DOI: https://doi.org/10.53555/nnbma.v2i1.114 **Publication URL: http://nnpub.org/index.php/BMA/article/view/114**

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

Ayman Talib[1]*
*[1]*Associate professor of MIS – Department of business and management DeVry University – Chicago USA*
atalib@devry.edu
Jamal Shaban[2]
[2]Verizon wireless Inc – Chicago USA jashaban@gmail.com

Corresponding Author: -
Email: atalib@devry.edu

Abstract: -

This study aims to explore the factors that hinder small organizations in the United States from adopting cloud computing. The study focused on extending the Technology Acceptance Model (TAM) to include the external variables that can have an impact on small organizations' decisions when adopting the cloud technology. This study focused on small organizations from three service sectors, financial, health care and leisure. An Internet based survey was sent out to 131 participants who were conveniently sampled with an attempt to collect information about their concerns of the cloud technology. The findings indicate that small organizations are not adopting the cloud technology due to five main factors: security, compliance, service level agreement, business continuity and contract lock-in.

Keywords: - *Cloud Computing; Security; Compliance; Service Level Agreement; Business Continuity; Contract lock-in*

1. INTRODUCTION

Cloud Computing (CC) is no longer the buzzword that had everyone's attention; rather it has become predominant throughout all industries in the past two years. According to a recent survey of 527 Harvard Business Review readers in large and midsize organizations around the world, over seventy percent of organizations have already adopted the Cloud technology[i]. A comparable survey on small businesses published by Intuit on April, 2015 revealed that thirty seven percent of small businesses in the United States are currently utilizing CC services. That number expected to grow to seventy eight percent in 2020[ii]. Although these results fairly correlate with Cloud adoption data reported globally, they however indicate that security and compliance are of the utmost concern for both those who adopted and for those who want to adopt. In one study conducted by the Federation of Small Businesses (FSB), data security was cited as the biggest concern with regards to companies not implementing cloud computing services. Other reasons included the lack of technology awareness, and concerns with regulatory compliance.

Adoption of the cloud has increased across the board, and this can be attributed to the flexibility of the cloud, the ability to constantly cope with an ever-changing environment, reduced administrative costs, and the burden of constant hardware and software upgrades.

Regardless, studies show that security continues to be the main hurdle in the fast adoption of the cloud among adopters and laggards [36]. Numerous security risks arise when housing data in the cloud according to [3] including data availability, integrity, confidentiality, access, segregation, privacy, recovery, accountability, and multi-tenancy issues. Another inhibitor is Contract Lock- in and Service Level Agreement (SLA). Contract lock-in is of interest to the cloud service provider (CSP), but when unsatisfied tenants decide to change a cloud service provider, they can face severe constraints in moving their data to another CSP and find themselves locked in [16].

Service level agreement describes the specific of services and expectations of delivery. Many if not all CSPs promise 99.99% uptime but network outages are inevitable. [29] presented an example of outages and the consequences: "In a period of less than 60 days, Apple MobilMe, Google Gmail, Citrix, and Amazon S3 all reported outages or periods of unavailability from 2 to 14 hours; in March 2009, Microsoft Windows Azure was down for 22 hours" and "A cell phone provider that stored customer data in a Microsoft subsidiary provided cloud became unavailable when the provider lost that data. Customers had to wait for days to be informed that a possibility (but no guarantee) existed that their data may be able to be restored. However, the extent of data recovery, the level of data integrity, and the timeline to restore remain to be seen".

Compliance is another critical issue that hinders organizations from moving their data to the cloud. Customers, specifically those in the financial and health industries, have their own regulatory compliance to conform with. Keeping their data on their own premises permits them to have the necessary controls to remain compliant with laws and industry regulations. However, by moving their data to the cloud, tenants need to observe where data will be kept since they no longer have control over it, as data is in the hands of the cloud computer service provider as noted by [3]. Additionally, as technology moves much faster than law makers, government and the industry are playing the catch-up game in declaring new regulations for gaps not being addressed by the Cloud service provider, as a result, the law is always behind[iii]. New regulations to protect customers might force Cloud service provider to assume more responsibility, which in turn encourages more organizations to adopt the Cloud.

In an attempt to study the factors that can have an influence on small business decisions to adopt the cloud computing, we will rely on the Technology Acceptance Model (TAM).

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 [2][11][39][40][34][42].

The *Technology Acceptance Model* (TAM) is widely used in the information systems' literature to help explain the factors that influence technology acceptance [5]. TAM, as cited in most research that dealt with user acceptance of technology was criticized by many because it attracted more quick research and gave less attention to the real problem [21]. Critics suggested exploring whether the Perceived Usefulness (PU) and Perceived Ease of use (PEoU) factors in TAM are the mediators of external variable effect, and if this effect is found, it will be very important to identify these variables [38][39]. In general, the TAM model explains between 30% and 40% of system usage [7]. Further, PU is often found to be the strongest determinant in the model [7][19][25]. A plentiful amount of research had extended the TAM model to enhance the knowledge of technology acceptance and adoption [44]. In this study, we will explore the possibility to extend the TAM model (Fig. 1) to include the external variables such as 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. More precisely, we will examine factors that contribute to small organizations reluctance to adopt the evolving CC 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

2. Cloud Computing Research

Current research on the cloud computing adoption rate among small businesses reports that more than 60% of small organizations are reluctant in adopting CC services. These studies revealed that lack of security and regulations in CC is a major drawback [31]. Government and the industry are currently playing the catch-up game in declaring new regulations for gaps not being addressed by the CSP. As a result, new regulations might force CSP to assume more responsibility in an effort to encourage more organizations to adopt the Cloud. To further investigate the factors behind small organizations reluctant in adopting CC, this study focuses on small organizations' in the financial, health care, and leisure industries reluctance to CC adoption, specifically with regards to compliance. 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 will not be ignored but rather briefly discussed and included in the data analysis as well.

2.1 Data Security in the Cloud

Many organizations still believe that data managed internally is more protected than being externally managed (e.g., Cloud provider)[iv]. Although data can be well stored and kept at a secure location, but it can be stored with un-trusted hosts as well, which creates enormous risks for data privacy [9]. Many breaches have already hit the health-care, financial, higher- education and federal markets, and even the security industry itself this year, which affected millions of people and exposed their personal information [35]. Among these companies were [CareFirst, BlueCross BlueShield, Anthem, Harvard University**,** Password management company LastPass, and Army National Guard][v] , According to Herrmann (2008), "Security is one of the core competencies of the Cloud provider" [45]. Some statistics show that one-third of internal data breaches are caused by lost or stolen laptops or other devices containing company confidential information or employees exposing data on the Internet, and 16% are caused by internal theft [27]. Since CSPs are equally subjected to security requirements, many do not accept responsibility for the data stored at their infrastructure. They relinquish their responsibility of any risk [10]. Loss of data control is not the only security concern but data-in transit, data-at-rest, processing of data, including multi-tenancy, data lineage, data provenance, and data reminisce (magnetization) are also equally concerns to account for [24]. Many firms, mainly financial institutions, are expected to adapt their information security policies, standards, and practices to incorporate the activities related to a CSP.

2.2 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 [18]. According to [1], "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". 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 [6], 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.

2.3 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. [41] 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 [33]. 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 [28]. For instance, when the tenant decides to move their software operation to a new CSP due to price increases or a 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 [8]. According to [6], "concern about the difficulty of extracting data from the Cloud is preventing some organizations from adopting Cloud computing".

2.4 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 [15]. 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 [43]. This 99.9% of network up-time translates mathematically into four minutes 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 [12][13]. 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. 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" [22]. 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.

2.5 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 [17]. 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, we will examine three regulatory compliances specific to the financial, health care, and leisure services, identified as FINRA, HIPAA, and PCIDSS.

2.6 Financial Industry Regulatory Authority (FINRA)

In general, FINRA's mission was to protect investors by making sure financial institutions operate fairly and honestly. They require that business-related electronic records be kept in non- rewritable, non-erasable format (also referred to as "Write-Once, Read-Many" or "WORM" format) to prevent alteration. The Securities and Exchange Commission has stated that these requirements are an essential part of the investor protection function because a firm's books and records are the "primary means of monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards". 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 2013, FINRA fined Barclays $3.75 Million for Systemic Record and Email Retention Failures. [14].

Some companies do not fully state they are compliant, but appear to have the standards in place to be compliant. Although, 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 complaint.

On outsourcing in financial services, Michael Macchiaroli (Associate Director, Office of Risk Management & Control, Division of Trading and Markets, U.S. Securities and Exchange Commission) 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 [23].

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.

2.7 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 [37].

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 healthcare 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 [32], 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, [20] 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. [26] Wrote about two recent data breaches at the Oregon Health

and Science University when the staff inappropriately stored unencrypted 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."

2.8 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. If a data breach occurs, tension leads decision makers to make difficult choices. These difficult approaches highlighted the challenges of maintaining consumer trust and compliance while abiding by different and conflicting disclosure laws [4].

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 [30]. 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 [30].

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.

3. Method and Sample

This study focused on participants from small organizations in three specific industries within the United States. The participants who completed the survey were conveniently sampled and comprised of individuals from a wide range of service sectors, but the main three industries were: financial services (12%), health services (25%), and leisure services (22%) in the context of small organizations in the United States. Participants included blue and white collar employees, IT Management, CTOs, and small business owners. The participants' knowledge of cloud computing were measured as no knowledge, beginner, intermediate and advanced; these measures came in as 20%, 34%, 31% and 15% respectively. In addition, 44% of the participants indicated that they are using at least one cloud computing service, 35% are considering the evaluation of the cloud service to be part of their business operation and 21% are not currently considering the cloud service. From those who indicated using or evaluating to use the cloud are considering the Infrastructure as a Service (IaaS) 30%, Platform as a Service (PaaS) 36%, and Software as a Service (SaaS) 66%. They also indicated they will utilize or evaluate to utilize the following cloud computing models, public cloud (32%), private cloud (47%), hybrid cloud (13%) and community cloud (19%).

3.1 Data Analysis

The main focus of this study was to extend the TAM model to include the external variables that are thought to have an impact on the cloud adaptation rate within small organization in three industries, health services, financial service and leisure services. The literature review had identified the following external variables: data security concerns, business continuity, contract lock-in, service level agreement and compliance as the major obstacles that prevent small organizations from adopting the cloud computing technology.

The objectives of this data analysis section are first to look at the participants who already are utilizing the cloud technology and to explore their own concerns as of why some organizations are still reluctant in adopting the cloud technology. The second objective is to look into the people who are evaluating the possibility of adopting this technology, but are still reluctant, we want to learn about their concerns. Our ultimate goal after the data analysis is to try to put together a logical extension to the TAM model with the focus on the identified external variables.

3.2 Measures

Information about the *data security concerns* in the cloud technology was administered with three Likert scale questions, each of which asked the participants to indicate their agreement on three key security factors: data availability and data security, loss of control over own data and data loss and privacy. The Likert scale questions measured the agreement level using five points scale ranging from (1- strongly disagree to 5 – strongly agree), the survey results came in with respondents mostly agreeing on the importance of the data security concerns if they want to make a decision to adopt the cloud technology (M = 4.1; SD = 0.7).

Business continuity information was obtained from two Likert Scale survey questions. The questions asked participants to rate their concerns about business continuity when adopting the cloud technology. The five points (1 – strongly disagree to 5 – strongly agree) Likert scale survey questions focused on business continuity concerns and business continuity and service availability; the respondents were moderately concerned about business continuity when the cloud technology is used or is evaluated for use (M = 3.7; SD = 0.8).

Contract lock-in information was obtained by summing the results of two Likert scale survey questions, the questions were constructed with five points scale (1 – strongly disagree to 5 – strongly agree). Participants were asked to rate the importance of contract lock-in if the cloud technology is the firm choice. This factor was also rated with moderate importance (M = 3.2; SD = 0.11).

Service level agreement was obtained from one single five points Likert scale question. The participants were asked to rate the importance of the service level agreement when using or considering to use the cloud technology. The participants felt that this factor is moderately important and could be an obstacle, if missing, when decisions are made to adopt the cloud technology (M = 3.6; SD = 0.1).

Compliance information was obtained from two Likert scale survey questions. We were interested to know how participants rate the importance of vendors' compliance fulfillment. It as found from the participants responses that compliance is an important factor that is always considered when firms are deciding to adopt the cloud technology (M = 3.4; SD = 0.9).

4. Discussion and Conclusion

Clearly, the scope of this study is limited due to its sampling technique. The assumption that these external variables do exist and can have an impact on the cloud computing adaptation rate is yet to be tested in a more comprehensive and detailed framework. Our main focus on this paper was to gather enough information about the cloud technology adoption concerns from actual cloud users or from users who are evaluating the cloud adoption idea. Therefore, by keeping this limitation in mind, we can comfortably state that the results from this data analysis have shed the light on few cloud computing adoption key concerns that we had classified as a set of external variables. The participants of this research were asked about their concerns of the cloud technology. After the analysis of the data, five factors were identified as the top major concerns that we thought to have prevented or slowed small organizations efforts from adopting the cloud technology. The identified external variables are compliance, security, SLA, business continuity and contract lock-in.

Our next step after the publication of this research is a follow up study that is going to test the effects of these external variables in the context of the TAM model (Fig. 1). Our plan is, first to test the direct effects of the external variables on the Perceived Usefulness (PU), Perceived Ease of Use (PEoU), intention to adopt and adapt within the TAM model to find out the degree of the association between these variables. Second, we will test the non-direct effect of the external variables on both the (PU) and (PEoU) with the attempt to test if the (PU) and (PEoU) factors in TAM are the mediators of external variables effect, as claimed by [38], [39].

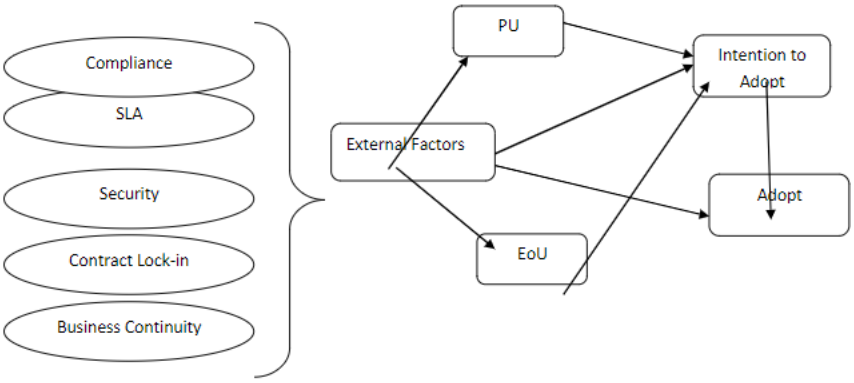

Fig. 1 The extended TAM model (inclusion of five external variables)

Finally, by keeping in mind the limitation about our sampling technique in the current study, our future research will employ a more generalized sampling method such stratified or random sampling techniques that will allow us to draw more generalized results.^{i}

References

[1].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

[2].Agarwal, R., and Prasad, J. (1999). "Are Individual Differences Germane to the Acceptance of New Information

Technologies?". Decision Sciences (30:2), pp. 361-391

[3].Ajakaiye, F., Eviwiekpaefe, A. (2013). The Trend and Challenges of Cloud Computing: A Literature Review. 10.18052. Retrieved from: http://www.scipress.com/ILSHS.16.13

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

[5].Arbuckle, J. A. (1995). Amos 16 Users Guide. Retrieved from: http://amosdevelopment.com

[6].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.

[7].Burton-Jones, A., & Hubona, G. S. (2006). The Mediation of External Variables in the Technology Acceptance Model, *Information & Management*. 43 (6), 706-717.

[8].Buyya, R., Yeo, C. S., & Venugopal, S. (2008). 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.

[9].Chang, H. and Choi, E. (2011). “Challenges and Security in Cloud Computing”. Retrieved from: http://www.chinacloud.cn/upload/2011-11/11112001061070.pdf

[10]. Cloud Security Alliance (CSA). (2011). Defined Categories of Service. Retrieved from: https://cloudsecurityyalliance.org/wp-content/uploads/2011/09/SecaasV10.pdf

[11]. 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.

[12]. Dekker, M., & Hogben, G. (2011). Survey and Analysis of Security Parameters in Cloud SLAs Across the European Public Sector. Online Abrufbar Unter: Retrieved from: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/survey-and analysisof-security-parameters-in-Cloud-slas-across-the-european-public-sector

[13]. European Network and Information Security Agency (ENISA). (2011). Survey and Analysis of Security Parameters in Cloud SLAs across the European Public Sector.

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

[15]. Greiner, L., & Paul, L. G. (2007). SLA Definitions and Solutions. Retrieved from: http://www.cio.com/article/128900/SLADefinitionsandSolutions

[16]. Hofmann, P. and Woods, D. (2010). "Cloud Computing: The Limits of Public Clouds for Business Applications." IEEE Internet Computing, November/December 2010: 90-93. Retrieved from: http://cms.ieis.tue.nl/Beta/Files/WorkingPapers/wp_412.pdf

[17]. Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication*, *800*, 144.

[18]. Kim, H., Lim, H., Jeong, J., Jo, H., & Lee, J. (2009). 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.

[19]. 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

[20]. Kumekawa, J. (2005). Overview and Summary: HIPAA: How our Health Care World has Changed. *OJIN: The Online Journal of Issues in Nursing*, *10*(2).

[21]. Lee, Younghwa; Kozar, Kenneth A.; and Larsen, Kai R.T. (2003) "The Technology Acceptance Model: Past, Present, and Future," *Communications of the Association for Information Systems*: Vol. 12, Article 50.

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

[23]. Loeb & Loeb. (2013). Outsourcing the Law Alert. Retrieved from: http://www.loeb.com

[24]. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. "O'Reilly Media, Inc."

[25]. 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

[26]. 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

[27]. Mills, E. (2009). Cloud Computing Security Forecast: Clear skies. *CNET News.*

[28]. Ommeren, V., E., & Van Den Berg, M. (2011). *Seize the Cloud: A Manager's Guide to Success with Cloud Computing*. IBM Press.

[29]. Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the Security Risks Associated with Governmental Use of Cloud Computing. *Government Information Quarterly*, *27*(3), 245-253.

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

[31]. Pearson, S. (2012), Privacy, Security and Trust in Cloud Computing. Retrieved from: http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf

[32]. Softlayer. (2009). Service Level Agreement and Master Service Agreement. Retrieved from: http://www.softlayer.com/sla.html

[33]. Sultan, R. (2009). Cloud Computing to Education: A new dawn? International Journal of Information Management, 30(2), 109-116.

[34]. 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.

[35]. Thomson, L. Health Care Data Breaches and Information Security. Addressing Threats and Risks to Patient Data. Chapter 15. Retrieved From: http://www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.a uthcheckdam.pdf

[36]. Ullah, S. and Xuefeng Z. (2013). Cloud Computing Research Challenges. IEEE 5th International Conference on Biomedical Engineering and Informatics, pp 1397-1401.

[37]. 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

[38]. Venkatesh, V., & Brown, S. (2001). A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. MIS Quarterly, 25(1), 71-102.

[39]. Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186-204

[40]. 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.

[41]. Viega, J. (2009). Cloud Computing and the Common Man. Computer, 42(8), 106-108.

[42]. 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.

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

[44]. Wixom, B. H., & Todd, P. A. (2005). A Theoretical Integration of User Satisfaction and Technology Acceptance. Information Systems Research, 16(1), 85-102.

[45]. Yates, Gillett, Saleh, & Dines, (2008). “Is Cloud Computing Ready For The Enterprise?”

[i] [i]https://hbr.org/resources/pdfs/tools/Verizon_Report_June2014.pdf

[ii] http://www.slideshare.net/IntuitDeveloper/ebook-the-appification-of-small-business

[iii] http://www.computerweekly.com/feature/CW500-The-legal-risks-of-migrating-to-the-cloud

[v] http://www.mckinsey.com/insights/business_technology/protecting_information_in_the_cloud

[v] http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm

[vi] https://www.finra.org/newsroom/2013/finra-fines-barclays-375-million-systemic-record-and-email-retention-failures