

Adopting cloud computing within the healthcare industry: opportunity or risk?

Linda Barthelus, Northern Virginia Community College, lbarthelus@nvcc.edu

Abstract

Innovative technologies enable firms to strengthen their market position in today's increasingly turbulent and competitive business environment. Cloud computing, an innovative technology, allows users to process and store data virtually via the internet and central remote servers. The purpose of this paper is to examine the forces that influence the adoption of cloud computing within the healthcare industry, through the theoretical lens of innovation resistance and the innovation decision process. This paper applied an evidence-based research methodology that consists of a systematic review of primary literature and a thematic synthesis of findings. The findings indicate that the primary reasons for resistance to cloud adoption within the healthcare industry are security and privacy risks to sensitive patient data, integration challenges, and a firms' potential to lose control of data to cloud providers. However, incorporating analytical tools and safeguards into the decision process can mitigate these challenges. This study deepens knowledge of innovation resistance, which has been limited to innovation research thus far, and presents a conceptual model of how resistance affects each stage of the innovation decision process. This study proposes the cloud adoption toolkit to healthcare decision makers as a practical solution to address the challenges of cloud adoption.

Keywords: Cloud computing, innovation diffusion theory, innovation decision process, innovation resistance and healthcare/medical industry

Introduction

The rapid growth of innovative information and communication technologies (ICTs) has created opportunities for firms to improve their responsiveness, flexibility, and adaptability to changes within their internal and external environments. Cloud computing is an innovative service that utilizes the Internet capabilities (Khajeh-Hosseini, Greenwood, Smith, & Sommerville, 2010) to increase the agility of firms in their communication and data storage activities. For example, ability to minimize the cost of managing physical servers, which typically house vast quantities of patient files and other medical records, is a significant advantage for healthcare entities. Certain demographic trends, such as rapidly ageing population (Laukkanen, Sinkkonen, Kivijarvi, & Laukkanen, 2007) and higher overall life expectancy (Sultan, 2014), have amplified the burden on the healthcare industry and have increased the need for scalable data storage. For this reason, healthcare decision makers are increasingly considering alternate measures to decrease costs and implement innovative solutions (Sultan, 2014).

On the other hand, the stringent regulation of the protection of patients' privacy and integrity makes the adoption of cloud computing challenging for the healthcare decision makers. Laws, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, were established primarily to protect the confidentiality of patient information (Witt, 2011). Additionally, the HIPPA Omnibus and the American Recovery and Reinvestment Act (ARRA) require all healthcare entities to migrate patients' personal and medical data to an electronic system by 2015 (Hon, Millard, & Walden, 2012). Failure to comply with this federal law can result in heavy penalties (Hon et al., 2012). A cloud-based system is a viable solution for fulfilling this mandate. The attributes of cloud computing and the virtual environment it operates in introduce issues of patient data safety and security. Therefore, it is imperative that the concerns associated with adopting cloud computing within the healthcare environment be identified and carefully examined, in order to identify potential solutions.

Given the above, this study aimed to achieve three goals: (1) to examine the general advantages and challenges of cloud computing, (2) to understand the impact cloud computing has on healthcare entities, and (3) to provide practical strategies for mitigating the identified challenges, allowing healthcare decision makers to adopt cloud computing effectively. Hence, the research question driving this study is, *what are the forces influencing the adoption of cloud computing within the healthcare industry?* It was addressed via a comprehensive literature review, aiming to elucidate the issues currently hindering cloud-computing adoption within the healthcare context.

This study is targeted primarily at healthcare providers, administrators, and IT professionals, including CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers), hereafter identified as *healthcare decision makers*, within healthcare institutions, such as hospitals, medical clinics, family practice firms, and pharmaceutical companies. Additionally, this research may also be relevant to business entities in other fields that are considering capitalizing on the opportunities afforded by cloud computing.

Literature Review

What is Cloud Computing?

Cloud computing is a technology that uses the Internet and remote servers to process and store data and applications (Shi, 2012; Tripathi & Jigeesh, 2013). The National Institute of Standards and Technology (NIST)—an agency established by Congress to eliminate impediments to the United States' industrial competitiveness and to focus on the measurement of infrastructure, from tiny nano scale devices to global communication networks—defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011, p. 2). Cloud computing is supported by two basic technologies, virtualization and grid computing (Sultan, 2014). Virtualization is a method or act of creating something virtually rather than in its actual or physical form, which simplifies interaction among different systems (Sultan, 2014). Grid computing, a network or collection of multiple computers dispersed geographically with significant computational power, facilitates virtualization.

Types of cloud deployment models

Cloud computing can be deployed as private, community, public, or hybrid service (Tripathi & Jigeesh, 2013; Zissis & Lekkas, 2012). Private cloud is the most secure way to utilize cloud computing. The infrastructure can be operated and managed within the confines of the organization or by third party vendors known as cloud providers and can be housed onsite or off premises (Zissis & Lekkas, 2012). Community cloud is a cloud infrastructure with a network of several organizations. The purpose of this cloud is to support the communal objectives and missions of a particular community (Zissis & Lekkas, 2012). Similar to private cloud, a community cloud can be managed by one or more organizations or a cloud provider and may be housed onsite or offsite. Public cloud, which is the most open type of cloud computing, consists of a cloud infrastructure that is accessible by the general public and/or industry group (Zissis & Lekkas, 2012). Public cloud is commonly operated and managed by cloud providers. Lastly, hybrid cloud is an infrastructure that consists of a combination of two or more private, public, or community clouds (Zissis & Lekkas, 2012). Within a hybrid cloud, each cloud remains distinct but may share “standardized or proprietary technology which enables data and application portability” (p. 584). Yet, little is known about the way services are delivered via the cloud to end users.

Cloud service delivery models

Cloud service delivery models can take form of software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) (Hossain & Luby, 2010; Park & Ryoo, 2012; Tripathi & Jigeesh, 2013). IaaS is defined as a service that provides users “processing power, storage, networks and other fundamental computing resources” (Hossain & Luby, 2010, p. 43). PaaS, a layer above IaaS, is “a service that includes middle wares, programming tools, application runtimes, operating systems and other tools” (p. 43). According to Park and Ryoo (2012), SaaS typically includes flexible and scalable IT applications that can be provided as a service via the Internet. When using all three-cloud service levels, organizations are able to provide users with uninterrupted service, allowing them to access, share, and store company information via the Internet (Park & Ryoo, 2012). Examples of cloud services include the use of email services provided by technology organizations such as Yahoo and Microsoft, and the capability to host websites via the cloud by open cloud company, Rackspace (Tripathi & Jigeesh, 2013). A basic cloud-computing model is depicted in Figure 1.

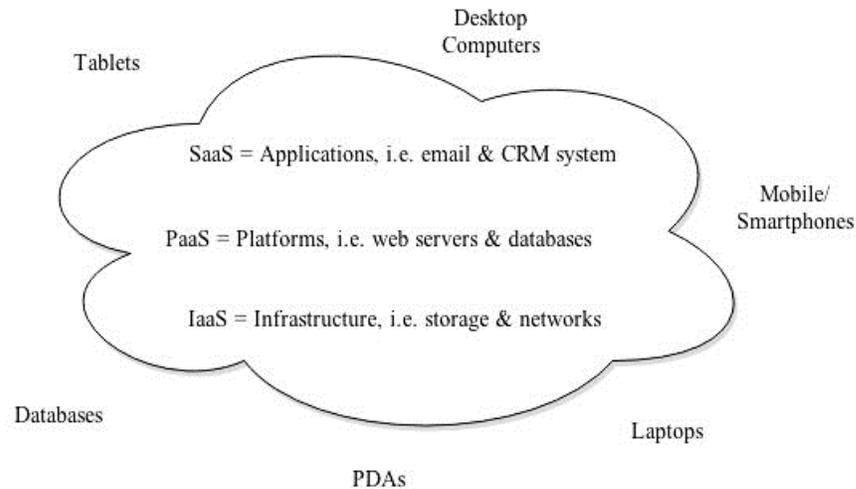


Figure 1. Cloud Computing with the Three Service Levels (IaaS, PaaS, and SaaS) Whereby the Technologies Listed Around the Perimeter of the Cloud All Connected Remotely to the cloud.

Benefits of cloud adoption

Available evidence suggests that business agility and resiliency, low-cost disaster recovery, rapid elasticity, and fast deployment are the main benefits of cloud adoption (Subashini & Kavitha, 2011; Tripathi & Jigeesh, 2013). The technical benefits enable substantial reduction in the total cost of ownership and maintenance of software and hardware infrastructures (Tripathi & Jigeesh, 2013), while enhancing portability and capacity to access and store information virtually (Sommer, 2013). Overall, cloud adoption allows firms to attain a greater focus on core activities and increased advantage over the competition.

Iyer and Henderson (2012) conducted a study aiming to elucidate the benefits realized by organizations when they leverage the capabilities of cloud computing. The authors interviewed IT executives from seven prominent service companies that had adopted cloud computing, who cited the ability to reuse IT infrastructure as the key advantage of cloud computing. For example, when Google, whose entire organization is built on a cloud, sought to expand its business in Bangalore, the ability to utilize existing tools and applications on the cloud significantly expedited the expansion (Iyer & Henderson, 2012). The authors thus concluded that the cost efficiencies and competitive advantages of cloud computing realized by organizations increase the likelihood of continued exploitation of this emerging technology.

Challenges of cloud adoption

In a study conducted by International Data Corp in 2009, “75% of the 244 CIO and IT executives surveyed rated security as their main cloud computing concern, and 63% rated performance and availability as the next two concerns” (Sultan, 2014, p. 182). As information processing becomes increasingly digitalized, the hardware and software applications that deliver the information must be changed as well (Shi, 2012). The primary IT security issue posed by

increased reliance on cyberspace is the vulnerability to nefarious activity from a high number of uncontrolled and often unknown entities within the cloud.

Subashini and Kavitha (2011) identified certain types of security risks at each level of the cloud computing service delivery models (i.e., SaaS, PaaS, and IaaS). Concerns regarding “data privacy and data protection” (King & Raja, 2012, p. 1), and the lack of visibility of data stored virtually are the fundamental challenges of cloud computing. Firms’ reluctance to adopt cloud computing due to security concerns despite its many advantages is justified by ample studies in this field (Subashini & Kavitha, 2011; King & Raja, 2012). There is a clear need for cloud users to be knowledgeable of the risks involved in cloud computing and to be vigilant against its vulnerabilities.

The threat to core business/proprietary information is another factor that inhibits cloud adoption. Adoption of cloud computing often involves transferring firms’ application software and databases to be managed externally by central data center managers (Subashini & Kavitha, 2011). Threats from access to sensitive data by unscrupulous individuals via the Internet, such as employee salaries, intellectual property such as trademarks and patents, and customers’ medical records, have prevented many firms from adopting this service (Shi, 2012). Furthermore, given that sensitive data is entrusted to the cloud providers, trust becomes a major concern (Tripathi & Jigeesh, 2013; King & Raja, 2012).

The release of firms’ data and applications to cloud providers is often associated with perceived loss of control over their business (Tripathi & Jigeesh, 2013; Sommer, 2013). The loss of direct management of data and applications can leave users feeling vulnerable to security flaws, data breaches, data loss, and theft. These concerns also include a decrease in firm’s interoperability and interconnectivity. Use of a cloud provider often prevents users from sharing data or communicating with other cloud providers’ systems (Tripathi & Jigeesh, 2013). This locks in cloud users with one cloud provider and limits users’ ability to attain customized cloud solutions. In summary, Khajeh-Hosseini et al. (2010) found that enterprises could not easily adopt cloud computing due to “practical, socio-political and socio-technical reasons” (p. 3). Business decision makers considering cloud adoption are challenged by “concerns about costs, confidentiality, control, the impact of work practice and constraints derived from existing business models” (p. 4).

Medical File Storage and the Healthcare Industry

In an earlier study, Hossain and Luby (2010) raised the issue of increased burden of storing and manipulating medical data due to higher life expectancy and the need to accommodate ongoing healthcare services for an ageing population. The authors also noted that the healthcare system was already affected by “high error rates, fragmentation of information, lack of coverage and rising costs” (p. 48). The issues that exacerbate the healthcare conditions in the US, according to Hossain and Luby (2010), include:

- 1) Isolated, non-communicational systems, which are encouraged by the healthcare/medical industry
- 2) Paper-driven system, whereby patients are required to complete forms by hand on each visit, necessitating that the medical personnel enter this information in a

- proprietary system. Handwritten medical records are often the main cause of high error rates due to inaccuracy in transposing information.
- 3) Inefficient methods employed when storing patient files, which often take up large amounts of storage space. Many healthcare or medical providers maintain hardcopies of their patients' files locally.

Overall, the authors found that the predominantly paper-driven method of capturing, processing, and storing patient data tends to be time consuming and redundant, leading to higher operating costs.

The US healthcare sector is also burdened by industry and government regulations. HIPPA, as one of the key federal regulations, aims to protect patients' sensitive data (Witt, 2011), which includes information on individuals' history of medical conditions, prescription drug use, gender, and sexual orientation (King & Raja, 2012). The healthcare industry is distinct from other industries in that its data is "highly sensitive and it has multiple entities having access to patients data, including hospital administration, labs, payers, and even patients" (Pasquale & Ragone, 2013, pp. 6-7). HIPPA regulates all healthcare providers, health plans, and healthcare entities labeled as "covered entities" (CEs) (p. 13). Moreover, liability is extended beyond the CEs to business associates operating within the healthcare industry, which includes service vendors and subcontractors (p. 14).

Healthcare sector is thus challenged to meet increasing burden on its resources with growing pressure to conform to stringent regulations. Hence, it is not surprising that cloud adoption has increased in popularity. Extant research reveals several factors that have driven cloud adoption in the healthcare context (Hossain & Luby, 2010; Sultan, 2014), including (1) the need for an effective electronic data management system, mandated by HIPPA Omnibus, and ARRA regulation; (2) the need to significantly decrease healthcare IT cost of acquiring, operating, and maintaining physical IT infrastructure; (3) global access to patient information on demand; (4) the need for scalable IT infrastructure with the capability to adapt to growing demand for data processing and storage; and (5) the ability to electronically track and measure performance against industry benchmarks.

GE Healthcare responded to some of these needs by introducing a cloud-based SaaS solution known as "Centricity Practice" (Sultan, 2014, p. 179). In partnership with the company Med Cloud, this cloud-based solution provides patients access to their own private portal via the Internet. Patients are thus able to securely interact with their healthcare provider, schedule medical appointments, and review their medical information (Sultan, 2014). Healthcare organizations that have adopted this cloud computing solution are thus able to provide their patients superior customer service, and increase overall efficiency in their operations, while decreasing their labor costs and reducing the time required for paperwork processing.

In addition to the many benefits of cloud adoption, healthcare decision makers must also be aware of certain disadvantages, in particular:

- 1) "security risks, integration issues and the inability of cloud computing to cope with business process changes" (Sultan, 2014, p. 182).

- 2) lack of control over organizations' data and applications when cloud services are managed by cloud providers through proprietary application programming interface (APIs), a software-to-software interface. This dependence on cloud providers increases operational and security concerns and magnifies opportunities for nefarious activity to occur (King & Raja, 2012).
- 3) susceptibility to system limitations and failures of cloud providers.
- 4) questionable reliability of cloud computing service in an event of updates and/or outages, whereby patients' data become temporarily inaccessible (Sommer, 2013).

Hossain and Luby (2010) identified additional barriers to cloud adoption by healthcare/medical personnel, namely reluctance of healthcare/medical personnel to change current practices, lack of proper training for healthcare/medical personnel, and difficulty in using the new system due to a higher learning curve for some staff. In a later study, Sultan (2014) highlighted that, in the US, over 300 electronic health record (EHR)/personal health record (PHR) systems are presently in use; however, only about 1% of these have adopted the innovation due to cost and poor usability. Sommer (2013) also noted that cost of acquisition and/or maintenance of cloud computing technology might be an issue for some organizations, especially small healthcare/medical entities. Moreover, when multiple users are sharing variety of resources virtually, the risks of unauthorized users viewing and/or accessing sensitive data increase substantially (King & Raja, 2012).

Theoretical Framework

A greater understanding of the benefits and risks of cloud adoption can be gained through the thoughtful application of theories related to innovation resistance, diffusion, and Rogers' (2003) innovation decision process. In this work, a theoretical framework incorporating diffusion and innovation resistance theories is employed as a basis for understanding the resistance to cloud adoption among healthcare decision makers.

Despite the popularity of diffusion theory, a universally agreed upon definition of diffusion does not presently exist (Surry & Farquhar, 1997). Rather, many elements originating from varying disciplines are incorporated into a meta-theory of diffusion (Surry & Farquhar, 1997). Diffusion was defined by Rogers (1983) as "the process by which an innovation is communicated through certain channels over time among the members of a social system" (p. 10). While Rogers (1995) introduced four diffusion theories—innovation decision process, perceived attributes, rate of adoption, and individual innovativeness—this work focuses on the innovation decision process only.

Before expounding on the innovation decision process, it is essential to define the term "innovation." Rogers (1983) understood it as "an idea, practice or object that is perceived as new" (p. 11). This definition of innovation places emphasis on individuals' assessment of something being new or not. Ram (1987) defined innovation from a marketer's point of view, as "a product which is perceived by the consumer as new" (p. 208). In this context, the newness of a product is considered an innovation if viewed as embodying a change from existing products, services, or processes. When an idea, object, or practice is considered new, the willingness to accept or adopt it depends on the individual's perception of the effect the innovation will have on his/her life (Laukkanen et al., 2007).

Ram (1987) labeled individuals' unwillingness to accept an innovation as resistance to change or innovation resistance. Innovation resistance can only occur if consumers perceive a product, service, or practice as new (Ram, 1987; Laukkanen et al., 2007). This aspect of innovation is crucial to this discussion because it explains why an innovation such as cloud computing may be met with resistance by healthcare decision makers during the innovation decision process. Innovation researchers often portray innovation as an auspicious development and an improvement over existing product/service or practice. However, as individuals may not share this view (Ram, 1987), their reluctance to adopt a product or service may result in its failure. Therefore, innovation resistance, "is the resistance offered by consumers to changes imposed by innovations" (p. 208). For this reason, the concept of innovation resistance was incorporated within the theoretical framework of this paper. With this understanding, the following propositions are made:

Proposition 1: Cloud computing is a new technology that imposes change on existing healthcare practices, specifically the management of patient data and applications.

Proposition 2: The change realized through cloud adoption within the healthcare industry will be encountered with resistance. The acceptance and adoption of an innovation greatly depend on how the innovation is diffused. This assertion has resulted in the notion of innovation decision process, referring to the manner in which individuals attain and interpret information about the innovation (Rogers, 2003). It comprises of five stages, denoted as knowledge, persuasion, decision, implementation, and confirmation (Rogers, 2003). In the current context, the process is used to identify the resistance healthcare decision makers experience at each stage. This reasoning leads to the third proposition below.

Proposition 3: Each stage in the innovation decision process provides individuals the opportunity to either adopt or resist the innovation. The exposure to an innovation through the innovation decision process creates an opportunity for change to occur. As information regarding the innovation is diffused, individuals' attitudes and perceptions become engaged. The decision to adopt or reject an innovation is typically based on the individuals' attitudes, perceptions, and behaviors toward the innovation. The conceptual model in Figure 2 provides a graphic representation of this construct, illustrating various reasons behind potential resistance to cloud adoption at each stage of the innovation decision process.

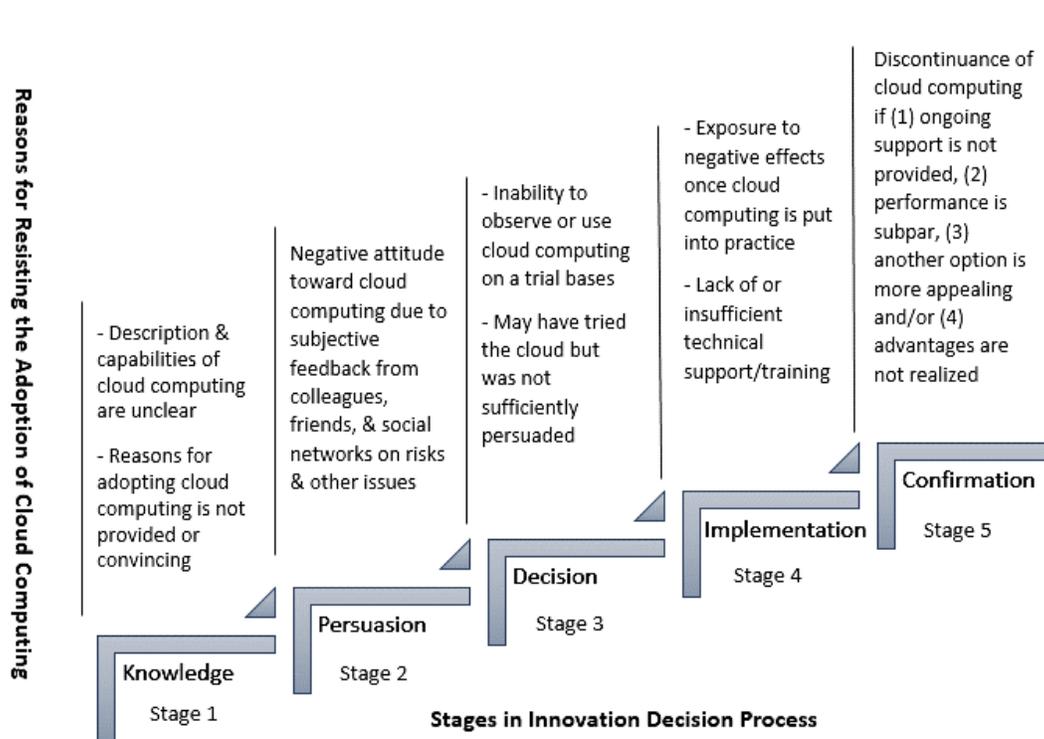


Figure 2. A Depiction of Resistance to Cloud Adoption at Each Stage of the Innovation Decision Process.

Conceptual Model

Knowledge stage: At the first stage of the innovation decision process, individuals learn about the innovation. The basic questions such as “*what is it? how does it work? and why is it needed or important?*” (Rogers, 2003, p. 21) are answered. Failure to provide a complete picture of the capabilities, limitations, and relevance of the innovation can lead to rejection.

Persuasion stage: Once the individual has attained a certain level of knowledge about the innovation, a negative or positive attitude is formed toward the innovation (Rogers, 2003). At this stage, the resistance to the innovation is influenced more strongly by opinions and evaluations of one’s peers and social group than by objective information from experts (Rogers, 2003).

Decision stage: The individual can chose to either adopt or reject the innovation at this stage. Rejection is typically classified as either active or passive. In the first case, the individual attempts to use the innovation but decides to reject it after further consideration (Rogers, 2003). On the other hand, passive rejection occurs when the individual rejects the innovation outright without any consideration of its potential utility (Rogers, 2003).

Implementation stage: In the implementation stage, the innovation is implemented, thus introducing uncertainty about the outcomes (Rogers, 2003). This uncertainty may produce many questions on the usability of the innovation.

Confirmation stage: At the final stage, the innovation can be fully accepted or its use can be discontinued. The discontinuation of an innovation can occur for many reasons, including the failure of the innovation to meet the individual's expectations or the discovery of a more suitable replacement (Rogers, 2003).

This framework indicates that, at each stage of the innovation decision process, decision makers considering cloud adoption must be cognizant that resistance is virtually inevitable and must be proactively addressed.

Methodology

In conducting this study, an evidence-based research approach was applied to review a wide array of primary literature. Certain steps were taken to ensure that scholarly and other relevant literature pertinent to the study objective was included. The literature review commenced by searching for appropriate sources using keywords, applying a selection process, and establishing criteria to narrow the list of final literature sources to be examined in the paper. Using a thematic approach, the findings were subsequently summarized and synthesized. A thematic synthesis compares diverse and multiple primary studies and systematically organizes data, allowing common themes to emerge (Barnett-Page & Thomas, 2009).

The search strategy extended to three primary academic disciplines: information and communication technology, healthcare management, and innovation management. To ensure that appropriate variety of articles was selected, the following databases were searched: Business Source Complete, ABI/Inform, Google Scholar, EBSCOhost, ScienceDirect, Web of Science, and ERIC. Five keywords/phrases were used in the search, namely cloud computing, innovation diffusion theory, innovation decision process, innovation resistance, and healthcare/medical industry. This strategy yielded several hundred potentially relevant literature sources.

In applying the "fit for purpose" approach, as proposed by Gough, Oliver, and Thomas (2012, p. 249), this initial set was subjected to further scrutiny, in order to select the most relevant sources applicable to this study. Initial screening of the research articles generated by the initial search was based upon a rapid assessment of titles and abstracts to determine the relevance to the topic and decide whether to include or exclude them in the final list.

Table 1. Criteria Used During Literature Search

Inclusion and Exclusion Search Criteria
1. Full text, scholarly journal articles, research reports, and books included
2. Keyword focused
3. Literature on cloud computing published within the last 10 years (2004 to present)
4. Dated literature included only work of seminal theorists
5. Both qualitative and quantitative studies included
6. Non-English literature excluded

Application of the criteria listed in Table 1 resulted in 17 scholarly journal articles, 2 research reports, and 1 conference paper. The topic of cloud computing is an emerging innovation and is being propelled by rapid changes in ICT; thus, the search was confined to literature sources discussing cloud computing that were published in the last 10 years.

Analysis/Findings

In synthesizing the findings of the literature review, several themes emerged and categorized under three groups of key healthcare stakeholders.

Healthcare Providers and Managers

Theme 1: Healthcare entities are governed by stringent industry and government regulations (Sultan, 2014; Pasquale & Ragone, 2013; King & Raja, 2012; Hossain & Luby, 2010).

Theme 2: Innovation challenges existing practices (Ram, 1987; Laukkanen et al., 2010), requiring individuals to change their attitudes, preferences, and/or behaviors to adapt to the attributes of the innovation.

Theme 3: Resistance is a normal response to change (Ram, 1987).

Theme 4: At every stage of Rogers' (2003) innovation decision process, users can either reject or adopt cloud-computing innovation.

Healthcare IT Professionals

Theme 5: Cloud computing is an innovative technology that exposes the healthcare industry to many benefits and challenges (Sultan, 2014; Hossain & Luby, 2010).

Theme 6: The attributes and complexity of cloud computing increase innovation resistance. The innovation itself is a problem for many users. Cloud computing is distinct from other computing products, as it is offered as a computing service via the Internet, benefitting from remote data servers (Khajeh-Hosseini et al., 2010). Thus, the intangible aspect of cloud computing and the fact that it functions within a virtual environment heightens users' uncertainty and discourages its adoption (Shi, 2012; Subashini & Kavitha, 2011).

Theme 7: Researchers and practitioners concur that cloud computing is fraught with risks. The primary risks involve security to patients' personal and medical data, as well as threats to software applications and IT infrastructure (Sultan, 2014; King & Raja, 2012; Shi, 2012; Hossain & Luby, 2010).

Cloud Service Providers

Theme 8: The risks of adopting cloud computing can negatively influence healthcare entities if not properly managed. There is a general assumption of trust between healthcare providers and their patients, one that is protected by industry and government regulations and extends to safeguarding verbal and written interactions and agreements between all parties in relation to the patients' personal and medical data (King & Raja, 2012; Tripathi & Jigeesh, 2013).

Theme 9: The use of cloud providers can result in loss of control over proprietary data, since the transition to cloud storage implicitly removes the responsibility of firms for supporting and maintaining the software, applications, and IT infrastructure that house the data in the cloud. This increases the risk that the security of proprietary information can be mismanaged both intentionally and unintentionally. Furthermore, inadequate security protection can enable malicious entities (such as hackers or identity thieves) to take advantage of security flaws (King & Raja, 2012; Tripathi & Jigeesh, 2013).

Theme 10: The inability to customize third-party cloud service solutions based on business needs decreases interoperability and interconnectivity with existing business systems (Tripathi & Jigeesh, 2013).

Discussion

The findings yielded by the literature review strengthen the conceptual framework proposed in this paper. In particular, they reveal that, at each stage of the innovation decision process, healthcare decision makers gain conceptual and practical knowledge on cloud computing, at which time negative conclusions may be formed that discourage cloud adoption. For example, the risk of security breaches to patient data was one of the primary challenges to cloud adoption revealed in the review of literature. Healthcare decision makers going through the innovation decision process could learn about this issue at the persuasion stage by seeking input from their colleagues or social groups. The subjective feedback may not be valid; however, the fact that it is treated as such and it influences the decision maker's resistance to cloud adoption makes it significant. Likewise, the possible loss of control of firms' data to cloud providers is another challenge that may arise at the implementation stage, as this is when hands-on training with a cloud provider typically takes place and users are exposed to the capabilities and limitations of cloud computing. Similarly, it is at this stage that unwillingness to entrust a third party vendor with the firm's data develops, as issues may arise while testing and assessing the workings of cloud computing.

Yet, despite these challenges, the benefits of cloud computing adoption for healthcare entities are worth considering particularly due to the HIPPA Omnibus and ARRA mandates. All healthcare entities are mandated to transfer all patient data into an electronic system while upholding the confidentiality afforded to patients by law. Cloud computing challenges this mandate due to the

impediments identified earlier in this paper. However, healthcare regulations and cloud adoption can coexist (Witt, 2011). Healthcare decision makers can confidently, albeit cautiously, adopt cloud computing by having a clear understanding of the benefits and challenges associated with cloud adoption and applying strategic tools during the decision process.

Implications for Healthcare Management Practice

This paper offers healthcare decision makers the *Cloud Adoption Toolkit* developed by Khajeh-Hosseini et al. (2010) as a possible solution to the issues currently associated with cloud adoption. The cloud adoption toolkit takes an analytical approach in assessing the capabilities and limitations of cloud computing within the organizational environment. There are two major advantages to employing the cloud adoption toolkit: (1) the viewpoints of all relevant stakeholders are captured to assist the innovation decision process, and (2) the toolkit utilizes existing organization's tools or techniques to respond to cloud adoption concerns (Khajeh-Hosseini et al., 2010).

Khajeh-Hosseini et al. (2010) classified concerns over cloud adoption into three groups, the first of which consists of the technical aspects of cloud computing, namely the "technical feasibility, availability and security of the system" (p. 5). The authors found "technology suitability analysis" (p. 5) the most useful tool for assessing the technical concerns of cloud adoption. Conducting a technology suitability analysis can assist healthcare decision makers in responding to the challenges identified earlier in this work, specifically "elasticity, availability and dependability, security and regulatory requirements" (p. 6).

The second group of concerns involves the cost of cloud adoption, which includes "operational costs and power consumption" (p. 5). A "cost modeling tool" (p. 5) allows the decision makers to estimate the cost of migrating and operating "IT systems on the cloud with the aim of minimizing costs" (p. 5) more accurately, while also facilitating "power consumption analysis" (p. 5). By being aware of the total energy IT systems will utilize for cloud computing, organizations can address many cost concerns associated with feasibility of cloud adoption (Khajeh-Hosseini, et al., 2010).

Finally, the third group of concerns pertains to the risks to work activities and overall organization's operation if cloud computing is adopted (Khajeh-Hosseini et al., 2010). The operational concerns of cloud adoption can be mitigated by "stakeholder impact analysis and responsibility modeling" (p. 5). The stakeholder impact analysis assesses the risks that cloud adoption would pose to existing work activities, as well as social and political factors (Khajeh-Hosseini et al., 2010). Thus, it is a significant tool for healthcare decision makers because it helps explain the resistance to cloud adoption at each stage of the innovation decision process.

Responsibility modeling helps decision makers identify the "responsibilities for constructing, operating, maintaining, and managing the IT system" across multiple organizations, departments, and cloud service providers (Khajeh-Hosseini et al., 2010, p. 9). This tool addresses the concern healthcare decision makers have regarding the loss of control over patients' information. It provides a clear outline of roles and responsibilities, thus helping minimize apprehension when negotiating contractual agreements with cloud providers. Hon et al. (2012) recommended that healthcare decision makers consider current and future business needs when discussing the terms

in cloud service contracts. When entering into cloud service contracts, “provider liability, service level agreements, data protection and security, termination rights, unilateral amendments to service features and intellectual property rights” are the most common changes often negotiated between cloud users and cloud providers (p. 79). Another safeguard is to secure that specialized staff established by cloud providers is dedicated to managing security challenges (King & Raja, 2012).

Despite the limited empirical research on the cloud adoption toolkit (Khajeh-Hosseini et al., 2010), it can be recommended for use by healthcare decision makers aiming to systematically address the challenges to cloud adoption.

Implications for Future Research

This study adds to the limited body of theoretical and practical research on cloud adoption within the healthcare context. Innovation theories have been extended by highlighting the relevance of incorporating innovation resistance to the discussion. The concept of innovation resistance is fundamental to understanding the effects that new technology has on users and warrants greater attention in innovation research. Recognizing that resistance to change is a normal reaction to anything new and that innovation can upset existing practices has important implications for researchers and practitioners. Furthermore, practical strategies were proposed in response to the challenges healthcare decision makers face during the decision process.

Future research can help strengthen the proposed cloud adoption framework and/or produce alternative viable solutions. Finally, though this research is limited to cloud adoption within the healthcare context, given the vast potential and wide applicability of cloud computing, additional research focusing on other industries may prove beneficial.

Conclusion

The objective of this study was to answer the research question, *what are the forces influencing the adoption of cloud computing within the healthcare industry?* Both benefits and challenges were examined with respect to their impact on healthcare decision makers tasked with adopting cloud computing in their organizations. The findings revealed that change stemming from innovation is often met with resistance. Moreover, the innovation decision process provides individuals the opportunity to reject or accept the innovation at each stage of adoption.

While the work presented here offers some guidance to healthcare decision makers, it is essential to ascertain whether the benefits of cloud technology outweigh the risks associated with its use in the healthcare industry. Based on the literature analyzed in this study, there is sufficient evidence to suggest that this innovation can bring significant benefits to the healthcare industry. Nonetheless, the risks—including breaches to the security and privacy of patient data and loss of control of data management to cloud providers—must be carefully evaluated, especially due to the stringent regulations that govern the industry. Nonetheless, those risks are not insurmountable and can be mitigated if the appropriate solutions, such as the application of analytical tools, are implemented during the decision process and effective safeguards are put in place, particularly in contractual agreements with cloud providers.

References

- Barnett-Page, E., & Thomas, J. (2009). Methods for the synthesis of qualitative research: a critical review. *BMC Medical Research Methodology*, 9, 59-69.
- Gough, D., Oliver, S., & Thomas, J. (2012). *An Introduction to Systematic Reviews*. London, UK: Sage Publications.
- Hon, W., Millard, C., & Walden, I. (2012). Negotiating cloud contracts: looking at clouds from both sides now. *Stanford Technology Law Review*, 79-129.
- Hossain, S., & Luby, D. (2010). Cloud computing in healthcare industry. In *Global Science and Technology Forum 2010 proceedings of the Annual International Conference on Cloud Computing & Virtualization* (pp. 42-50). Retrieved July 2, 2014, from <http://www.globalstf.org/docs/proceedings/ccv/193.pdf>
- Iyer, B., & Henderson, J. C. (2012). Business value from clouds: learning from users. *MIS Quarterly Executive*, 11(1), 51-60.
- Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2010). The cloud adoption toolkit: addressing the challenges of cloud adoption in enterprise. *Software: Practice and Experience*, 1-10.
- King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, 28(3), 308-331. Retrieved July 20, 2014, from <http://dx.doi.org/10.1016/j.clsr.2012.03.003>
- Laukkanen, T., Sinkkonen, S., Kivijärvi, M., & Laukkanen, P. (2007). Innovation resistance among mature consumers. *Journal of Consumer Marketing*, 24(7), 419-427.
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Retrieved July 27, 2014, from <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Park, S., & Ryoo, S. (2012). An empirical investigation of end-users' switching toward cloud computing: a two factor theory perspective. *Computers in Human Behavior*, 29(1), 160-170.
- Pasquale, F., & Ragone, T. A. (2013). The future of HIPAA in the cloud. Retrieved July 13, 2014, from http://digitalcommons.law.umaryland.edu/fac_pubs/1363/#?
- Ram, S. S. (1987). A model of innovation resistance. *Advances in Consumer Research*, 14(1), 208-212.
- Rogers, E. (1983). *Diffusion of Innovations* (3rd ed.). New York, NY: Free Press.
- Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York, NY: Free Press.
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.

- Shi, M. (2012). Incorporating information security in analysis of business strategy: a conceptual framework. *Computer & Information Science*, 5(5), 1-16.
- Sommer, T. (2013). Cloud computing in emerging biotech and pharmaceutical companies. *Communications of the IIMA*, 13(3), 37-53.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11. Retrieved July 20, 2014, from <http://dx.doi.org/10.1016/j.jnca.2010.07.006>
- Sultan, N. (2014). Making use of cloud computing for healthcare provision: opportunities and challenges. *International Journal of Information Management*, 34(2), 177-184.
- Surry, D. W., & Farquhar, J. D. (1997). Diffusion theory and instructional technology. *Journal of Instructional Science and Technology*, 2(1). Retrieved July 29, 2014, from <http://www.southalabama.edu/coe/bset/surry/papers/dtit/dtit.htm>
- Tripathi, S., & Jigeesh, N. (2013). A review of factors that affect cloud computing adoption. *IUP Journal of Computer Sciences*, 7(4), 48-59.
- Witt, C. (2011). HIPAA versus the cloud. *Journal of Health Care Compliance*, 13(5), 57-68.
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592. Retrieved July 19, 2014, from <http://dx.doi.org/10.1016/j.future.2010.12.006>

Author's Biography

Linda Barthelus is the Director of the College Call Center at Northern Virginia Community College in Virginia. She holds a B.S in Marketing; a Master's in Business Administration and earned her Doctorate in Management in 2015 from University of Maryland University College. Dr. Barthelus has worked in the call/contact center industry for the last 15 years. She has earned several performance-based awards for managing contact center operations with high efficiency & effectiveness. Her research interest includes innovative technologies, tools and practices that effectively drives and supports contact center business, telework, e-business, web-based and e-learning, omni-channel communications and customer relationship building and management.