweek.de/showarticle.jhtml?articleID=207800804&pgno=1

Himmel, M. A. (2012). Qualitative analysis of Cloud Computing risks and framework for the rationalization and mitigation of Cloud risks. *ETD Collection for Pace University.* Paper AAI3520142. Retrieved from http://digitalcommons .pace.edu/dissertations /AAI3520142

ISACA. (2007). CobiT, Retrieved from www.isaca.org/cobit/

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public Cloud computing. *NIST Special Publication*, *800*, 144.

Kim, H., Lim, H., Jeong, J., Jo, H., & Lee, J. (2009, March). Task-aware virtual machine scheduling for I/O performance. In *Proceedings of the 2009 ACM SIGPLAN /SIGOPS international conference on Virtual execution environments* (pp. 101-110). ACM.

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management, 43*(6)*,* 740-755. doi: 10.1016/j.im.2006.05.003

Krigsman, M. (2008). Mediamax/the linkup: When the Cloud fails. *IT Project Failures, News and Blogs, ZDNet*.

Kumekawa, J. (2005). Overview and summary: HIPAA: How our health care world has changed. *OJIN: The Online Journal of Issues in Nursing*, *10*(2).

Leavitt, N. (2009). Is Cloud computing really ready for prime time?. *Computer*, *42*(1), 15-20.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, *12*(1), 50.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information and Management, 40*(3), 191-204. doi: 10.1016/S0378-7206(01)00143-4

Leong, L., & MacDonald, N. (2011). Cloud IaaS: Security Considerations. Report No. G00210095.

Loeb & Loeb. (2013). Outsourcing the law alert. Retrieved from http://www.loeb.com

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance*. "O'Reilly Media, Inc."

McFarland, D. J., & Hamilton, D. (2006). Adding contextual specificity to the technology acceptance model. *Computers in Human Behavior, 22*(3), 427-447. doi: 10.1016/j.chb.2004.09.009

McGee, M. (2013). HIPAA breaches in the Cloud. 2 Oregon incidents reveal omnibus fog. Retrieved from http://www.healthcareinfosecurity.com/hipaa-breaches-in-Cloud-a-5959

McNulty, E. (2007). Boss, I think someone stole our customer data. *Harvard Business Review*, *85*(9), 37.

Michael, S., & Pearce, J. (2009). The need for innovation as a rationale for government involvement in entrepreneurship. *Entrepreneurship and Regional Development, 21*(3), 285-302. doi: 10.1080/08985620802279999

Mills, E. (2009). Cloud computing security forecast: Clear skies. *CNET News.*

Mirzaei, N. (2008). Cloud Computing. *Pervasive Technology Institute Report, Community Grids Lab, Indiana University*, 1-12.

Misra, S. C., & Mondal, A. (2011). Identification of a company's suitability for the adoption of Cloud computing and modeling its corresponding ROI. *Mathematical and Computer Modeling, 53*(4), 504-520.

Nesbary, D. (2000). *Survey research and the World Wide Web*. Needham Heights, MA: Allyn and Bacon.

NIST, S. (2012). 500-292: Cloud computing reference architecture, v1. 0.

Ochieng, D. O., Waema, T. M., & Onsomu, J. O. (2012). Mobile Interfaced Crops Diagnosis Expert System (MICDES): A case for rural Kenyan farmers. *International Journal Services, Economics and Management, 4*(1), 4-26.

Opitz, N., Langkau, T. F., Schmidt, N. H., & Kolbe, L. M. (2012, January). Technology acceptance of Cloud computing: Empirical evidence from German IT

departments. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 1593-1602). IEEE.

Pan, M., & Jang, W. (2008). Determinants of the adoption of enterprise resource planning within the technology-organization-environment framework: Taiwan's communications. *Journal of Computer Information Systems*, *48*(3), 94-102.

PCI. (2010). Payment Card Industry (PCI) Data Security Standard. *PCI DSS Requirements and Security Assessment Procedures, Version 2.0.* s.l.

Rayport, J. F., & Heyward, A. (2009). Envisioning the Cloud: The Next Computing Paradigm. Marketspace.

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public Cloud. *IEEE Internet Computing*, *16*(1), 69-73.

Rodrigues, T. (2013). What us businesses should know about compliance and regulatory issues before adopting a Cloud strategy. *Cloud: How to do SaaS Right*. Retrieved from http://www.zdnet.com/what-us-businesses-should-know-about-compliance-and-regulatory-issues-before-adopting-a-Cloud-strategy-7000012085/

Rogers, E. M. (1982). *Diffusion of innovation* (3rd ed.). New York, NY: The Free Press.

Rose, P. W., Beran, B., Bi, C., Bluhm, W. F., Dimitropoulos, D., Goodsell, D. S., ... & Bourne, P. E. (2011). The RCSB Protein Data Bank: Redesigned web site and web services. *Nucleic Acids Research*, *39*(suppl 1), D392-D401.

Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard Business Press.

Security Guidance for Critical Areas of Focus in Cloud Computing. (2009). Cloud Security Alliance. Retrieved from https://Cloudsecurityalliance.org /csaguide.pdf

Shackelford, J. S. (2009). The promise and peril of property rights formalization. *Social Science Research Network*, 1-53. Retrieved from http://ssrn.com/

Small Business Act. (1979). Title 48: Federal acquisition regulations system, Part 19-Small business programs. Washington, DC: U.S. Government Printing Office. Retrieved from http://ecfr.gpoaccess.gov/cgi/t/text/textidx? c=ecfr;sid =95e6aceaea6ee2b0bf8d1e96b077bcb4;rgn=div8;view=text;node= 48%3A1.0.1.4.19.0.1.1;idno=48;cc=ecfr

Staten, J., Yates, S., Gillett, F. E., Saleh, W., & Dines, R. A. (2008). *Is Cloud computing ready for the enterprise?* Cambridge, MA: Forrester Research.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147-169.

Sue, V. M., & Ritter, L. A. (2007). *Conducting online surveys*. Thousand Oaks, CA: Sage.

Sultan, R. (2009). Cloud computing to education: A new dawn? *International Journal of Information Management, 30*(2), 109-116.

Taylor, C. W., & Hunsinger, D. S. (2011). A study of student use of Cloud computing applications. *Journal of Information Technology Management, 22*(3), 36-50.

Thong, J. Y. L., Venkatesh, V., Xu, X., Hong, S. J., Tam, K. Y., Hsu, I. C., & Sabherwal, R. (2011). Ensuring quality science from "R" to "D": An optimal adoption strategy for in-licensing of pharmaceutical innovation.....

Udoh, E. (2012). Technology Acceptance Model Applied to the Adoption of Grid and Cloud Technology. *International Journal of Grid and High Performance Computing (IJGHPC)*, *4*(1), 1-20.

U.S. Department of Health & Human Services. (2003). Entities covered by HIPAA privacy rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa /understanding/training /coveredentities.pdf

van Ommeren, E., & van den Berg, M. (2011). *Seize the Cloud: A Manager's Guide to Success with Cloud Computing*. IBM Press.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the Clouds: Towards a Cloud definition. *ACM SIGCOMM Computer Communication Review*, *39*(1), 50-55.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11,* 342-365. doi: 10.1287 /isre.11.4.342.11872

Venkatesh, V., & Brown, S. (2001). A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges. *MIS Quarterly, 25*(1), 71-102.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

Viega, J. (2009). Cloud computing and the common man. *Computer*, *42*(8), 106-108.

Walczuch, R., Van Braven, G., & Lundgren, H. (2000). Internet adoption barriers for small firms in the Netherlands. *European Management Journal*, *18*(5), 561 -572.

Wang, Y. S., & Shih, Y. W. (2009). Why do people use information kiosks? A validation of the Unified Theory of Acceptance and Use of Technology. *Government Information Quarterly, 26*(1), 158-165.

Windows Azure SLA. (2014). Retrieved from http://www.microsoft.com /windowsazure/sla/

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. *Information Systems Research*, *16*(1), 85-102.

Zhu, K., & Kraemer, K. (2005). Post-adoption variations in usage and value of e-business by organizations: cross-country evidence from the retail industry. *Information Systems Research*, *16*(1), 61-84.

Zhu, K., Kraemer, K., & Xu, S. (2003). Electronic business adoption by European firms: A cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems*, *12*(4), 251-268.

APPENDICES

APPENDIX A

Survey Questionnaire

(Please check all that apply)

1. What is your age?
   - ☐ 18-24
   - ☐ 25-34
   - ☐ 35-49
   - ☐ 50-65
2. Gender
   - ☐ Male
   - ☐ Female
3. What is your title?
   - ☐ Owner
   - ☐ CEO
   - ☐ CTO
   - ☐ IT Management
   - ☐ IT Staff
   - ☐ Other_____
4. Number of employees
   - ☐ 1-99
   - ☐ 100-240
   - ☐ 250-499
   - ☐ 500+

5. Which of the followings best describe your firm current status?
   - ☐ Currently utilize one or more Cloud computing services
   - ☐ Evaluating the Cloud services for my firm's IT business operation.
   - ☐ Not considering the Cloud computing services

6. What Cloud Computing Services do you currently use/evaluate?
   - ☐ Infrastructure as a Service (IaaS)
   - ☐ Platform as a Service (PaaS)
   - ☐ Software as a Service (SaaS)

7. What type of laws and regulations pertain to your firm?
   - ☐ e-Discovery

- ☐ FINRA
- ☐ HIPAA
- ☐ PCI DSS
- ☐ SOX
- ☐ Other _____ _____ _____

8. Did your firm experience any type of security breach in the last 3 years?

- ☐ Yes
- ☐ No

9. Was your firm fined for non- compliance in the last 3 years?

- ☐ Yes
- ☐ No

10. What steps is your firm taking in improving its IT infrastructure?

11. What of the followings best describes your action in evaluating / adopting Cloud computing?

	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
Cost reduction					
Flexibility and business agility					
Data backup & disaster recovery					
Loss of Control over own data					
Integration with existing infrastructure					

Lack of industry standards					
Legality and Compliance					
Data Loss and privacy					
Contractual agreement					

12. Which industry does your organization represent?

- Manufacturing
- Financial services
- Professional services
- Computer-related business or service
- Retail
- Healthcare
- Construction
- Transportation & logistics
- Education
- Telecommunications
- Wholesale & distribution
- Utilities
- Government
- Media & entertainment
- Leisure services
- Agriculture, forestry, & fishing
- Hosting
- Nonprofit

13. Do you think adopting the Cloud does/will help you in?

	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
Reduced Operation Costs					
Flexibility and Scalability					

Business continuity					
Useful use of technology					
Ease use of technology					
Meet legality mandates					

14. Which Cloud Model does your firm utilizing or evaluating?

- ☐ Public Cloud
- ☐ Private Cloud
- ☐ Hybrid Cloud
- ☐ Community Cloud
- ☐ Other_____

15. How has been your experience migrating to the Cloud?

	Dissatisfied	Somewhat Satisfied	Neutral	Satisfied	Very Satisfied
Data Security and Availability					
Contractual Agreement					
Business Continuity and Service Availability					
Service Level Agreement (SLA)					
Legality and Compliance fulfillment					
Useful technology use					
Ease of technology use					

16. How do you rate your knowledge with Cloud computing?
    - ☐ Advanced
    - ☐ Intermediate
    - ☐ Beginner
    - ☐ Heard the term but not sure what it means
    - ☐ Other_____

17. ***Health Insurance Portability and Accountability Act (HIPAA***) requires a business associate to sign a Business Associate Agreement (BAA) when handling your data. Would it be an encouragement to adopt the Cloud if Cloud service provider offers such agreement?
    - ☐ Yes
    - ☐ No

18. ***Payment Card Industry Data Security Standard (PCI DSS):*** requires the Cloud service to the protect cardholder data against theft and misuse. If such solution is available in the Cloud, would it motivate you in adopting the Cloud?
    - ☐ Yes
    - ☐ No

19. ***Financial Industry Regulatory Authority (FINRA***) requires the Cloud service provider under rule 17a-4 to deliver SAS 70 audit letter annually to their broker-dealer. Would that motivate you in adopting the Cloud?
    - ☐ Yes
    - ☐ No

20. What are some other concerns of yours about Cloud computing that were not mentioned?