Communications of the IIMA

Volume 12 | Issue 3 Article 1

2012

Cyber Security Considerations When Moving to Public Cloud Computing

Muhammed A. Badamas
Morgan State University

Cyber Security Considerations When Moving to Public Cloud Computing

Muhammed A. Badamas
Morgan State University, USA
muhammed.badamas@morgan.edu

ABSTRACT

Cloud computing has the capability to level the playing field for small and medium sized businesses that find it difficult to acquire and operate the type of information technology found in large organizations. Public cloud computing, the focus of this paper, describes the situation whereby resources are dynamically provided over the Internet via web applications/web services from an off-site third-party provider who shares resources. Public cloud computing provides immense benefits but introduces huge security and privacy risks which makes some organizations apprehensive. This paper examines the potential and possibility of data security concerns to derail the future of public cloud computing. The results of the study reveal that data security concern is the single greatest concern when moving into the cloud.

Keywords: cloud, security, data, private, public, hybrid, service model, Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service

INTRODUCTION

The fundamental shift known as cloud computing has the capability to level the playing field for small and medium sized businesses (SMBs) who find it difficult to acquire and operate the type of information technology found in large organizations. Entrepreneurs, startups, medium and small companies would have new alternatives and opportunities that were not available to them previously. These benefits would save the organizations millions of dollars because they will have the choice to only rent the necessary computing power, storage space, and communications capacity from a large cloud computing provider that has all of these assets connected to the Internet. Cloud computing can be deployed in four ways: Private cloud, public cloud, hybrid cloud and community cloud. Private cloud refers to the management of data and processes within the organization; public cloud describes the situation whereby resources are dynamically provisioned over the Internet, via web applications/web services from an off-site third-party provider who shares resources. Hybrid cloud consists of multiple internal and/or external providers while cloud computing refers to a situation where several organizations jointly construct and share the same infrastructure as well as policies and concerns (Yang & Chen, 2010). This paper deals specifically with public cloud computing.

Public cloud computing enables organizations to spend money only on services they actually receive and consume with the flexibility to adjust the amount of resources they need based on their unique circumstances. While public cloud computing provides immense benefits, it

introduces huge security and privacy risks which makes some organizations apprehensive. Many studies have been conducted into the security risks associated with public cloud computing, but what is lacking is determining whether any of these security breaches could potentially derail the future and momentum of public cloud computing. This paper examines the potential and possibility of data security concerns to derail the future of public cloud computing. The paper identifies measures that could be employed by providers to boost the confidence of existing cloud users and attract potential users.

LITERATURE REVIEW

Cloud computing has been touted as a technology which is gaining momentum at an alarming rate (Rimal, Choi, & Lumb**,** 2009). Cloud computing has been defined in many different ways by many researchers (Bisong & Rahman, 2011) but the most comprehensive definition is the definition provided by (Brandl, 2010), who defines cloud computing as "collections of IT resources, (servers, databases, and applications) which are available on an on-demand basis, provided by a service company, available through the Internet, and provide resource pooling among multiple users."

Classification of cloud computing into different layers is based on the type of services provided by the cloud. At the lowest level of the service model is Infrastructure-as-a-service (IaaS). The infrastructure layer provides basic components such as Central Processing Units (CPU's), memory, and storage (Jensen, Schwenk, Gruschka and Iacono, 2009). An example of IaaS is Amazon's Elastic Compute.

Directly above the IaaS is Platform-as-a-Service (PaaS). PaaS provides developers with a platform for carrying out their functions including the provision of systems and environments for developing, testing, deploying and hosting of web applications (Rimal et al., 2009). An example of PaaS is the Google App Engine. Paas offers clients/developers hundreds of readily available tools and services (Rimal et al., 2009).

At the top of the service model is Software-as-a-Service (SaaS). SaaS provides clients with "ready to use applications" (Jensen et al., 2009) and it is an alternative to applications that are run locally in organizations (Vaquero, Rodero-Merino, Caceres, & Lindner, 2009). SaaS, involves the distribution of application software to clients (Rimal et al., 2009). An example of SaaS is the online alternatives of typical office applications (Vaquero et al, 2009. Figure 1 shows the layered architecture of cloud computing.

Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)

Figure1: Cloud Service Model.

Cloud computing enables organizations to spend money only on services that they actually receive and consume with the added flexibility of adjusting the amount of resources they need

as their circumstance varies. Organizations receiving such services do not also have to take possession of hardware and all costs associated with it (Smith, 2009). Wang, von Laszewski, Kunze and Tao (2008) reveal that cloud computing technology is synonymous with the hitherto centralized processing by stating that "cloud computing where users move out their data and applications to the remote "Cloud" and then access them in a simple and pervasive way. This is a Central processing use case. Now with the advent and popularity of the Internet, centralization of programs and data over the Internet is once again becoming popular and this paradigm is synonymous with the hitherto central processing paradigm

Chief information officers have also come under intense pressure to scale back investments in capital assets, employees, and support costs thus enhancing the possibility of cloud adoption (Brandl, 2010). Cloud systems enhances the potential of organizations to increase profitability through the reduction in investments in capital assets, IT maintenance costs, and direct labor costs (Brandl, 2010).

Organizations moving their services to the cloud have to be aware of the challenges and risks that they may face including securing sensitive information such as intellectual property, and trade secrets. Other challenges include dealing with confidentiality, Integrity, and availability issues, data loss, and system outages due to attacks from hackers and so on. Kamara and Lauter, (2010) noted that while the benefits of using a public cloud infrastructure are clear, it introduces very serious security and privacy risks. Securing critical information such as intellectual property, trade secrets, personally identifiable information and so on are issues that customers of cloud computing have to contend with. It must be noted that the threats facing cloud computing exist in other computing platforms, networks, intranets, and Internets.(Bisong & Rahman, 2011).

The importance of data security has been studied by several researchers. With cloud computing, physical location of data are spread across wide geographical area. The physical location of data becomes a top security concern for enterprises. This is more so if they are located in another country, where laws of the host country may affect the security of the data (Smith, 2009). According to Kamara and Lauter (2010), it seems that the biggest hurdle to the adoption of cloud storage is the confidentiality and integrity of data. Storing large amounts of data, including critical information, on the cloud also motivates highly skilled hackers (Srinivasamurthy & Liu, 2010). Cloud Security Alliance (2010) identifies seven major threats:

- ***Abuse and Nefarious Use of Cloud Computing Services***

Clients would risk facing grave consequences if their relative anonymity is abused.

- ***Insecure Application Program Interfaces***

. The security and availability of the public cloud services would thus be contingent upon the security of the API's.

- ***Malicious Insiders***

Many public cloud computing providers do not disclose their hiring standards and policies. There is also the lack of transparency in the way access is granted to public cloud employees that deal with physical and virtual assets.

- ***Shared Technology Issues***

Providers of public cloud computing such as the IaaS vendors provide scalable services by sharing infrastructure whose underlying components (e.g. CPU, caches, GPU, etc.) were not originally designed for offer potent isolation properties within a multi-tenant environment.

- ***Data Loss/Leakage***

There is the need to put in place measures that would prevent unauthorized persons from gaining access to data. There is also the need to protect encoding keys as any loss of encoding key could result in the destruction of critical data.

- ***Account Service and Traffic Hijacking***

Cloud computing increases the level of risk of attack. Once attackers gain access to credentials they may eavesdrop on client activities and transactions, manipulate data, return falsified information, and redirect subscribers' customers to illegitimate sites.

- ***Unknown Risk Profile***

Cloud computing allows organizations to reduce hardware and software ownership and maintenance in order to concentrate on the core business issues with a view to achieving financial and operational benefits. These security issues could result in unknown exposures that could impact organizations very negatively.

Most studies on the security concerns of cloud computing have focused on listing the threats but have stopped short of determining the potential of any of these threats to derail the future of public cloud computing (Jensen et al., 2009; Srinivasamurthy & Liu, 2010).

The existence of cloud computing and hence web services technologies has provided a fertile ground for discussions of Service-Oriented Architectures (SOA). Vouk (2008) states that "cloud computing, a relatively recent term, builds on decades of research in virtualization, distributed computing, and more recently networking, web and software services. It implies a *service oriented architecture*, reduced information technology overhead for the end-user, great flexibility, reduced total costs of ownership, on-demand services and many other things". SOA "involves the delivery of an integrated and orchestrated suite of functions to an end-user through composition of both loosely and tightly coupled functions, and services – often network-based" (Vouk, 2008). In SOA environments, end-users make requests for IT services (or an integrated collection of services) at a certain required functional, quality, and capacity levels and the service providers respond to these requests either instantly or at a specified time (Vouk, 2008).

SOA is a component-driven framework designed to support workflows, fault-tolerance in data, and an ability to audit processes, data, and results. Components of SOA include: Reusability (ability to re-use elements), substitutability (easy implementation of alternatives), extensibility and scalability, and customizability (ability to tailor generic features to suit specific and unique needs) (Crnkovic & Larsson, 2002). SOA is also designed to ensure reliability and availability of the components and address issues pertaining to security (Ludäscher et al., 2006). In line with the concepts/principles of SOA, some characteristics of cloud computing are: no upfront costs, lower operating costs, high scalability, easy access and

reduced business risks and maintenance expenses (through outsourcing of service infrastructure to the clouds), (Zhang & Zhou, 2009).

METHODOLOGY

The study uses a combination of questionnaire, survey and interviews in the data collection process. The questionnaire and scales were developed based on studies by Bisong and Rahman, (2011), Cloud Security Alliance (2010), Reese (2009), Stallings (2006), and Rittinghouse and Ransome (2009**).** The survey also adopted the 5-point Likert scale. Generalized Anxiety Disorder (GAD) used by Orsillo, Roemer, and Barlow (2003) was adopted and modified for this study. In the GAD study, four individuals were presented for treatment at the Center for Anxiety and Related Disorders (CARF) at Boston University. Participants were interviewed, and immediately before the first group session, participants completed a questionnaire packet. A post treatment survey was then formulated to enhance the reliability of the study using the 5-point Likert Scale.

Instead of four participants, we used four companies to complete questionnaires. These companies were subsequently interviewed to provide them with the opportunity to expatiate on some of the factors that influenced their decisions. In line with the anonymity clause in the questionnaire, the four companies are identified as Alpha, Beta, Gamma, and Theta. Alpha and Beta are large companies, while Gamma and Theta are small companies. Each of the respondents were given the questionnaires in Appendix A and Appendix B to be completed

RESULTS

- **Alpha**

The questionnaire, Appendix A, was completed by the Head of IT. Alpha is in the manufacturing/business with average annual revenue of hundreds of billions of dollars. Alpha's staff strength is in the millions and the company is a member of the Fortune 100 companies. Alpha currently has its services deployed on the cloud and the company is satisfied with the services it is receiving from the cloud provider. The respondent who completed the questionnaire and submitted himself for interview noted that "data security is the single greatest concern when considering moving into the cloud". The respondent gave various marks to data security concerns relating to the protection by provider of clients data integrity (5), Providers ability to protect the confidentiality of client data (5) and not knowing the location of the organization's data (5). The respondent was neutral on the issue of sharing the provider's server with other organizations (3). The mean score for data security concerns was thus 4.5. The respondent emphasized his concern for data security by ranking it first, thus sending the message that emphasis should be placed on data security concerns when considering ways to enhance patronage of public cloud computing.

In respect of preventive and contingency planning, none of the questions posed received the maximum score of 5.The most important issue to the respondent was the provider's turn-around

time which received a score of 4. He was not particularly concerned with the provider's ability to deal with system outages (3). The mean score was 2.75. This section was ranked 4th by the respondent emphasizing its relative unimportance.

In respect of network security, the main concern was the provider's ability to enforce encryption, authentication, and the use of firewalls (5). This was followed by the ability of the provider to deal with packet sniffing (4). Ability of provider to deal with malicious attacks such as viruses and worms and denial-of-service received scores of 3 and 2 respectively indicating their relative limited importance. The mean score was 3.5. This section was ranked third.

The general security concerns subsection was the second most important concern to the respondent. The provider's physical security of the computer system as well as the risk of government intervention received the maximum score of 5 showing the level of importance attached to them. The respondent was neutral when it came to the remaining items in this subsection: risk of provider going out of business, activities of malicious insiders, and protection of organization's trade secrets as each received a score of 3. The mean score was 3.8.

In terms of measures to be employed to enhance patronage of cloud computing, Appendix B, the respondent was of the opinion that primary attention needs to be given to the following: Service level agreements between provider and client companies, effective measures to deal with encryption, authentication, and firewalls, and regular audits particularly of provider's data security (5 each). The respondent also felt the following were relatively important (with a score of 4 each): Regular audits of provider's general security, guarantee that governments would not interfere with client data, and satisfaction with provider's security architecture. Satisfaction with provider's preventive and contingency plans, regular audits of network security, and satisfaction of provider's hiring criteria each received a score of 3 showing the indifference of the respondent to such issues. Segregation of data from other companies was not considered important. Table 1 provides a summary of the average scores for all the companies including an overall summary.

- **Beta**

The survey was completed by the head of IT. Company Beta is a direct marketing company in the United States with average annual revenue in billions of dollars. The staff strength of this company is about 2,300. The respondent was of the opinion that every provider should have in- built redundancies in order to qualify to be a public cloud provider. The company currently utilizes the services of a reputable cloud provider. The respondent ranked data security, network security, and general security concerns equally; the three therefore tied at first place. Disaster recovery security concerns were relatively unimportant to the respondent as it placed fourth. Under data security concerns, the respondent indicated his major concern for the ability of provider to protect the integrity and confidentiality of data high (4). The location of data and the sharing of data with other organizations on the same server were not important to the respondent as they received very low scores of 2 and 1 respectively. The mean score for this subsection was 2.75.

In respect of preventive and contingency planning, the author's main concern is the turn-around time (4). Provider's ability to deal with system outages received a neutral score (3). The efficacy of provider's preventive and contingency plans was viewed by respondent as relatively unimportant. The mean score was 2.25.

The respondent's main concern under network and security is the efficacy of provider's encryption, authentication, and firewall techniques with a mark of 4. The other issues under this section: ability of provider to deal with: packet sniffing, denial-of-service attacks, and malicious software such as virus and worms were less important as they each received a score of 3. The mean score was 3.25.

In respect of general security concerns, malicious attacks from provider's employees and the protection of organizations trade secrets were the primary concerns. The risk of government intervention was given a neutral rating while provider's physical security and providing going concern status were unimportant. The mean and score were 2.6 and 3.0 respectively.

In terms of measures to enhance utilization and patronage of public cloud computing: service level agreements between provider and client, effective security measures such as encryption, authentication, and firewalls, regular audit of provider's network security, and regular audits of provider's general security each reach the maximum mark of 5. Regular audits of provider's data security by reputable audit company, regular audit of provider's preventive and contingency plans, satisfaction with provider's security architecture, and satisfaction with provider's hiring criteria each received high mark of 4 indicating their relative importance. Respondent is not particular about provider's preventive and contingency plan and government's interference client data. Sharing of server with other organizations, to the respondent is a non-issue.

- **Gamma**

Gamma is a small IT company with an average annual income of about 200,000 dollars. The company has six employees' and currently does not utilize the services of any cloud provider. The company is involved in web development, hardware repairs, and provides consulting services for organizations. The respondent for this survey and interview was one of the two partners of the company.

The company's primary concern regarding public cloud computing is data security. Consequently, provider's ability to protect the integrity, confidentiality, and location of data each received very high marks of 5. Sharing of provider's server with other organizations is also of concern to this company. The mean score was 4.75.

In respect of preventive and contingency planning, the respondent was concerned about the provider's turn-around time and ability to quickly deal with system outages with each receiving a score of 5. The respondent also rated the efficacy of the provider's preventive and contingency plan high with a score of 4. Mean scores was 4.5.

In respect of network and security concerns, the respondent's primary concern is the ability of

provider to implement effective encryption, authentication, and firewall techniques, as each received a maximum score of 5. The other network concerns: ability to deal with: packet sniffing, denial-of-service attacks and viruses and worms were also rated high with a score of 4 each. Mean score was 4.25.

In respect of general security concerns, the respondents' main concerns are; the provider's physical security, malicious activities of provider's employees, and security of organizations trade secrets (each received a score of 4). The respondent was not too concerned about government interference with client data and was felt the risk of client going bankrupt was not an issue. The average score for this section was 4.25. In terms of ranking, data security and network concerns were judged by the respondent as the most important as they tied at first place. General security and disaster recovery concerns were the judged to be of equal importance after data security and network security concerns.

The respondent was of the opinion that the following measures are of equal importance in enhancing patronage of public cloud computing: Service level agreements between provider and clients, effective encryption, authentication, and firewall techniques, satisfaction with provider's preventive and contingency plan, regular audits of provider's data security by reputable audit company, regular audits of provider's network security, regular audits of provider's general security, and satisfaction with provider's security architecture. The respondent was not particular about interference of data by governments and segregation of organization's data from other companies. Provider considered satisfaction with provider's hiring criteria unimportant.

- **Theta**

Theta is a small company involved in web and graphic design. The company's average annual income is about $130,000 (U.S.) and there are only two employees. The company currently implements public cloud computing. The survey was completed by the owner of the business. The respondent's primary concern was data security which he demonstrated in the ranking of the security concerns. In respect of data security concerns, the respondent displayed concern for the ability of the cloud provider to protect the integrity and confidentiality of data by giving those two questions the maximum mark of 5. Sharing of provider's server with another organization was also a major concern but played second fiddle to security over confidentiality and integrity as it was awarded a score of 4. The respondent was not particularly worried about the location of data and thus gave this a score of 2. The mean score was 4.0. In respect of concerns over preventive and contingency planning, the respondent expressed his affinity for data protection and quick recovery procedures by awarding all the questions under this category the maximum score of 5. The mean score was thus 5.0.

In respect of network and security concerns, the respondent gave maximum marks to concerns pertaining to distributed denial of service attacks and the provider's ability to deal malicious attacks from viruses and worms. Concerns over encryption, authentication, and firewall received a score of 4 while the provider's ability to handle packet sniffing received a score of 3. The mean score for this category was 4.25.

In respect of general security concerns, the respondent's primary concern was the provider's ability to deal with physical security issues pertaining to the information technology infrastructure and the organization's trade secrets as they both received the maximum score of 5. Concern over the malicious activities of insiders, provider going out of business, and risk of government intervention all received a moderate score of 3 each. The mean score for this category was 3.8. In terms of ranking, the author ranked the concern in decreasing order of importance as follows: data security concern, disaster recovery, general security and lastly network security.

In the opinion of the respondent, the two most important measures to boost the confidence of potential public cloud users is to have effective service level agreements between cloud provider and the client and also guarantee by cloud provider that there will be no government interference with client's data. The rest of the items under this category all received a score of 4. Tables 1, 2, 3 and 4 show the mean scores for the companies and the rankings of security concerns by the companies.

DISCUSSION

The objective of this study as noted earlier is to ascertain the impact of data security concerns on the future of public cloud computing and in particular determine whether the data security concerns have the potential of derailing the future of public cloud computing. The overall results of the four companies (2 large and 2 small) as shown in Table 1 reveal that indeed data security is a critical consideration when organizations make decisions regarding whether or not to adopt public cloud computing.

Company	Data Security	Preventive and Contingency Planning	Network Security	General Security
	Mean	Mean	Mean	Mean
Alpha	4.5	2.75	3.5	3.8
Beta	2.75	2.25	3.25	2.6
Gamma	4.75	4.5	4.25	4.25
Theta	4.0	5.0	4.25	3.8
Overall	4.0	3.69	3.81	3.4

Table 1: Mean Score for the Four Companies.

The overall mean score was the highest from the analysis, 4.0. This revelation is very important as it could help client providers position themselves strategically to continue to exist as a going concern by devising measures to attract clients. Company alpha a multibillion dollar and fortune 100 company with thousands of employees and stores spread throughout the United States was exceedingly particular about data security and this was made very clear during the interview. When the respondent was asked during the interview about his primary concern with public cloud computing, he remarked "Data security is the single greatest concern when moving into the cloud". A large company will hedge its bets using other clouds

or internal systems." To the same question, company theta, a small company with average annual income of about $200,000 (U.S.) remarked "Data security is our primary concern. We currently have an agreement with PayPal to receive payments from clients on our behalf because of security. We would not want the sensitive information of our clients to be captured and used fraudulently by anyone. We are not using public cloud computing because of our concern for data security and we do not consider using these services in the near future. We would have to be confident that our data can be protected before we would go cloud". In terms of ranking, data security concerns came out tops as all companies ranked it as number 1, although in some cases data security concerned tied with other concerns. It is important to note that network security was also a very important concern as its overall scores came second with a mean score of 3.8. Preventive and contingency planning concerns and general security concerns followed in that order as shown in Tables 2 and 3.

Company	Data Security	Preventive and Contingency	Network Security	General Security
Alpha	1	4	3	2
Beta	1	4	1	1
Gamma	1	3	1	3
Theta	1	2	4	3
Position	First	Fourth	Second	Third

Table 2: Rankings of Security Concerns by Companies.

Company	Data Security	Preventive and Contingency Planning	Network Security	General Security
	Mean	Mean	Mean	Mean
Alpha	4.5	2.75	3.5	3.8
Beta	2.75	2.25	3.25	2.6
Combined	3.6	2.5	3.4	3.2

Table 3: Mean Score for Large Companies.

The overall results was not entirely consistent with the ranking as general security and contingency planning changed places in the rankings with general security being ranked third and preventive and contingency planning fourth. A breakdown of the overall results into large and small companies revealed something very interesting: while large companies place very little emphasis on preventive and contingency planning concerns small companies place much emphasis (Table 4).

Company	Data Security	Preventive and Contingency Planning	Network Security	General Security
	Mean	Mean	Mean	Mean
Gamma	4.75	4.5	4.25	4.25
Theta	4.0	5.0	4.25	3.8
Combined	4.4	4.75	4.3	3.6

Table 4: Mean Score for Small Companies.

This culminated in the discrepancy between the overall results and rankings with regards to the preventive and contingency planning and General Security concerns. A review of the interview conducted with the respondent of one of the large companies, Beta revealed preference for general security compared to preventive and contingency planning as he argued that his choice of cloud provider depends heavily on the provider's "in-built redundancies, in the sense that the provider should have the ability to deal with issues pertaining to outages and so on". This requirement makes preventive and disaster planning of little importance to him as he would have addressed this concern prior to selecting the provider. On the other hand, the respondent for company gamma, a small company, noted that without the assurance and trust that the cloud provider can deal with disasters in-time for work to resume he would not consider going cloud. The other small company, theta amply demonstrated his concern for preventive and contingency planning by giving all the questions under this section a score of 5 and ranking preventive and contingency planning, second to data security concerns.

A look at Table 3, Table 4 and Table 5 reveal another interesting phenomenon. While Alpha ranked general security ahead of network security, Beta did the exact opposite. Alpha's concern for government intervention and physical security may have influenced this ranking. For small companies, while from the summary company Table 4, network security was rated more important compared to general security, mixed results were experienced in the ranking; company gamma indicated that attention be placed on network security while company theta indicated that attention be given to general security (Table 5).

Company	Data Security	Preventive and Contingency	Network Security	General Security
Alpha	Integrity, Confidentiality, & Location		Encryption, Authentication, & Firewall	Physical Security, & Government Intervention
Beta				
Gamma	Integrity, Confidentiality, & Location	Turn-Around Time, & System Outages	Encryption, Authentication, & Firewall	
Theta	Integrity & Confidentiality	Preventive & Contingency, Turn- Around Time & System Outages	Distributed Denial of Service, & Worms/Viruses	Physical Security & Trade Secrets

Table 5: Key Individual Items (5 score).

This therefore makes the results inconclusive and necessitates further studies with much more data for purposes of generalization.

A critical look at the key individual concerns (Table 5) revealed that the two most important issues facing user's of public cloud computing are the Integrity, and Confidentiality of data. Also of concern is the ability of provider to encrypt, authenticate, provide firewalls and provide physical security. The emphasis on the integrity and confidentiality of data amply demonstrates the importance of data security concerns and makes the issue a prime consideration in public companies based on size. While large companies place very little emphasis on preventive and contingency planning, small companies pay much attention to it. It is very informative to note that company theta currently using the services of a cloud provider rated all the measures very high (4 and 5) indicating the importance of all the measures. This clearly means that providers would have to find ways of dealing with the measures raised in a bid to enhance patronage as it stresses the importance of all the other factors including but not limited to: dealing with government intervention, segregation of data, and hiring criteria. What this also means is that future work is required to identify the most important measures and segment them according to companies and types of business segment to enable focus on certain segments based on their core competencies. It is also significant to note that both large and small companies are concerned about malicious activities of provider's employees and protection of clients' trade secrets.

To boost the confidence of existing clients and to attract potential customers it is important that the measures unanimously agreed upon by the companies be taken into serious consideration. The four companies as shown in Table 6 agreed to the following measures: the implementation of service level agreements between public cloud providers and clients, that the provider should have effective encryption, authentication, and firewall mechanisms, there should be regular audits of provider's data security, network security, and general security by reputable companies.

Name of Company	Key Determinants
Alpha	Service level agreements; Encryption, authentication, and firewall; Regular audit of provider's data security by reputable audit company
Beta	Service level agreements; Encryption, authentication, and firewall; Regular audit of provider's network security and general security
Gamma	
Theta	Service level agreements; Absence of government interference

Table 6: Critical Mitigating Factors for Large and Small Companies (5 score).

While these are the overall concerns, it is important state that emphasis seems to be slightly different between the two sets of companies. While all the measures received very high marks for company theta, company gamma did not attach much importance to government intervention (3), segregation of data (3) and provider's hiring criteria (2). For large companies, the following did not appear very important; client providers preventive and contingency plans, and segregation of data.

CONCLUSION

The results of the study reveal that data security concern is the single most important concern when moving into the cloud. Key measures that providers could adopt to boost the confidence of current and potential clients are to enter into enforceable service level agreements with clients and allow for the regular audits of data and network security by reputable audit companies.

The significant impact of data security concerns has serious implications to providers and clients of public cloud computing. Providers must put in place measures to boost the confidence of to regular audits. The audits should be performed by reputable audit companies. Providers need to find ways of dealing with network security concerns as these concerns unanimously ranked second to data security concerns and was considered very important by all companies irrespective of size. In addition, providers of public cloud computing would by default have very effective in-built redundancies to deal with unforeseen eventualities. Small companies articulated the importance of preventive and contingency planning by rating it even higher than network.

The use of a large sample size would have enhanced the quality of work and increased the reliability and validity of the study. This limitation severely impacted the ability to generalize the results of the study. The use of two large and two small companies made it difficult to resolve any discrepancies between these categories and to make a definitive statement as there were only two companies in each category. It may be important to replicate this study but with a large sample size. The results of the study reveal that data security concern is the single greatest concern when moving into the cloud. It also reveals that an important means for public cloud providers to boost the confidence of current and potential clients is to enter into enforceable service level agreements with clients.

The study has significant implications to researchers as it provides a fertile ground for further studies to be conducted. Researchers should conduct further studies into the measures necessary to enhance patronage by identifying additional measures and segregating these measures into various industries and business types. Such studies will enable providers identify which segments of the market to compete in.

REFERENCES

Bisong, A., & Rahman, S. M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA), 3*(1), 30-45.

Brandl, D. (2010). Don't cloud your compliance data. *Control Engineering,* 57(1), 23.

Cloud Security Alliance. (2010). *Top threats to cloud computing: Survey results update 2012*. Retrieved from https://cloudsecurityalliance.org/research/top-threats/

Crnkovic, I., & Larsson, M. (Eds.) (2002), *Building reliable component-based software systems.* Norwood, MA: Artech House Publishers.

Jensen, M., Schwenk, J. O., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. In *IEEE International Conference on Cloud Computing, 2009*, 109-116.

Kamara, S., & Lauter, K. (2010), Cryptographic cloud storage. *Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization.* Retrieved from http://research.microsoft.com/pubs/112576/crypto-cloud.pdf

Ludäscher, B., Altintas, I. , Berkley, C., Higgins, D., Jaeger, E, Jones, M., . . . & Zhao, Y. (2006). Scientific workflow management and the Kepler system: Research articles. *Concurrency and Computation: Practice & Experience, 18*(10), 1039-1065. doi: 10.1002/cpe.v18:10

Orsillo, S. M., Roemer, L., & Barlow, D. H., (2003), Integrating acceptance and mindfulness into existing cognitive-behavioral treatment for GAD: A case study. *Cognitive and Behavioral Practice, 10*, 222-230. doi: 10.1016/S1077-7229(03)80034-2

Reese, G. (2009), *Cloud application architectures: Building applications and infrastructure in the cloud: Theory in practice*. Sebastopol, CA: O'Reilly Media.

Rimal, B. P., Choi, E., & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. *Fifth International Joint Conference on INC, IMS and IDC*, 44-51.

Rittinghouse, J. W., & Ransome, J., F. (2009), *Cloud computing implementation, management, and security*. Boca Raton, FL: CRC. Press

Smith, R. (2009). Computing in the cloud. *Research Technology Management*, 52(5), pp.65-68.

Srinivasamurthy, S., & Liu, D. Q., (2010). *Survey on cloud computing security.* Retrieved from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_67.pdf

Stallings, W., (2006), *Network security essentials: Applications and standards* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Vaquero, Luis., M, Rodero-Merino, L., Caceres, J., & Lindner, M. (2009), A break in the clouds: Towards a cloud definition, *ACM SIGCOMM Computer Communication Review, 39*, 50-55.

Vouk, M. A. (2008), Cloud computing: Issues, research and implementations. *Journal of Computing and Information Technology, 16*(4), 235-246.

Wang, L., von Laszewski, G., Kunze, M., & Tao, J. (2008), Cloud computing: A perspective study. *Proceedings of the Grid Computing Environments (GCE),* 1-11

Yang, J., & Chen, Z. (2010). Cloud computing research and security issues. *International Computational Intelligence and Software Engineering (CISE),* 1-3.

Zhang, L., & Zhou, Q. (2009). CCOA: Cloud computing open architecture, *IEEE International Conference on Web Services, 2009,* 607-616.

Appendix A

CONCERNS

The following set of questions deals with security concerns pertaining to public cloud computing. For each question, ***please circle the number*** *that best indicates the extent to which you agree to the statement on a scale from 1 to 5 (see below).*

Strongly Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Strongly Agree
1	2	3	4	5

	Strongly Disagree				Strongly Agree
1. Data Security Concerns					
a) Provider's ability to protect the integrity of my organization's data is of concern to me	1	2	3	4	5
b) Provider's ability to protect the confidentiality of my organization's data is of concern to me	1	2	3	4	5
c) Sharing of provider's server with other organization's is of concern to me	1	2	3	4	5
d) Not knowing the location of my organization's data is of concern to me	1	2	3	4	5
2. Prevention and Contingency Planning Concerns					
a) I am concerned about efficacy of provider's preventive plans	1	2	3	4	5
b) I am concerned about efficacy of provider's contingency plans	1	2	3	4	5
c) I am concerned about provider's system turn-around time	1	2	3	4	5
3. Network Security Concerns					
a) Ability of provider to handle packet sniffing is of concern to me	1	2	3	4	5
b) The risk of high distributed denial of service attacks is a concern	1	2	3	4	5
c) Encryption, authentication, and firewall issues are of concern to me	1	2	3	4	5

	Strongly Disagree				Strongly Agree
4. General Security Concerns					
a) Provider's physical security of computer systems is of concern to me	1	2	3	4	5
b) The risk of provider going bankrupt is of concern to me	1	2	3	4	5
c) The risk of government intervention in the country where data is stored is of concern to me	1	2	3	4	5

The next question asks you to rank in order where you think the emphasis should be placed in dealing with the above-listed concerns. You are asked to rank the concerns pertaining to data security, disaster recovery, network security, and general security. Please mark with an **X** your first, second, and third choices.

5. Prioritizing Concerns	**First Choice**	**Second Choice**	**Third Choice**
Data Security			
Preventive and Contingency Plan			
Network Security			
General Security			

Appendix B

MEASURES TO ADDRESS CONCERNS

Now, we are interested in your view on measures that would mitigate the concerns pertaining to the use of public cloud computing.

For each of the following statements, indicate your perception of the level of importance from **Low Importance** (1) to **High Importance** (5).

Measures to Address Concern	Low Importance				High Importance
a) Contract between provider and client regarding data protection	1	2	3	4	
b) Effective security measures, such as encryption, authentication, and firewalls	1	2	3	4	5
c) Satisfaction of client with provider's prevention plans	1	2	3	4	5
d) Satisfaction of client with provider's contingency plans	1	2	3	4	5
e) Regular audits of provider's data security by reputable audit company	1	2	3	4	5
f) Regular audits of provider's contingency plans by reputable audit company	1		3	4	5
g) Regular audit of provider's network security	1	2	3	4	5
h) Regular audits of provider's general security	1	2	3	4	5
i) Guarantee of no government interference with client's data	1	2	3	4	5