The Adoption of financial Information Cloud Backup methodology in Term of Income and Education in the United States

Malik R. Elhaj
Assistant Professor, Accounting & Finance Department,
Prince Mohammad Bin Fahd University (PMU),
Kingdom of Saudi Arabia

Shadi Z. Barakeh
Chief Operating Officer,
Barakeh Travel Inc., Chicago, USA

Abstract

Online financial and non-financial information backup service is beneficial for individuals and businesses because it enables them to gain access to their data without restrictions on time orlocation.The purpose of this quantitative study are to evaluate the factors that may have an influence on consumers' decision to adopt to cloud backup procedures. The dependent variable was whether or not the participant uses a cloud backup process and the independent variables were income and education. An online survey was used for data collection. The results indicate that age and gender were not related to cloud adoption rate. In addition, the adoption of cloud for backup will depend on consumers' perceptions of the innovation including the perceptions of the advantages of the new technology and the ease with which it can be adopted. Future researchers should include additional independent variables, perform qualitative or mixed-method studies, replicate the results from this study outside the United States, and examine the relationships between compute usage variables and cloud backup adoption rates.

Keywords: Delta blocking, Hybrid cloud, Intelligent file selection, Local backup, Private cloud, Public cloud, Cloud backup, Financial information.

1. Introduction

Consumers have a high demand for the use of data backup whether for work or personnel. Most people backup their data directly on the computer they are using. Other common backup practices are via external hard drive, flash drive (USB stick), CDs, DVDs, Blue Rays, MP3 Players, and cell phones. However, consumers have always complained about data loss, stolen, or corrupted due to hard drive failure, physical damage to the media device, or device has been stolen. Another issue is data availability; consumers can access their saved data only if they have the physical backup device carried along with them. Also, those backup devices are expensive and consumers pay for extra memory space that they do not occupy. As a result, many technological researches have addressed those issues and have developed a new technological backup concept, which can be referred to as *cloud backup*.

Cloud backup, also known as an online backup, is a service that provides users with a system for the backup and storage of computer files. It also refers to storing data on centralized computers that are located offsite. Cloud backup is a subset of cloud computing technology that falls under the *backup as a service* and *software as a service* category. Since cloud backup is part of cloud computing, it is necessary to understand and study cloud computing first. More details in regard to the cloud computing are provided in the literature review of this dissertation.

2. Research Questions

Based on the purpose of this study, four research questions were developed with one question for each of the four demographic variables to be examined.

RQ1. To what extent, if any, is income related to consumers' decision to adopt to cloud backup?

RQ2. To what extent, if any, do consumers with a college degree and consumers without a college degree differ with respect to the decision to adopt to cloud backup?

3. Literature Review

3.1Cloud Storage and Cloud Backup

Cloud storage is a computing service of storing data securely in a remote location which can then be accessed through the Internet (Robert, 2012). Cloud storage is a service where consumers can save their files to remote servers and access them whenever they want via a wide range of computing and mobile devices. Cloud storage service providers store consumers' files on their servers that are located in huge data centers. These are the same type of devices that enable you to access your emails; also those are the same devices that store your social networking information and your favorite websites. Cloud backup is a computing service that enables users to backup their computer to a remote location and to access or restore the data anytime they desire. Organizations that offer this type of service are called cloud backup service providers.

The cloud computing method of delivery for this type of service is software as a service as discussed earlier. Cloud backup sounds very close to cloud storage, however there is a quite differences between the two services. In cloud storage, the user must manually save the file to the cloud storage desire location. In cloud backup, the user will only configure the backup software once to specify the schedules backup task and which folders they would like to backup regularly. Cloud backup is done automatically versus cloud storage which is done manually (Rouse, 2010).

Consumers will have control only to configure the backup settings only on the user level. Consumers do not have control over the cloud IT infrastructure nor the developing of the backup software (Rouse, 2010). The cloud backup software normally runs on a scheduled basis that is set by the user. For instance, if the user set the backup to be done on his or her computer on a weekly basis, then the backup will start automatically every week as requested by the user. Generally, cloud backup providers will set the backup to be incremental, which means that the initial computer backup will take a longer time because every single file is being backed up, and then afterwards the software will only backup any modified and new files or folders. With that being said, the process of backup time will decrease the second time around using cloud backup (Rouse, 2010). There are many companies are entering the cloud backup sector. The major players such as Google, Amazon, Microsoft, and Apple are dominating the cloud backup sector. However, there are many startups companies that became large in the cloud backup sector such as Barracuda, Dropbox, Mozilla, and Carbonite.

3.2Advantages of Cloud Backup

Cloud backup technology has many advantages that scholars and researchers have identified. From the business prospective, cloud backup is cost effective because it will save on physical space formerly needed to house the backup servers (Armbrust et al., 2009). Also, cloud backup technology will reduce the utility costs because to house backup servers requires certain power source characteristics, temperatures, and so forth. Cloud backup will reduce the cost of IT staff to maintain and operate backup servers. From the individual consumer's prospective, the cost benefits are substantial. Consumers may only pay for the amount of storage they use. As a result, they save money on storage costs. Consumers may also save money by not having to purchase external hard drives or other expensive storage media to run at home (Armbrust et al., 2009).

Another advantage to cloud backup is data availability. With the cloud backup method data are available anytime the consumer requires them. The technological secrete behind this attractive data availability benefit is that the data is being backed up in multiple locations and cloned on multiple hard drives by the service provider. Even if one server or an entire datacenter is destroyed the consumers' data is still available due to the multiple clones (Sedayao, 2008).Consumers do not have to carry flash memory stick or their laptop to school or work to access their files since they are available everywhere.

Accessibility and mobility are benefits that come along with the cloud backup package. Consumers are able to access their data from anywhere they desire on any type of display media they use (Smith, 2009).Currently, computers are not the only instrument that people utilize to access the Internet. There are many different devices that enable consumer to access the Internet such as mobile phones, tablet PCs, iPads, iPods, televisions, and so forth. As a result, consumers' data are accessible via any device possible that have an Internet capability.

With this type of benefit, consumers may enjoy the freedom of not to worry about forgetting their important files at home when they go to work or a term paper for school, because they will be able to access it anytime they desire from any location (Smith, 2009).

Cloud backup is highly automated. With cloud backup the time spent in backing up files is reduced and the entire backup process will happen seamlessly so the consumer may enjoy working on his or her computer while the backup is taking place (Smith, 2009). With the old backup technology, the consumer was required to have some type of knowledge with computers and software in order to get the backup completed. In some cases, consumers were required to read the external hard drive manual before utilizing the backup technology. With cloud backup consumers do not need to read or be knowledgeable about computers or backup technology. The use of Internet is enough to perform the registration with the backup providers, where the providers will take care of the rest (Smith, 2009).

Cloud backup is dynamically scalable and allows users to pay only for the storage they use. When consumers use more storage capacity, the system will automatically scale more to serve more storage for the consumers' data. On the other hand, when consumers use less storage capacity, the system will scale back (Sedayao, 2008). With this benefit comes the economy of scale to allow users to reduce the costs associated with backup. With the old backup method consumers had only a few choices regarding the required initial investment such as external hard drive capacities (Sedayao, 2008).

In summary, cloud backup has many advantages. It is inexpensive and does not require any hardware installation. It does not require any hardware. Cloud backup system does not require physical space or environmental constraints in the home or office. No IT staff is required. However, cloud computing, as any other technology, has disadvantages as well. Major disadvantages are also barriers of adoption to such new technology are performance, availability, incompatible interface, lack of standards, and questions about data security (Miller, 2009).

3.3 Cloud Backup Disadvantages and Barriers to Adoption

As a new technological concept, some concerns are expected with cloud backup and disadvantages need to be considered. Cloud backup has some disadvantages that could be barriers to adoption for consumers. One of the cloud's disadvantages is system performance. Cloud backup performance depends on the bandwidth speed. Accessing a file on a local area network within the home or at work is faster than accessing the file over the wide area network (the Internet). As a result, it may take a long time to download or upload files to the cloud backup. Consumers may not have the patience to wait for so long to store or backup their files. However, researchers claim that the bandwidth speed is advancing today, which might reach a great level of compatibility with cloud backup that may solve such performance issues(Miller, 2009).

Data availability might be one disadvantage in case of network failure by the cloud backup providers. Network failure can be caused by several factors such as global network disruptions, solar flares, severed underground cables, or satellite damage. Cloud backup depends heavily on the network connectivity between the user's network and the cloud backup provider's network located on the Internet (Miller, 2009). Network connectivity failure means that the cloud backup's network is completely unavailable which also means that the data will not be available to the user. On the other hand, many cloud backup providers promises that the data will be cloned on different servers located at different sites. Even though the data is still available on the provider's hard drive, but if there is a network outage, then the user won't be able to view their data or download it until the network outage is fixed (Miller, 2009).

Another disadvantage is the lack of protocol standardization. Each backup provider has a different software protocol which makes it difficult for consumers to swap between different providers. In some cases, the user must download all of his files to his computer or a local backup device from previous backup provider prior to switching to a different provider because of protocols compatibilities. This issue is not noticeable among consumers because there are not many customers who switch providers, but when the switch happens, then they will face this type of issue (Sedayao, 2008).

Security is the biggest concern of all. Many individuals are hesitant to have their data saved and operated from an external location. Users may fear that a company's server that might be co-hosted with a third company's application or data which might be accessed by someone else by mistake.

Having data stored by cloud backup provider might have a high risk of data vulnerability because any staff employed by the cloud backup provider might have access to personal and confidential information (Binning, 2009).

Any small mistake from the IT staff might open cyber doors to thieves to sneak in. According to Harvard law professor, Jonathan Zittrain, "Before, the bad guys usually needed to get their hands on people's computer to see their secrets; in today's cloud all you need is password." However this is true for every computer network, including any personal networks. As long as people have their computer connected to the Internet their data are automatically vulnerable even if they have the best data protection software that it is available. Cloud service providers do not typically provide data location details to subscribers. As aresult, individuals and companies are uncertain as to whether their data are being safeguarded in the cloud and whether laws and regulations compliance is being met. There are external audits and security certification can to some extent alleviate this issue, but nothing is fully guaranteed.

Another barrier to the clouds is laws and regulations. Many people are concerned about the laws in different countries that might give the government the right to access data. There are many different laws and regulation that might be a barrier to the use of cloud backup systems. One important law is the U.S. Health Insurance Portability and Accountability Act which requires organization that handles personal health data to have strict access. Cloud backup provider might need to follow this law if they store any health data or ask the user to identify the type of file being saved. Laws and regulation is a very important aspect of cloud backup that consumers should be aware of to understand their rights before they consider adopting cloud systems. The laws and regulation will be covered in the next section with more details with the purpose of understanding the law within the clouds.

3.4 Cloud Backup vs. Local Backup

Many people are wondering why they should leave the traditional way to backup their data locally and switching to cloud backup. Despite the advantages and disadvantages of cloud backup, we may conclude that there are major differences between cloud backup and local backup. The first major differences between local backup and cloud backup services that the cloud backup allows for delta blocking to ensure only modifications are recorded (Clapperton, 2000). Delta blocking is a method used to divide and save files into blocks.

Each block will be assigned with a digital signature that is compared against the last known digital signature of the same blocks in the same files that has been modified (Zhang, 2006). When modified blocks in a file are being detected it will be transmitted and stored along with the original files that are already stored on the backup system. The technique of delta blocking in a backup system reduces the backup time because the data that is being backed up each time are small which reduces the demands on storage and bandwidth (Zhang, 2006).

Intelligent file selection is another feature for cloud backup that doesn't exist with local backups. Intelligent file selection does not backup nonessential files such as clipart and cookies that are stored on the computer to increase network efficiency (Kane &Hopkins, 1993). Also, intelligent file selection enable to servers to save more space. Cloud backup allows minimal user intervention and it gives the user the ability to continue work while the backup is done in the background without any interruption. On the other hand, local backup requires the user to interact on every step of the backup process.

File restoration is easier and more efficient with the cloud backup than local backup. Cloud backup allow users to restore all files with a click of a button. On the other hand, restoring from a local backup requires extra work and user intervention which might be vulnerable to data loss if the user was under pressure. It is virtually impossible to damage your backed up data with the cloud backup method because the data is stored and encrypted in multiple locations. Using the local backup method the files are located only at one device and may not be encrypted due to the user lack of knowledge.

3.5 The Evolving of Laws and Regulation on the Clouds

Cloud backup is famous for storing files at multiple locations to ensure data recovery efficiently in case of a disaster. Many cloud backup providers are renting data centers that are located in different countries to reduce cost and save money. However, many users concern whether the files are being backup in locations outside of their countries which will give such country jurisdiction to practice their laws on data that is being saved there.

When information travels offshore, the governing legal, privacy, and regulatory regimes can be vague and raise a selection of concerns (Canadian Broadcasting Corporation News, 2004).

Therefore, the homeland security and the U.S cyber defense has put together serious laws and regulation to protect national cyberspace from any malicious attacks that might be delivered through data stored on any cloud backup servers. The Canadian government has also implemented laws that prevent government IT workers to utilize IT services that are operated within U.S. borders because the Canadian are concerned that their data will be subject to being accessed through the U.S. Patriot Act.

Another important concern to be considered is whether the laws in a foreign country permit the flow of data to be inspected by high end security system that might interrupt the data after the inspection. Those laws give the foreign country the right to act upon the files after the transfer is completed and whether those laws present any serious harm to the files that are being stored (Eisenhauer, 2005). In other words, who should have the authority to govern the data transferred from one country to another? For example, you want to send a confidential file over the Internet to a cloud backup provider that has servers in India. The Indian government found a threat in the file you've sent, and then they have restricted your access to their system. Now, who shall have the jurisdiction over your case? Can the government of India press charges on you and put you in their local jail? Would the United States have the authority to transfer the case from India and place charges on you through the U.S courts? Technical, physical and administrative safeguards such as access controls, often apply. For example, European data protection laws may impose additional obligations on the handling and processing of data transferred to the United States.

For U.S. federal agencies, the major security and privacy compliance concerns include the Clinger-Cohen Act of 1996, the Office of Management and Budget (OMB) Circular A-130, particularly Appendix III, the Privacy Act of 1974, and the Federal Information Security Management Act (FISMA) of 2002. Also of importance are National Archives and Records Administration (NARA) statues, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (Title 36 of the Code of Federal Regulations, Chapter XII, Subchapter B).

The Clinger-Cohen Act assigns responsibilities for the efficiency, security, and privacy of computer systems within the federal government and establishes a comprehensive approach for executive agencies to improve the acquisition and management of their information resources (U.S. Department of Defense, 2006). Circular A-130 under the Clinger-Cohen Act was issued to create policy to manage federal information. Circular A-130 provides analytic guidelines for creating certain aspects for these policies. The Circular A-130 consist of the Privacy Act of 1974 as Appendix III which requires strict and efficient security measures that is provided for all agency information to be collected, stored, transmitted, or distributed in main application and systems. The Privacy Act also controls and manages the data collection process as well as maintaining the data of personally identifiable information of individuals by federal agencies.

The NARA regulations and the Records Act give direct responsibility for agencies holding federal records to manage these records effectively and securely throughout the lifecycle. Administering the federal records includes storing data securely and retrieving it with care to insure data integrity still the same. Also, agencies must transfer federal records to NARA in an acceptable format that is standardized by the federal records (Ferreiro, 2010).

Certain organizations are protected by laws and regulation that was made specifically for them such as the Veterans Health Administration falls under the Health Insurance Portability and Accountability Act standards to protect data for private and public health care facilities (Department of Veterans, 2002). This Act requires high standards of security measures in both software and hardware which may develop issues for some cloud backup providers.

Finally, laws and regulation all over the world have tightened the freedom of technical practices in the clouds. Cloud backup providers must be careful in terms of the storage locations and they must review the law and regulations of the country hosting their backup servers. Cloud backup providers must comply with the U.S. laws and regulation for data security and privacy protection before offering their service to the public (Ferreiro, 2010). Consumers must read the service level agreement, a digital subscription contract between the cloud backup provider and the consumers that is provided by the cloud backup provider prior to signing up with their backup service to ensure that they comply with all laws and regulation of the country they operate from (Truitt, 2009)

Consumers must understand the risk factors that might result from subscribing to a provider that does not follow all laws and regulations that they might lose their data at any given time due to the federal shutting down the servers they operate from. Cloud backup providers are liable for data protection and data exposures under the laws and regulation (Mather et al., 2009).

Consumers are also liable for the type of data sensitivity they store on the clouds which they will be held accountable of there is any threat to the country it is hosted by. Consumers must be continuously educated about the cloud backup method to further promote and advance the technology. This can ease the way of cloud computing adoption into their life. There are different laws and regulations that reside in different countries in regard to the data flow in and out of the country. It seems like not only people need passport to travel from one country to another, as data will eventually need some type of identification in order for it to be traveling across borders. Many online companies are struggling when doing business outside the United States because they need to follow the laws of the hosted company.

3.6Adoption Theories

Between any new technological innovation and an individual comes a gap of adoption to such new technology. It is important for companies that provide a new technology to understand the adoption gap between the consumer and the new technology such as cloud backup. Commonly people backup their data on small media devices so they can access their data on the go simply by plugging the small memory media directly to the computer. The downfall that the memory device is small that people intend to forget it attached to the computer they are using at school or library. Also, some people intend to need more memory space, which is more expensive to buy. It is very important for people to be educated about new technological advancement that might be very beneficial to them and to be more open minded to try new technology by taking caution and extra safety measures.

The ground fundamental of the innovation theories that is developed mostly today is derived from the diffusion of innovation theory that was developed by Rogers in 1962 (Lundblad, 2003). According to Rogers (1962), there are three major factors for technological innovation adoption by an individual: the actor's identity and perception of the innovation, the process, and the result (either adoption or rejection). There are three primary elements were considered by Rogers for technology adoption (lundblad, 2003). These elements include an innovation, a time frame for adoption, and a social structure that fosters technology innovation adoption.

In order for cloud backup to be adopted by people, it must offer great benefits to the users and be compatible with the users' current technology (Lundblad, 2003). When new technology enters the market, people are looking for its advantages and the value that it can bring to their daily tasks. Also, before consumers purchase the new technology, they would like to make sure that the new technology is compatible with the technology they currently use. For instance, cloud backup must work on Applea nd PC machines and under a variety of operating systems. Education and communication is vital to promote a new technology amongst consumers. Adoption of new technology occurs in stages and there is different time frame for cloud backup adoption occurred. Early adopters of cloud backup have embraced the technology as a beta version before the mainstream users begin using it.In 1986, The Technology Acceptance Model (TAM) was developed by Davis to model patterns of user adoption of information systems (Davis, Bagozzie & Warshaw, 1989). The TAM is used to evaluate the usefulness, ease of use, and the attitude toward using a technology. These results are used to determine the intention for a user to adopt the technology, and are compared to the actual technology usage (Davis, 1989). Technology's friendliness and usefulness to the user are often results to be the major factors in technology adoption when using TAM by the researchers (Straub & Burton-Jones, 2007).

Normally, when a person or organization sees an advantage to accepting a new form of technology, there is an incentive to accept it. An example is a study by Lease (2005) that covered reasons why computer security managers adopt biometric security technologies. Rogers (2002) stated that prior experience with a technology could influence technology adoption decisions, both positively and negatively.

3.7 Major Players: Cloud Backup Providers

As the new cloud computing technology is dominating the IT world today, cloud backup is increasingly spreading out in today's market. The first company to offer cloud computing services is DriveHQ.com starting its outsourcing services in 2003 (Delahunty, 2009). DriveHQ.com offers several cloud services including cloud storage and backup. Today there are hundreds and of cloud backup providers and the number is still increasing. The top cloud backup providers for consumers are Carbonite, Barracuda, and Mozywhich offer different affordable packages for consumers to backup their data seamlessly and securely (Delahunty, 2009).

Many giant companies are taking their places in the cloud backup and storage market today. For instance, Microsoft is offering the Skydrive service as a storage service allowing its consumers to use the first 25 GB of storage for free.

Apple is not only dominating the mobile market with its innovative iPhone technology, but it is also offering its users iCloud storage free for the first 5 GB of storage. iCloud offers great benefits such as simple configuration and registration where consumers can simply register for the service on their mobile device just by providing and email address and a password (Poindexter, 2012).

iCloud is user friendly which simplified the cloud backup and synchronization for consumers to adopt so quickly. All the files, photos, videos, music, and contacts are saved and restored anytime the consumers will desire on iCloud by Apple Corp servers. The benefits of offering such great service for free for the first 5 GB of storage will eventually push the mobile user to purchase more storage when their important data increase (Poindexter, 2012). Google also has a market share in the cloud storage business by offering the Google Drive. Google Drive offers its users 5GB free storage that is highly secured and trusted by consumers.

The entrance of large knowing corporation into a new technological advancement such as Google, Microsoft, and Apple will help more people to adapt to cloud storage and backup technology quickly. Such companies have great reputation and creditability among consumers. Consumers are less hesitant to use iCloud than to use a private new startup company that offers the same storage benefits and in some cases better offers. However, researchers believe that after the entrance of the giants company into the cloud world, the consumers' technology acceptance will increase, and then more consumers will start to look for alternative companies that offer more competitive prices.

4. Research Design

A quantitative research design was used in this study. According to Creswell (2009), quantitative research designs are most appropriate when (a) the constructs of interested are readily quantifiable and (b) specific hypotheses are tested. Both of these characteristics applied to this study because the variables of interest, use of cloud backup, income and education, were readily measurable, and there were specific hypotheses related to the effects of any, income, and education on the use of cloud backup.

The dependent variable in this study was whether or not the participant uses a cloud backup process. Whether or not the participant uses a cloud backup process was a dichotomous variable. The independent variables were the demographic characteristics of income (annual household income), and education (whether or not the participant has a bachelor's degree). The two research questions (and corresponding hypotheses) of this study each related to one of the two independent variables. The independent variable (education) was categorical while the (income) was continuous. Chi-square tests were used to determine if the categorical independent variables are related to whether or not the participant uses a cloud backup process (for the second research question). Independent samples *t* tests were performed for the two continuous variables to determine if participants who use a cloud backup process differed from those who do not in terms of income (for the first research questions).

4. Instrumentation

A survey was designed for use in this study which consisted of measures of the independent and dependent variables as well as additional items related to the use of cloud backup processes. The first null hypothesis was:

H_{1o}: Income is not related to consumers' decision to adopt cloud backup.

An independent samples *t* test was performed to compare those who have adopted cloud backup and those who have not in terms of annual household income. The second and final null hypothesis was:

H_{2o}: Consumers with a bachelor's degree and consumers without a bachelor's degree do not differ with respect to the decision to adopt to cloud backup.

A chi-square test was performed to compare participants with a bachelor's degree and those without in terms of whether or not they have adopted cloud backup from this study to computer users in other countries.

Most of the participants had obtained a college education (83.1%). The average age of the participants was 35.43 years old (*SD* = 10.39 years) and the average income was $76,401.48 (*SD* = $102,925.75).

5. Results

The first research question was: To what extent, if any, is income related to cloud adoption rate? The null hypothesis for this research question was:

H_{1o}: Income is not related to cloud adoption rate.

Table 7 shows the mean incomes for the participants had and had not adopted cloud backup. Participants who had adopted the cloud earned less income (M = \$66,861.90, SD = \$75,519.48) than those who had not adopted the cloud (M = \$91,811.56, SD = \$135,530.42), but this difference was not statistically significant, $t(134) = 1.38$, $p = .170$. The null hypothesis was not rejected and it was concluded that income was not related to cloud adoption rate.

Table 1Descriptive Statistics for Income as a Function of Adoption of Cloud Backup (N = 136)

Group	*M*	*SD*
Have not adopted cloud	\$91,811.56	\$135,530.42
Have adopted cloud	\$66,861.90	\$75,519.48

The second research question of this study was: To what extent, if any, do consumers with a college education and consumers without a college education differ with respect to cloud adoption rate? The corresponding null hypothesis was:

H_{2o}: Consumers with a college education and consumers without a college education do not differ with respect to cloud adoption rate.

Table 2 shows the crosstabulation of education and adoption of cloud backup. Among those with no college education, 65.2% had adopted the cloud while among those with a college education 61.1% had adopted the cloud. This difference was not statistically significant, $\chi^2(1) = .14$, $p = .709$, and the null hypothesis was not rejected. Therefore, it was concluded that consumers with a college education and consumers without a college education did not differ with respect to cloud adoption rate.

Table 2Crosstabuation of Education and Adoption of Cloud Backup (N = 136)

	Had not adopted cloud		Had adopted cloud	
Group	Frequency	Percentage	Frequency	Percentage
No college education	8	34.8	15	65.2
College education	52	38.9	69	61.1

6. Findings

The second research question was: To what extent, if any, is income related to cloud adoption rate? The null hypothesis was not rejected and it was concluded that income was not related to cloud adoption rate. The fourth and final research question of this study was: To what extent, if any, do consumers with a college education and consumers without a college education differ with respect to cloud adoption rate? The null hypothesis was not rejected indicating that consumers with a college education and consumers without a college education did not differ with respect to cloud adoption rate.

7. Conclusions and Recommendations

None of the two demographic variables (income and education) were related to the adoption of cloud backup procedures. Past researchers had not specifically examined these four independent variables and so no direct comparisons are possible. In the context of the theoretical frameworks for this study (i.e., innovation theory from Rogers [1962] and Lundblad [2013] and the technology acceptance model of Davis [1986]), the adoption of cloud for backup will depend on consumers perceptions of the innovation including the perceptions of the advantages of the new technology and the ease with which it can be adopted.

These factors may depend on the demographic and background characteristics of the users but no evidence supporting these potential differences were found in the current study. Another key finding from the currents study was that most of the participants used cloud backup at least to some extent (62%). Given that cloud computing and backup has only been available since 1999 to consumers (Chang et al., 2010), the 62% figure represents substantial market penetration in just over a decade.

8. Implications for Research

Based on the methodology and research design used in this study and the results, there are several implications for future research. The first implication is that future researchers should expand the list of potential independent variables to be included. In the current study, four independent variables were included: age, gender, income, and education. None of these variables were found to be related to whether or not an individual had adopted cloud backup. However, it may be the case that there are other independent variables that would be related to cloud backup adoption, and therefore further research is required before final conclusions regarding individual characteristics and cloud backup adoption are drawn. It may be the case that one's familiarity with computers, choice of a college major (e.g., in a technology-related field or not), computer platform (PC versus Mac), or other similar variables would be related to cloud backup adoption.

A second implication for future research based on the results from this study would be to perform qualitative or mixed-method studies. Given that none of the independent variables in this study were related to the adoption of cloud backup, the question of what kinds of variables would be predictive of the adoption of cloud backup remains unanswered. Directly asking participants in an interview-type study (either in a purely qualitative study or as part of a mixed-method study) could provide answers to these questions. Understanding participants adoption (or lack of adoption) of cloud backup at a deeper level than can be assessed using a survey (e.g., through the use of in-depth interviews or focus groups) could provide cloud backup service providers with additional information that they can use to facilitate the adoption of cloud backup among consumers.

Third, the generalizability of the results from this study should be tested in additional samples. For example, all participants in this study were currently residing in the United States. Given the global nature of the Internet, it is important to determine if computer users in different countries have different levels of cloud backup adoption or if some of the demographic independent variables examined in this study are predictive of cloud backup adoption in other countries. Differences in access to cloud backup systems between the United States and other countries, for example, indicate that the use of cloud backup may also differ from country to country.

The fourth implication for future researchers is that the relationships between other compute usage variables and the adoption of cloud backup should be examined. It may be the case that individuals who use cloud for other purposes are more likely to adopt cloud systems for backing up files. For example, individuals who store music files in the cloud rather than on a local computer may be more likely to adopt cloud backup systems for general file backup purposes. Understanding how individuals use computer and various components of the Internet is a complex topic and assessing the interrelationships among these uses is important to developing a comprehensive picture of cloud backup adoption.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G.,…Zaharia, M. (2009). *Above the clouds: A Berkeley view of cloud computing. University ofCalifornia at Berkeley Technical Report No. UCB/EECS-2009-28.*Retrievedfrom http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.htm

Binning, D. (2009). *Top five cloud computing security issues.* Retrieved from http://www.computerweekly.com/Articles/2010/01/12/235782/Topfive-cloud-computing security-issues.htm

Canadian Broadcasting Corporation. (2004). *USA Patriot Act comes under fire in B.C.* Retrieved from http://www.cbc.ca/canada/story/2004/10/29/patriotact_bc041029.html

Cearley, D. (2010). *Cloud computing key initiative overview.* Retrieved from http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_CloudComputing.pdf

Chang, W., Abu-Amara, H.,&Sanford J. (2010). *Transforming enterprise cloud services.*New York, NY: Springer Science.

Clapperton, G. (2000). Understanding online backup.*PC Network Advisor, 121*, 15-18. Retrieved from http://www.pcadvisor.co.uk/

Creswell, J. (2009). *Research design.*Thousand Oaks, CA: Sage.

Delahunty, S. (2009). *State of enterprise storage.*Manhassett, NY: UnitedBusiness Media Limited.

Denning, P., & Metcalfe, R. (1997). *Beyond calculation: The next fifty years of computing.*New York, NY: Springer.

Eisenhauer, M. (2005). *Privacy and security law issues in off-shore outsourcingtransactions.*Retrieved from http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

Federal Information Security Management Act of 2002. H.R. 2458, 44 U.S.C.§3541 (2002).

Ferreiro, D. (2010). *Guidance on managing records in cloud computing environments*. Retrieved from http://www.archives.gov:80/records-mgmt/bulletins/2010/2010-05.html

Kane, P., & Hopkins, A. (1993). *The data recovery bible: preventing and surviving computer crashes*. New York, NY: Brady.

Lundblad, J. (2003). A review and critique of Rogers' diffusion of innovation theory as itapplies to organizations. *Organization Development Journal*,*21*(4), 50-64.Retrieved from http://www.highbeam.com/publications/organization-development-journal-p61828/april-2011

Mather, T., Kumaraswamy, S., &Latif, S. (2009). *Cloud security and privacy.* New York, NY: O'Reilly Media.

Miller, M. (2009). *Cloud computing: Web-based applications that change the way you work and collaborate*. New York, NY: Que.

Poindexter, A. (2012).*iCloud: Apple Corp articles.* Retrieved from http://coe.uncc.edu/pcs/images/stories/docs/The_Cloud/iCloud_Review.pdf

Robert, A. (2012). *The history of the cloud*. Retrieved from http://blog.livedrive.com/2012/08/the-history-of-the-cloud/

Rogers, M. (1962). *Diffusion of innovations.* New York, NY: The Free Press of Glencoe.

Rouse, M. (2010). *Definition of cloud backup (online backup).* Retrieved from http://searchdatabackup.techtarget.com/definition/cloud-backup

Sedayao, J. (2008). *Implementing and operating an internet scale distributed application using service oriented architecture principles and cloud computing infrastructure* [Electronic version]. Proceedings of the 10th International Conference on Information Integration and Web-based applications & Services, 417-421.

Smith, R. (2009). Computing in the cloud. *Research Technology Management*, *52*(5), 65-68. doi:10.1142/9789812839527_0042

Straub, D. W., & Burton-Jones, A. (2007). Veni, vidi, vici: Breaking the TAM logjam. *Journal of the Association for Information Systems*, *8*(4), 223-229.Retrieved from http://aisel.aisnet.org/jais/

Truitt, M. (2009). Editorial: Computing in the "cloud". *Information Technology & Libraries, 28*(3),107-108. Retrieved from http://www.ala.org/lita/ital/front

U.S. Department of Defense. (2006). *Department of Defense CIO desk reference (Volume I): Foundation documents.*Retrieved from http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

Zhang, X. (2006). *Tape storage solutions: Meeting growing data demand.* Minneapolis, MN: University of Minnesota.