“Who is Guarding the cloud?”

TABLE OF CONTENTS

Declaration

I declare that, except where indicated through the proper use of citations and references, this is my own original work. It is submitted as a partial fulfilment of the requirements for the award of: BSc (Hons) Business Information Systems at the University of Portsmouth.

It has not been accepted or submitted for any academic purpose by any student in any University.

…………………………………………………………………..
Sign

……………………………………………………………………..
Date

Abstract

The purpose of this paper is to provide Small and Medium-size Enterprises (SMEs) an understanding of the cloud computing and cloud security control responsibilities. The study conducted a primary research consisting of interviews and questionnaires which examined the perception of SMEs on who is responsible for cloud computing security control. It was found that cloud computing currently has no security standard that clearly describes ownership of cloud control environment. This therefore, created a scenario where neither the cloud providers nor cloud users agreed to own the security responsibility of the cloud environment. Recommendation made was that in the absence of cloud security standard, SMEs should audit the credibility of cloud computing in the areas of available security policies before deciding on what cloud services or cloud provider to use.

Acknowledgment

I would like to thank my supervisor, Mrs. Penny Hart for her understanding and professional academic support that has made this project possible. I would not have being able to do this without her.

Most importantly, to get to this stage of my academic career would not have been possible unless without love, moral, spiritual and financial support from my family.

Particularly my sincere gratitude to my uncle Mr. Inuwa Iyodo and his wife Mrs Rahmat Iyodo for their parental love, care and support as a child to this stage of my life. And I owe sincere and earnest thankfulness to my brothers from another parent Ismail Iyodo and Mohammed Iyodo for their brotherly support, sincere advice both in sickness and good times. Furthermore, I would not stop without thanking my lovely sister Zainab Ismail Iyodo and my two little angels Fauzier and Firduasi.

I would also like to thank my Mother Amina Audu who has suffered for me to be alive to see this day and to my beloved wife Hadiza Ahmad Audu as well as our little lovely daughter Muhsina Audu.

1.0 CHAPTER ONE: INTRODUCTION

This project is about 'cloud computing' security, privacy and trust. The study looks at the role and responsibilities of SMEs as well as cloud providers regarding cloud security control. Concept of cloud computing is not new. The advancement in networking and sophisticated database technology can be seen as the major factor that inspired the concept of cloud computing.

The concept of cloud computing in a simple term is another model of outsourcing data centre to a third party on a pay-as-you-use scheme.

The internet in recent years have witnessed a remarkable development from the well known communication tool (e.g. email) and content management system (e.g. web) to a deployable virtual development platform, virtual application, and virtual infrastructure where managed computing capabilities and data storage are made available as utilities. In the last four years, cloud computing have received a large number of publicity from different computing background. Google, Amazon, Microsoft, IBM are some of the big industries who are presently utilizing the possibilities of the new business model that is backed by the technology.

The promises backed by the technology are drawing a great attention of large, medium and small companies. The ability of the technology to release businesses from the burden of acquiring and maintaining IT infrastructure at a higher price i.e. running the traditional data centre, gives Small and Medium-size Enterprise (SME) the opportunity to enter into the industry with almost a no capital budget. A report in mid 2011 by redshift (2011) suggests that some businesses were already using cloud computing and some were still investigating. The same report also shows that a reasonable number of the companies in USA, EU and ASIA being studied belong to the Small and Medium Size Companies. The study also revealed how beneficial the technology is to those companies. Similarly, PC world in 2010 indicates that they have saved $4000 in up 'front costs' by moving some of their business processes which includes e-mail, web hosting, virus protection and even more similar services to an entirely web based solution (Martin, 2010).

While some professionals still perceive the technology as immature therefore possesses lots of security threats, businesses are embracing it and the adoption rate keeps rising. Data transactions over the internet generally is characterised by data security and privacy concerns. Cloud computing however is believed to characterised with even more concerns.

The cloud security concerns became more visible when Amazon's Elastic Compute Cloud service in April 2011 experienced outages which caused sites like Foursquare, Reddit and Quora to go offline for some days (BBC Business News, 2011). Similarly SONY's online gaming services, Playstation Network and other similar services experienced a security breach in April 2011 where information of over 100 million customers was compromised in what was described as a 'Massive Cyber attack' (BBC Business News, 2011). Such security breaches and service outages may be easily restored by larger companies like SONY who was able to identify and fixed the problem, utilizing the readily available resources at its disposal. Small businesses therefore shoulders bigger concerns over the security issues as they may not have readily available resources to combat such failures.

1.1 Problem statement

The current trend in security, privacy and reliability issues concerning cloud computing technology did sparks fears and discussions in almost every published work on the technology, knowing that larger companies have the financial and technical capacity to handle the impact of any outage or security breach. The actual fear lies on SMEs with lower financial and technical knowhow to handle issues of outages and security breach. The research attempts to answer the following questions

- What is cloud computing?
- Is cloud computing security a concern for SMEs?
- Is cloud security control the sole responsibilities of SMEs?

The above questions are taken for the reasons that some of the background studies and previous surveys suggests some SMEs are either not aware about the challenging security issues as not being important in cloud computing environment. The awareness of SMEs who are either planning on using the cloud or already using would be increased or improved by the outcome of this research. The answers to the above questions would also help SMEs to understand their responsibilities in cloud security control environment as against the provider.

Better understanding of the technology however may as well ignite reasonable thoughts about risks accompanying third party hosted transactions where self control is almost not possible. The second questions assesses the level of understanding of Enterprise of what cyber security is as it is observed that most businesses mainly conceder's data breaches as the only security worries not knowing that there are more challenges in cloud computing than just data breaches.

Understanding the responsibilities of cloud providers and the cloud users is important as to which of the actor is liable for which security controls at which particular period In time, these therefore enables users to make security strategic plan and make better decisions when deciding the type of cloud service in regard to making service agreement with cloud providers.

The project findings are expected to demonstrate that despite the promises of cloud computing and the level of up-take, there are still concerns hovering over its reputation. The project would also demonstrate the level of what businesses understands or do not understand about their security responsibilities in the cloud environment.

1.2. **Method of study**

This research uses existing published article, journals, online resources as well as books for background study and fact finding on existing current practices in the cloud computing field. A number of semi-structured face-to-face interviews with CIO and CEOs were conducted. The use of online questionnaires was also employed for information gathering.

1.3**. Scope of the Project**

The project studies security and privacy issues in the cloud environment from the perspective of SMEs and cloud service providers in regard to the responsibilities of both parties**.** It is aimed at key decisions makers and staffs with good IT knowledge background in organisations. The nature and the key elements of cloud computing has been discussed so to enable the reader understand the concepts of the technology. Cloud security threat were also identified and discussed to broaden the study about what security and privacy is in the cloud computing environment and shed more light on the position of information technology professionals.

1.4**. Delimitation**

The study limits its focus on Small and Medium size enterprise (SMEs). It has no intention whatsoever to portray the work identified in the project as standard or specific way of managing cloud security. Similarly, the research is not design with a specific country or region in mind; therefore it is not intended for any particular country or region. The study is not meant to be a blueprint for SMEs considering or planning to adopt cloud computing for their organisations.

2.0 CHAPTER TWO: LITERATURE REVIEW

This Chapter explores and present an overview of work previously carried out on related topics. The section provides the relevant background study of the topic for the purpose of the project. It will discuss the fundamentals of the technology in regards to the research questions. The section provides the definitions of cloud computing, technical elements that create the enabling environment on which the technology exists, the technology rationale and security risks.

2.1 The General concept of cloud Computing

The term cloud computing according to Zisses et al (2010) was inspired by the cloud symbol used to represent the internet in the popular 'flow chart diagram'. Apart from the cloud symbol, the technology is characterized by essential building block which includes on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (Mell and Grance, 2011).

Though the definition of cloud computing varies, Armbrust et al (2010) defined cloud computing as 'both applications delivered over the internet and the hardware and systems software in the data centre that provides those services'. This definition in relation to the characteristics of cloud computing identified by Mell and Gance does lack some of the main purpose of the technology which includes 'measured services' and on-demand self services. The technology enables users to pay for only the amount of computing resources they require and scale up or down if they want. For the purpose of this study, we adopt the definition from the US's National Institute for Standard and Technology (NIST), for the reason that, it attempts to holistically incorporate the characteristics of the technology in the definition. NIST described cloud computing as a 'model for enabling convenient, on-demand network access to a shared pool of configurable computing resources' for example (networks, servers, storage, applications and services (Mell and Gance, 2011).

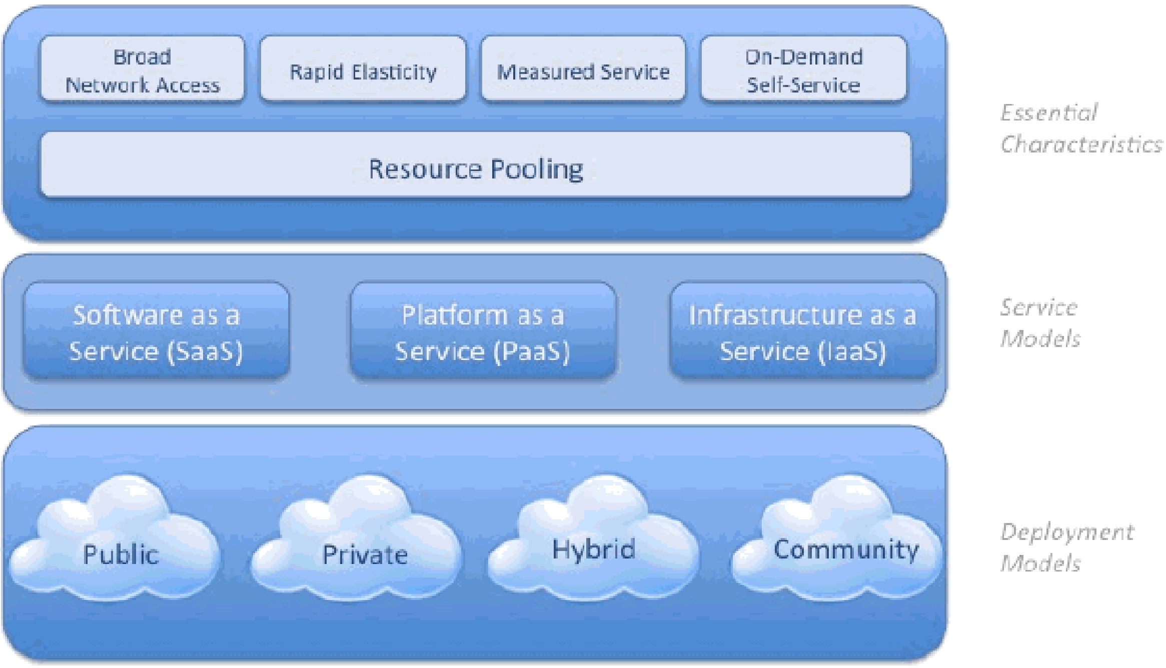


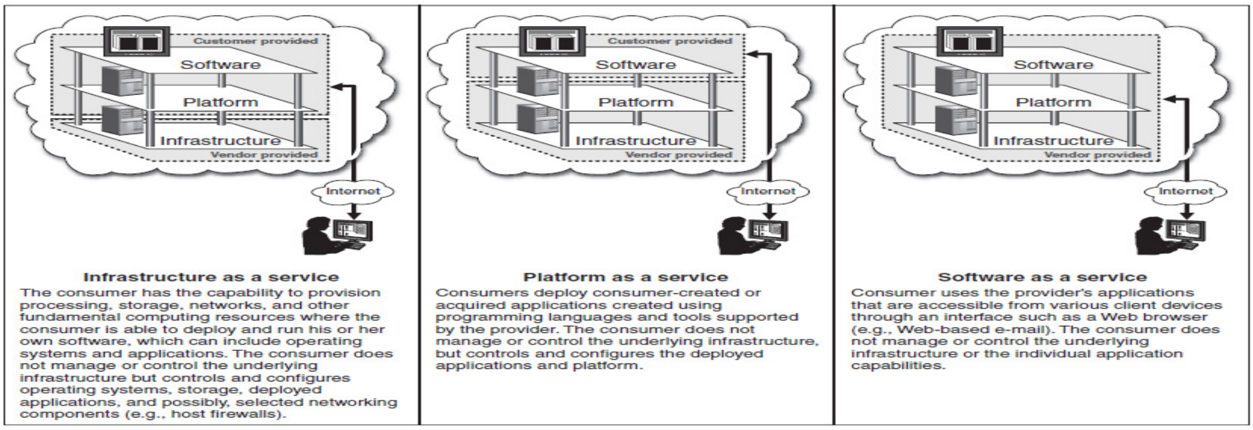
Figure 1: NIST Visual Model of Cloud Computing Definitions

(CSA, 2009)

Cloud computing as shown in the figure 1 is characterized with three basic service models and four basic deployment models; the models forms the bases on which computing resources are delivered to users via the network on pay as you use bases.

2.1.1 Cloud computing service delivery model

(McAfee, 2011) indentified three major cloud computing service delivery model, which are Software-as-a-Service (SaaS), Platform-as-a-Service and Infrastructure-as-a-Service



Infrastructure as a service
The consumer has the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run his or her own software, which can include operating systems and applications. The consumer does not manage or control the underlying infrastructure but controls and configures operating systems, storage, deployed applications, and possibly, selected networking components (e.g., host firewalls).

Platform as a service
Consumers deploy consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying infrastructure, but controls and configures the deployed applications and platform.

Software as a service
Consumer uses the provider's applications that are accessible from various client devices through an interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying infrastructure or the individual application capabilities.

Figure 2: Cloud computing service delivery model (GAO, 2011)

2.1.1.1. *Software as a Service (SaaS)*

SaaS is the most matured and largest service model among the three (McAfee, 2011). It is an application or suits of applications that are delivered over the cloud. In cloud computing, software applications reside in the cloud instead of the user's computer. Salseforce.com's customer relationship management (CRM) software is one of the SaaS successes (McAfee, 2011).

2.1.1.2. *Platform as a Service (PaaS)*

Virtualized run time platform for developing applications or application services delivered on on-demand bases. IaaS is hosted and managed by cloud service vendors. The model provides readily available tools for professionals to build applications such as database systems, business intelligence applications like dashboard, web applications and host of more (OpenCrowd, 2011).

2.1.1.3. *Infrastructure as a Service (IaaS)*

Provides processing, storage, networks and host of other fundamental computing resources to consumers where they are able to deploy and run software which can include both application and system software (Mell, 2011).

2.1.2 **Cloud Deployment Models**

Regardless of the cloud delivery model in adopted, SaaS, PaaS or IaaS, there are four major ways in which they are deployed. CSA (2009) identified Private cloud, public cloud, community cloud and Hybrid cloud as the four major cloud deployment models, see figure 1.

Private cloud is solely owned by a single organization comprising multiple users which could be the organization's business units sharing the resources. Private cloud may exist on or off-site and may be owned, operated and managed by the organisation, third party or both (NIST, 2011).

Public Cloud are owned, managed and operated by designated service provider can offer dedicated single-tenant or multi-tenant shared computing resources with all the characteristics and benefits of cloud computing. Public cloud is usually at the premises of the cloud service provider and by definition it is off-premises to the consuming organisation.

Community Cloud, NIST (2011) compared community cloud deployment model with private cloud, stating that the difference is that the ‘infrastructure and computational resources are exclusive to two or more organization that have common privacy, security, and regulation considerations.

Hybrid Cloud is combination of two or more other clouds and it is thought to be more complex due to the fact that it combines public and private or community cloud (NIST, 2011). Each member of these combined cloud remain unique entity unless they are bound through standardization.

2.1.3 **Virtualization**

Virtualization, according to (Technology Review, 2009) dates back to the late sixties, 1967 specifically and was only available on mainframe but when data centres and the Internet became common, it existence begin to gain some popularity. (McDonald, 2010) described virtualization as an approach to server handling as a technique which enables the cloud service providers to share one physical server amongst bigger number of users. With this approach, in public cloud environment, users will have the feelings that they own rented physical server not knowing that, the physical server is being shared with other customers.

Virtualization allows cloud customers to only obtain the bits of server space they require and can scale up and down depending on their needs. Studies shows that in an average data centre, 10 to 25% out of their physical server processing power are used, while the rest remain unused and such inspired the scalability nature of the cloud (McDonald, 2010). In addition Harvard Business Review (2010) discussed that the benefits of using the cloud’s virtualization approach is undoubtedly understood as businesses needn't have to consume above what they require however.

2.1.4 **Hypervisor**

Software needed to run copies of the virtual machines in order to make sure same resources are not used simultaneously (McDonald, 2010). Hypervisor is needed on every host physical machine to create, delete and manage virtual machines delivered to users (Technology Review, 2009). The technology enables cloud service providers to create more than one virtual machine (virtualization) on one single physical machine when they are required and can easily be deleted when not needed.

2.2. **The Social aspect of cloud computing**

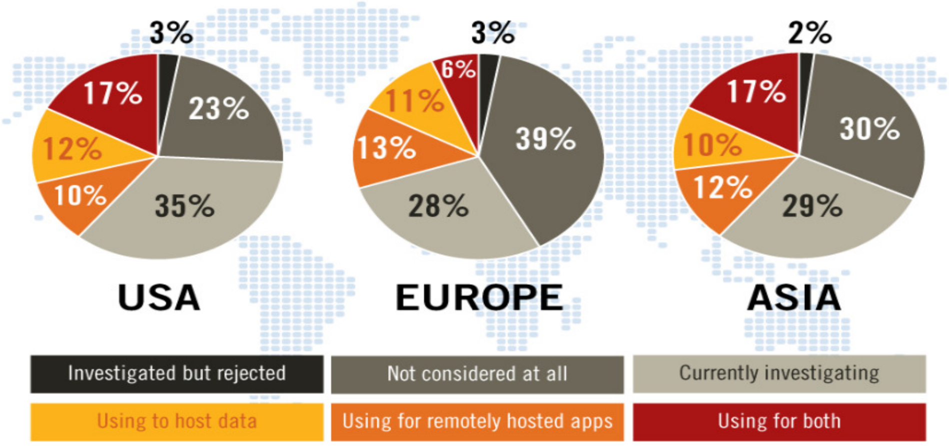
2.2.1 **Driver for the take-up of cloud computing**

A survey carried out by ENISA (2009), a European Union agency; found that 68% of the SME that responded to the survey indicates that avoiding capital expenditure in hardware, software, IT support and information security is behind their possible   engagement in cloud computing while 64% of the responses also indicated flexibility and scalability of IT resources as their reasons. Similarly, KPMG (2010) in a study revealed that the technology is driven by cost savings and more flexibility. Similarly AWS also believed that cost saving, flexibility and instant elasticity of computing platforms (Amazon Web Services, 2012) are some of the top reasons identified to be the rationale for take-up of the technology. Amazon did support this claim with the identification of the University of Melbourne, University of Barcelona, Washington Post, Harvard Medical School and a lot more utilising the high performance nature of the technology compared to the in-house data centre.

Similarly, in other surveys, one-third of 3,645 companies that answered a survey carried out by TNS, a market research company cited that the need to better connect their employees who use large number of computing devices as their Number one aim of adopting cloud computing (InfoWorld, 2011). These perceptions of users about the reasons for cloud take-up have demonstrated the different use or purpose of the technology to different organisations. The reasons depend hugely on the organisational IT needs but generally, it is perceived that cost cutting is a main reason.

The technology however have hidden charges that is accrued overtime in such that at first, it will be less expensive but may cost over time, as data charges begin to accrued when customer starting to demand for more service power (Havard Business Review, 2010). However Harvard Business Review, 2011) claimed that the findings about cost is conflicting as a Mckinsey case study in 2009 revealed that putting entire data centre into the cloud would increase cost by 144%.

Cloud computing at this time have seen different region's adoption rate at a different stage with different attitudes towards the technology take-up, some of the business that participated in a research (redshift, 2011) provided different opinion on the taking-up or not taking-up of the technology. In Late 2011, a large number of businesses in the United State are investigating the technology before taking up compared to the large number of the EUROPEAN businesses which have not at this stage considered it at all.



Organisation's Positions in relation to cloud adoption

(redshift, 2011)

Towards the end of 2011, the technology experienced 37% take-up rate globally to remotely host application or host data and even both (redshif, 2011).

2.2.2 Commercial Implementations of cloud computing Services

There are numbers of cloud providers who have successfully implemented the cloud services for commercial purposes. Discussing some of the well recognised cloud providers, Nebil (2011) identified Amazon and its number of cloud services and one of such is the Elastic Compute Cloud (EC2). The EC2 introduced in 2006 is a virtual computing environment that offers users the ability to customize and monitor access to their own 'virtual' web server. And another service of this kind is the S3 (Simple Storage Service) also owned and controlled by Amazon. The S3 provides users with web interface that enables them to store and retrieve data of 'any size' from the Internet. Google however is also a long time provider of cloud services and one of its most used Cloud Service is the 'Gmail' and others include 'Google Apps', a collection of web based applications that run over the web. Another function of the Google apps is that it allows for data storage on the web (Papadopoulos, 2011).

Similarly Microsoft is also a cloud provider offering users of 'hotmail' the Windows Live SkyDrive that provides Microsoft words, Excel and even the popular Presentation software (PowerPoint) over the Internet for free. Azure Services is one of the biggest eras of Microsoft cloud services. The Azure comprises of Window Azure (Cloud operating system) and Infrastructure services (Network World, 2008). IBM was also identified by Papadopoulos (2011) as another provider of cloud services such as 'Smart Cube', 'Smart Desk' and 'Smart Market'. Recognizing some of the major service provider at this stage will enable the research to give some supports to the discussions on security, privacy and reliability strategies behind some of these services.

2.3 Cloud Security and Privacy

Robinson et al (2010) described security as that which concerns confidentiality, availability and integrity of data. In relation to the definition, examples of security breaches can be unexpected system or network outages which are mostly attributed to man-made errors or natural disaster that can affect the service availability as identified by Paquette et al (2010).
Security is the major concern about the technology (redshift, 2011). A survey carried out by International Data Corporation of 'Chief Information Officers and IT Executives sighted by Nabil (2011) can reveal that 75% of respondents worry solely lies on securing their data on cloud. Subashini et al (2011) also sighted another survey by CSA (Cloud Security Alliance) that enterprises across sectors are willing to adopt cloud computing but the security concerns over cloud computing is a major threat.

Growing focus on the issue of security, privacy and trust challenges about cloud computing sparked up discussions in forums, professional gatherings, published journals, articles etc. Example of such scenario is the SecureCloud2012 organised by Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA) to hold in Frankfurt this year with aim of educating political and decision makers in industries such as CEOs (Chief Executive Officers) and Chief Information Officers to learn about the security issues (CSA, 2012). Similarly, the 2010 European Security Round Table (ESRT) forum organised to discuss about Risks and opportunities of cloud computing and the security assessment for local entities.

2.3.1. Cloud Security and Privacy Risks

Some of the top risks associated with cloud computing includes loss of control, Vendor lock-in, compliance risks, isolation failures, data protection, malicious insider, insecure or incomplete data deletion (ENISA, 2009).

2.3.1.1. Loss of control

Cloud computing involve customer giving away control and custody of company's confidential data, application to third party to in form of a wrap-click agreement. The level of control customers may have depends on the cloud service provider (Verizon, 2010). The cloud provider owns the physical storage facilities; therefore have the ultimate control over the data as well as every application that runs on those facilities. The users may be given access to some controls but over the browser and access to the back ends is lost to cloud provider as seen in figure 4.

2.3.1.2. Vendor lock-in

Implementing cloud solutions means buying into certain protocols and tools of the cloud provider. Vendor lock-in makes future migration of data, application or even infrastructures more 'difficult and expensive for cloud users; this may be due to non-agreed standard for regulating the cloud delivery models (CIO, 2012). Migrating for one cloud provider to another for some reasons known to the customers is hindered by the lock-in protocol of cloud service provider.

2.3.1.3. Compliance risks

There are certain kind compliance issue associated with cloud computing. Dr. Chenxi Wang of Forester argued that none of the compliance law and regulations recognized that a 'service provider may hold the data on-behalf of the liable organization'. Therefore, most of the compliance issues assign all of the responsibilities in cloud environment to the user (CIO, 2010). Golden of CIO added that despite the fact that compliance in this scenario is a shared responsibility, 'most or all the risks falls on the user'.

2.3.1.4. Data protection

Protecting data in cloud the cloud is one of the difficult because of cloud computing because of the different ways it can be compromised. Data can be loss due to some natural, man-made errors or data leakages through unauthorised access (Intel, 2010). Large businesses may have the financial and readily available skills which may make such scenario planned against but the fate of SMEs in this case remains a doubt.

2.3.1.5. Isolation Failure

Multi-tenancy is one of the characteristics of cloud computing that allows multiple users on one physical cloud resources through virtualization and hypervisor mechanism. Failure of these mechanism used in separating different users operating on the same cloud resources may give space chance for what is known as ‘guest-hoping attack’ (ENISA, 2009). This risk may give other malicious users the opportunity to access other users information sharing the facility.

2.3.1.6. Malicious Insider

Customers data can be maliciously altered from its original forms, deleted or disassociate from the larger context (Intel, 2011). Such risks can be associated with the data controller or even the cloud provider (ENISA, 2009). A survey conducted by GAO (2011) revealed how agencies are concerned about potential inadequacy of background security investigations concerning cloud vendor employees which may lead to increase in negative activities of malicious insiders.

2.3.1.7. Insecure or Incomplete Data Deletion

This represents a high risks to the customer in the case of multi-tenancy. When request to delete cloud resource is sent, it may not result in actually wiping of data or timely deletion of data because either the copies of the data are stored but not available at that time or there are other client on the same facility.

In addition to the risks described here by ENISA, Judith M. Myerson a systems engineer and Architect at (IBM, 2011) points out other important risks within the cloud environment.

Myerson stated that compromised ‘hypervisor’, missing security policies such as instance resource, user, and data requests associated with cloud service provider, insecure cryptography and bloated load balancing are some of the important aspect of cloud security issues.

2.4. Cloud vendors, customers and cloud control responsibilities

This is required for the study to understand properly the relationship between cloud service providers and cloud customer as well as the level of security responsibilities that exist between them. A vendor (cloud provider) owns the computing facilities and resources including hardware and in some cases SaaS, Users may be business, government agencies and individuals (Biswas, 2011) but for this study the users are SMEs. To understand properly, the relationship between customers and vendors Jansen and Grance (NIST, 2011) presents the diagram in figure 2 below. The 5-layered diagram describes the relationship between cloud providers and cloud customers illustrating the level of control by cloud providers against the cloud customers. Customer of IaaS has 3 layers of control over the others with 1 and 2 respectively.

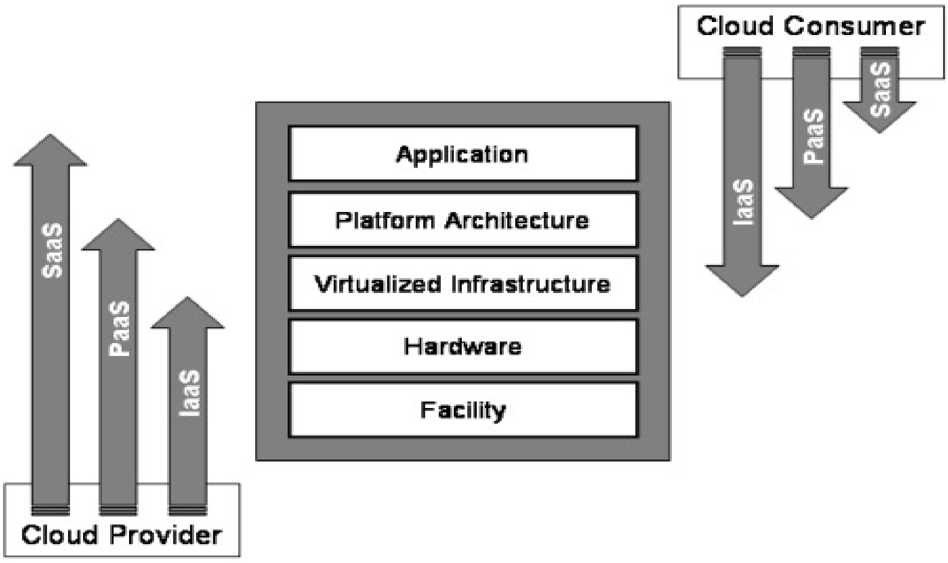


Figure 3: Differences in Scope and Control among Cloud Service model

(Jansen and Grance, 2011)

A Study carried out by Ponemon (2011) to learn how users and cloud providers are addressing the need to safeguard information in the cloud reveal that cloud vendors do not consider cloud computing security as one of their most important responsibility and as such allocated only 10% of their resources to security. The study also revealed 73% of US Cloud Service providers and 75% of their European colleague said their services did not substantially protect and secure their customers. Consequently, approximately 69% of cloud providers that participated in the survey did not believe that securing customers data was their responsibility. 16% of the respondent however did felt that securing data should be shared responsibility. The study also revealed that majority of the providers does not have dedicated security personnel to oversee the security of their applications, platform or infrastructure.

Similarly in 2010 user study carried out by the same institute Ponemon Institute revealed 35% of the participant thought that securing their data in the cloud was their responsibility while 33% thought it was a shared responsibility (Ponemon, 2010).

IBM (Technical White Paper, 2011) did agree that security control should be a shared responsibility. Figure 3 below described IBM's framework for a shared responsibilities.

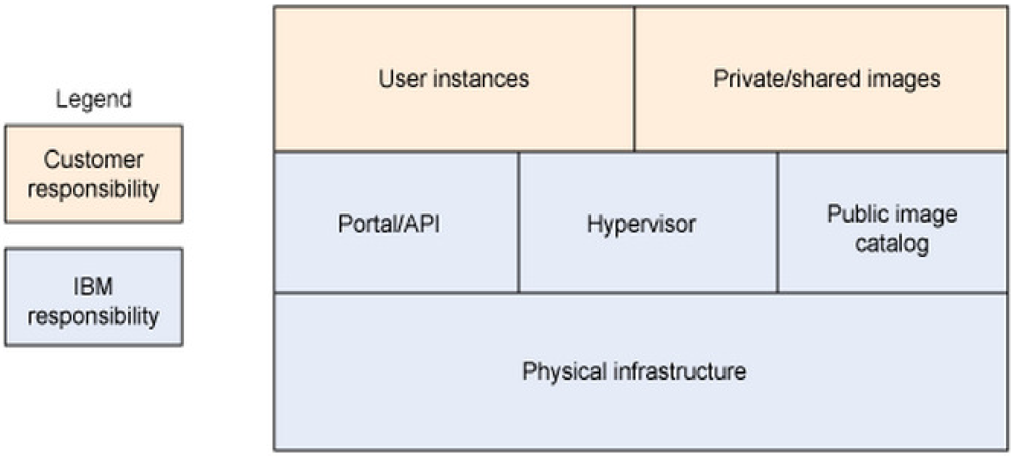


Figure 4: Divisions of responsibilities (Dkeyrel, et al, 2012)

2.5 **Law and regulations within cloud computing**

2.5.1 **Data Protection law**

Cloud computing services operate across different national boundaries with different restrictive policies. Differences in these cross border requirement for transfer of data and data ownership is a major barrier for cloud take-up (BSA, unknown date). A senior manager of global compliance at Google sees this as a difficult issue to 'juggle' (Savage, 2012).

2.5.1.1. **European Law**

The 1998 EU Data Protection Act governs the protection of personal information created and processed in the EU. The Act is applicable to companies that are situated or doing business in the UK or companies using equipments residing in the UK to process personal information (Gilbert, 2012). The regulation prohibits citizen's personal data residing within the EU to be transferred to any country outside the EU jurisdiction.

In response to this in 2000, the US initiated the Safe Harbor policy agreement that requires that any US companies that don't join the Safe Harbor must obtain 'authorization separately from each of the European countries' (Search CIO, 2001)

3.0. CHAPTER THREE: METHODOLOGY

The research strategy is developed around collecting data through primary and secondary data sources. The secondary data sources focuses on reliable written and published work, events or study on the areas of the nature of cloud computing, cloud security and privacy risks. The Primary data sources basically interviews and questionnaires are used to inquire from sampled participants in around small and medium sized business using or planning to use Cloud computing services to carry out some of their business operations. The main inquiries is built around trying to find out the level of understanding of cloud computing, availability of the knowledge needed to handle cloud adoption programme, users perceptions about cloud risks as well as their understanding of who is responsible for cloud security and privacy in the cloud environment.

This chapter intend to discuss the paramount approaches to data collection and analysis with the aim of identifying suitable research method to be used to collect informative evidence needed to justify and determine the proposed explanation and the outcome of the project.

3.1 Research Design

There are different approaches in carrying out a primary research. The Fixed design which is commonly known as quantitative research is a pre-planned approach in such that the researcher has beforehand a goal in mind “before the main stage of data collection takes place” Robson(2002,pp.81). Another form of research method which is mostly regarded as the qualitative research is the flexible design, an evolving approach that tends to change while the project is being carried out (Robson, 2002). The flexible design allows the researcher to make changes if the need arise in the course of the research process. Qualitative (flexible) design enables the researcher to apply an exploratory approach in the research process.

The strength or advantage of qualitative research is that it helps uncovers people’s experience and also focuses on small groups of which it can be less expensive.

People experience here involves data about what people feels, think or how they behave. However the research method does not allow for the collection of statistical data which is the major strength of the quantitative methodology. Data collected with qualitative method cannot be used for assumptions beyond the purpose of the research and can be heavily biased. The strength of quantitative methodology gives the researcher the freedom to easily measure and analyzes data in context of the study and can be used to gather demographic data for the research.

However, the strength of both approaches can be used concurrently or sequentially, most especially during data collection and analysis, such combination is what is regarded as mixed method or Multi-strategy (Robson, 2002). The infant nature of cloud computing may lead to a complexity of phenomena, thus in order to curtail such situation the project adopts the mixed method with believe that the researcher used the outcome of one data source to inform the design of the other data source.

The reasons for adopting this research strategy are wholly tailored towards a better validity of the data and to provide a more holistic and clearer understanding of the study. Table 3 below shows the main reasons for the selection of mixed strategy for the project.

Reasons	**Explanation**
Development: (inform questionnaire design)	Tends to use the outcome of the Interviews (qualitative data) to inform or help develop the questionnaire (quantitative) where appropriate.
Data Triangulation: (Data gathering and analysis and interpretation)	Using more than one method of data collection rather than relying on one single approach, with aim of improving validity of results. This is mostly needed in the data gathering and data analysis to filter responses for a clear interpretation.
Expansion:	Seeks to extend the breadth and range of enquiry by using different methods for different enquiry components.
Complementary: (Data analysis and interpretation)	To increase interpretability, meaningfulness, and validity of constructs and inquiry results by both capitalizing on inherent method strengths and counteracting inherent biases.

Table 1**: 'Purposes of mixed method research'** (David et al., 2011, Table 17.1)

3.2 Secondary Data Collections

3.2.1 Paper Selection Approach

Taking the research questions into consideration, keywords are carefully selected alongside their related terms to search for literatures in different sources. The searches produced different forms of literature including journals, whitepapers, seminar reports, Cloud computing related online news. Some of the main sources used include EBSCO host Business source Premier database, Cloud Business Review website, Google Scholar, Cloud Security Alliance Websites, Cloudtweaks, Computerweekly as well as some of the universities recommended websites and published materials.

3.3 Primary Research Strategy

3.3.1. Data collection Approach

There are different methods for carrying out a primary research; and some of the most common ones are interviews, questionnaire and/or survey to direct observations. For the purpose of limited time, the amount and types of data required as well as cost savings, this research will be using Interviews and questionnaires to obtain data.

3.3.1.1 Questionnaires

Questionnaires are inexpensive and most convenient way of obtaining data from people and with the advancement of the Internet facilities, it could be used to obtain data regardless of geographical location of the correspondent. This project will take advantage of these qualities to collect data.

Questionnaires however do have issues associated with it. The results or a response relies heavily on the type of questions asked. The project thus intends to use closed-ended items (Tashakkori et al, 2003) on a single questionnaires focusing mainly on the questions that will be relevant in the analysis, this is relevant in the sense that due to time constraints, minimizing irrelevant inputs is important. Relevant questions in this case means, questions that are targeted at generating the needed data that will be required for the analysis of the questionnaire results, for example, the project did not intend to emphasize its findings based on or around gender, and therefore if gender is not required for the analysis or towards answering, then it should not form part of the questions. The number of questions may affect the response rate if the questions are too many or comprises of long sentenced questions, the recipient may feel intimidated or feel too busy to attempt answering the questionnaire.

The questionnaire is designed to address the level of understanding of the technology by the participants and most importantly their understanding and perceptions of cloud security and cloud environment control responsibilities.

3.3.1.2 **Interview**

Interview is one of the major instruments used for collecting qualitative data. Frei and Oishi (1995) defined interview as 'a purposeful conversation in which one person asks prepared questions (interviewer) and another answers them' (interviewee). Thus, there are various issues concerning the interview method of data collections. First, there is a problem of respondent being biased in their responses. Interviewee biases are difficult problem to rule out in interviewing (Robson, 2002). The interviewee may provide socially desirable response rather than being honest. In order to try and establish the closest truth, a semi-structured interview method is adopted for the data collection. The semi-structured interview is adopted because there is the tendency that interviewees may have little or no idea about what cloud computing is which may give the interviewer the opportunity to add or make amendment to questions that suits the situation.

A good advantage of semi-structured interview and interview generally is its nature that provides the interviewer the opportunity to observe the respondent's behaviour face-to-face and make quick judgement by modifying the next line of questions or enquiry. Advantage of interview to this study enables the project to gain insight and thought of SMEs regarding their security concerns and understanding their responsibility in the cloud. Responses from interviews provide rooms for new thought that may be required to inform and encourage further insight and ideas into the study.

Structured interview is only relevant when the interviewee understands the phenomena from all perspectives. Unstructured interview on the second thought is also not required for the purpose of this study due to its informal nature as it tends to make the interviewer lose or deviate from the major results needed from the interview.

The interview is targeted at ten different SMEs with different industrial background. The reasons is to get a sample views of some of the IT decision makers who are mostly Chief Information Officers (CIOs) or the Chief Executive Officer (CEO) within the enterprise about their understanding of cloud computing and its major security concerns, responsibilities as well as how it may affect their decisions when planning adoption of the technology, their awareness of the security threat. The interview design helps the project to attempt answering the research questions in a systemic manner.

3.4 **Population and Sampling**

The target participants of the study comprises of two groups, one of which is a key decision makers identified by redshirt (2011) as the 'CEOs' and 'CIOs' of any selected company, preferably from the Information system or IT department to participate in the interview. The key decision makers is targeted because, their desperation to add new things to their business processes may be an attribute to explore which may give them a thought in providing the study with their best opinion. Some organisations however, may have different organisational structure which may require the researcher to identify and approach different personnel who is more credible to participate in the interview. The second participating group are samples of 10 staffs each from 10 different companies, preferably IT department and/or IT staffs of different industry sectors to participate in the questionnaire bringing the total size of participants to 100. However, the numbers of participants may be affected due to the willingness of the participants or other unseen circumstances which may affect the outcome of the response. The purpose is to create a sample of ten interviewee and hundred for the questionnaire respectively each to an industrial sector who may be perceived to have potentials of leveraging the power of technology to achieve the business goals.

3.5 **Characteristics of the Participants**

Due to time limit, the study specifically identified personals who are involved in decision making basically about IT strategy and IT implementation planning. This therefore picked company's Chief Information Officers (CIO) or Chief Executive Officers (CEOs) as identified by (redShift, 2011) to participate in the interview. Personnel with good or basic IT knowledge were also identified to participate in the questionnaire part of the study. The targeted industries include banking and Finance, marketing, Hospitality, Health, Information Technology, Retail, Accountancy and Business services.

3.6 Data Analysis

The data analysis will be based on the ‘exploratory’ research philosophy, a connected data analysis developed to generalize the research findings. The exploratory approach is brokered into three major steps identified by Creswell (2007). The analysis will try to analyze the collected qualitative data (Interview) separately and then collect and identify the quantitative data (questionnaire) independently and finally link results from both data group with the aim of using one of the group, leveraging the qualities of mixed design to support the other in areas where one is weak and one is strong in order to achieve a more reliable evidence that will explain the research questions.

However, the secondary data containing survey carried out on issues regarding cloud computing and security concerns will be referenced along with the analysis in other to identify during the review of literature comprising of journals, online articles as well as online magazines and published materials. The analysis makes extensive use of a group of software which are Google spreadsheets and Microsoft Office Excel to analyse the quantitative data and group the results for each variable. The variables however will be complemented with a broad descriptive analysis of each of the findings and results.

3.6.1 Analysis and Interpretation Method

Data Triangulation (Robinson, 2002) is required here and the reason is that there are data from different sources which requires the study to establish a systemic link between the problem and the outcome in order to make a better informed thought and insights to the findings. In other words, triangulation enables the researcher to merge the findings from the data collected through interviews and questionnaires. The data interpretation is carried out in two stages; individual interpretation which involves analysing and interpreting each data set separately and then the merged interpretation which involves synchronising the findings from the different sources in order to generate a single thought and then compare with the findings from reviewed literature.

The table bellow (Table 2) illustrates the process of triangulation from the analysis stage through to the process of data interpretation of each of the sources i.e. interviews and questionnaires. Triangulation enables the study to check the credibility and relevance of the findings and emphasises on the best possible interpretation of the data which may encourage further studies if findings are not relevant to the purpose of the study.

Input Output Analysis of the triangulation Process

Triangulation Process Described *Process – the triangulation process just like the data flow diagram described the relationships between data from different sources, how they inform each other and the merging process of the findings.*		
Inputs	**Process**	**Outputs**
Interview Data →	Analyse each interview Data →	Findings
	use observation to inform	
Questionnaire Data →	Analyse questionnaires data →	Findings
	Compare and merge interview data with questionnaire data	
Findings from Interview and questionnaire →	Compare findings with findings from reviewed literature →	Research findings
	compare with research questions	
Research question		

Table 2: Triangulation Data analysis processes

3.7 Ethical Issue

David et al (2011, pp.30) described ethics as a systemic study of or formalization of rules concerning the separation of good conduct from bad.

Ethical consideration is relevant in a research study that involves human subjects. This study seeks volunteer's attention and time, therefore will have to abide by some certain professional conduct in other not to harm the participant or make use of information obtained from them for public consumption without their consent. Some of the Ethical implications that need thorough consideration when carrying out the study include the participant's anonymity, no harm, confidentiality, voluntary participation, reporting as well as purpose of the study.

The research provides consent statement containing a number of issues presented on the information sheet which the participants have absolute right not to agree or agree (see Appendix A and B). The Information sheet contains the purpose of the study and some legal statement detailing the do and don't of the researcher.

Some of the documents are sent online and some by hand delivery to the targeted enterprise. The consent document has to be agreed upon and a careful study of the returned document is to taken down to the project diary as reminder of the appointment for interviews.

4.0. CHAPTER FOUR: DATA COLLECTION

This chapter discusses how the data for the study was gathered. With limited amount of time, study of this calibre need a carefully designed data collection instruments and a well thought of measures to gather the data. Data were collected through face-to-face interviews and online questionnaires after initial contacts with the targeted companies. The data gathering however did encounter some difficulties in getting some of the targeted interviewee to participate in interviews.

For the Interview processes, Initial arrangement to some company's CIOs and CEOs with request of their time to participate in the study was carried out. Interviews with the identified participants were arranged and consent given. The interview was intentionally carried out before the design of any further research instruments for the reasons that the observations and thoughts from the response and behaviours of the interviewee will help develop a better questionnaire later in the study. The response of 2 interviewees was recorded both in sound and hand written key points while the other two refused recording, key points however were taken down (see Appendix C to F).

As described in Chapter three, semi-structured interviewee was adopted, which gave the interviewees the freedom to express their feelings and perceptions towards the subject. The interview was conducted during working hour and 1 of the interviewee did invite a technical staff from IT division to join in the interview.

Beginning the questionnaire design, responses from the interviews were assessed and responses such as “the cloud security responsibilities questions was added in the questionnaire design. The study used Google doc forms to develop the questionnaire online. Letter of consent including the link for the online-questionnaires as well as the information sheet was sent to the identified participants for the questionnaire, this however created some delays from participants who did not respond to the requests on time. The questionnaire was handed to 10 different companies but 7 out of the 10 acted on the requests. The questionnaires gained 53 responses.

5.0 CHAPTER FIVE: DATA ANALYSIS AND INTERPRETATION

This chapter analyze and presents the results of the data collected. The fundamental goal that led to the collection of the data was to explore how SMEs approach the processes of engaging clouding computing services in their businesses. Do they have the knowledge about different forms of security, privacy and trust that are connected with the technology? The sampling data collected is expected to present a result that demonstrates an understanding of what the SMEs knows regarding the technology and its security concerns.

5.1. Interviews

The Interview was conducted and obtained some thoughts and opinion of specifically with three CIOs and one CEO from three different industrial background. The interview generated a number of findings and the overview of the key points is presented in the following paragraphs.

Interview ONE

This interview was with the Chief Information Officer of Microfinance bank, he attended a seminar on cloud computing October 2011. The interviewee shows a good understanding of cloud computing. The interviewee described cloud computing as ‘outsourced IT resources on subscription. Some of the key points obtained from this interview was that businesses particularly SMEs over relies on IT service providers with security issues. When the interviewer tries to understand the company’s fear over cloud computing, the interviewee conceded that trust and bandwidth were the major issues. However added that cloud ‘providers should have the mechanism to cub security issues’. The interviewee agreed that the cloud security is wholly the responsibility of the cloud provider but the company will only be responsible for keeping user information confidential.

Interview TWO

This interviewee holds a degree in computer science is with the Chief Executive Officer (CEO) of ASD Motors, automobile retail company with branches in about 10 states in the country, supplies automobiles to the government agencies and individuals. The points obtained from the interview can rightly acknowledge the importance of cloud computing to SMEs but stressed on security concerns. The Interviewee stated that SMEs embarking on such technology only does that on their own risks that he believes security control of the technology should not be overly relied upon. The interview made an interesting finding regarding compliance across multiple jurisdictions. Making it clear to the interviewer the nature of the data location, he said I quote “The problem with this type of technology, like I read on paper is that when my information got missing, who I should talk to, you?”

Furthermore, the interviewee as revealed in the first interview also revealed that at the moment, some SMEs including his are still reluctant to adopt the services because of trust and data privacy issue. The companies’ still uses BPM software locally on their internal data centre which he also confirms to be difficult and expensive sometimes. The interviewee concedes that the cloud security control responsibility is a shared approach, however did not attach much of importance to security control measures.

Interview THREE

This Interview is with a CIO, Quanteq Technology Services, an IT consultancy firm the interviewee agreed that cloud computing has huge advantages to SMEs having difficulty in engaging IT solutions for their businesses. He also stressed how the technology could create opportunity for traceable business processes that has suffered setback. (SMEs) lack the needed expertise and the funds to manage the technology in a manner that will benefit them rather than creating fear and remorse after adopting the services. The interviewee stated that there are occasions where companies will subscribe to business portals services for their company but will not last long before going out of the contract due to non-frequent usage. The interviewee agreed that his company was planning to expand its businesses to other locations within the country and therefore planning to run their CRM and BPM software on the cloud with a cloud computing service provider in the UK ‘possibly’ but presently shelved the idea. The interviewee produced some valid point on the issue of appropriate internal security measures to consider, stating that the security control should ‘mostly’ be handled by the services provider and as well advice adoptees about internal security measures.

Interview FOUR

The interview involved the CIO of a retail store with ‘lots of branches’, the store supplies both official and household equipments, electronics, foods, clothing, cosmetics and other accessories. The company presently have an in-house data centre managing their account and staffs information.

The Interviewee stressed that insufficient knowledge on “security control” with SMEs who have IT division is a concern and also added that in the case of cloud computing, ‘the security control should be taken care of by the service provider’. He further discussed that, confidential information are also at risk of being intercepted or obtain by external bodies. That they have being managing a business-to-business collaboration relationship locally with other business and would love to automate such processes but weak enforcement of standards and regulations within this jurisdiction can hamper a quick introduction of the technology to his organisation. The interviewee stressed that transaction over the internet is not safe.

5.1.1 Summary of Interviews

The Interview made some significant findings. There is a strong indication that there are major series of security concerns about the technology which may not directly be a different scenario with most SMEs. Not surprisingly, one of the major findings from the four interviews saw the majority from their body language and responses indicates that security controls should be solely the responsibility of cloud service provider. Two of the interviewee also believed that there is insufficient knowledge on handling IT security generally.

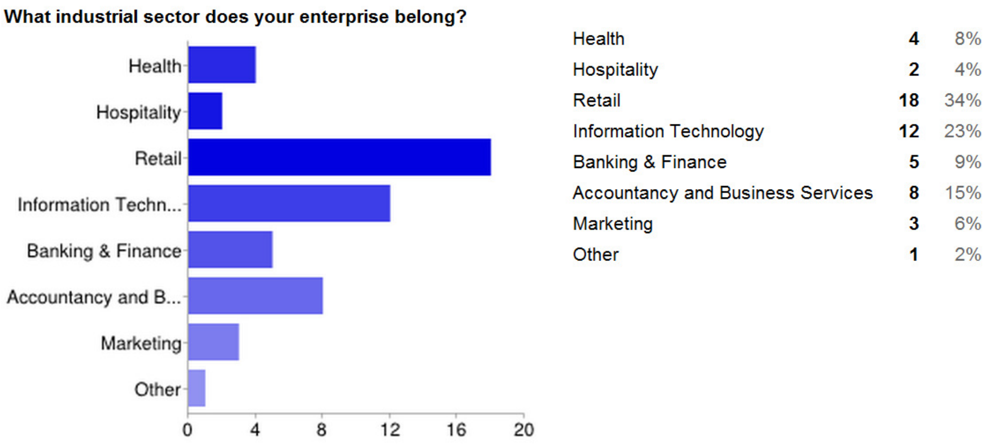
5.2. Questionnaire

5.2.2. Demographic characteristics of the respondents

The design was developed having a sample of 70 participants from different industrial background. Some SMEs were observed to have low number of IT/IS staffs; therefore the number of respondents was expected to be significantly low. Having that in mind, the research made a sample of 10 participants each from different background. A significant 75.7% respond rates was achieved from the questionnaire having 53 responses from the expected 70 participants.

Question one : Categories of participating companies

The questions is designed to categorize responses from individual participants according to the industrial sectors. The information may be required to check the level of popularity of cloud computing existence within all sector of businesses.

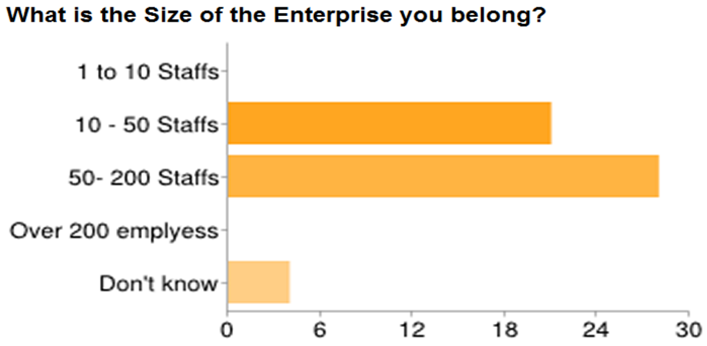


Health	4	8%
Hospitality	2	4%
Retail	18	34%
Information Technology	12	23%
Banking & Finance	5	9%
Accountancy and Business Services	8	15%
Marketing	3	6%
Other	1	2%

Analysis of the chart can reveal the number of correspondents that answered the questionnaires. The highest percentage of them all is the retail sector with 34% over 23% percentage of the Information technology sector. This means that retailers are becoming aware of the technology and are interested in knowing what it offers. Accountancy and Business service sector with 15% and the Health sector 8% respectively indicate the growth of interests from the SMEs.

Questions two: Size of the participated enterprises (total number of staffs)

The question looks at the size of organization of which each respondent belong. The data can be used to indicate that the study was actually based on the Small and Medium size enterprise.



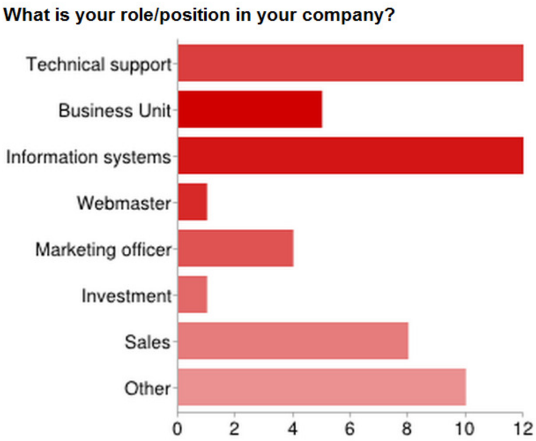
1 to 10 Staffs	**0**	0%
10 - 50 Staffs	**21**	40%
50- 200 Staffs	**28**	53%
Over 200 emplyess	**0**	0%
Don't know	**4**	8%

Analysis

Though 8% of the total number of those that answered the questionnaire may have the knowledge about the staff size of their working place and are not willing to disclose and it could as well be that the question was not specific enough, may be they have thought that size of a company may be the company's worth or its annual turnover. However, the purpose of the questions was achieved, 53% of the participants of the study did indicate that the size of the company they belong to is within 50-200 manpower and 40% respectively for the 10-50 staffs. The findings have shown that 100% of the participants are mainly from the small and medium size enterprise type of company.

Questions three: Position of the correspondents in their respective company

The question tends to understand the role of each of the participants in order to measure their technical knowledge about the technology.



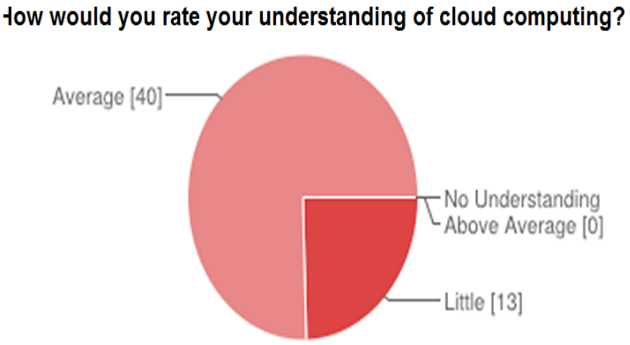
Technical support	12	23%
Business Unit	5	9%
Information systems	12	23%
Webmaster	1	2%
Marketing officer	4	8%
Investment	1	2%
Sales	8	15%
Other	10	19%

Analysis

As shown in the graph, about half of the correspondents have better background knowledge of information system in business. 48% of the respondents have shown a strong indication that about half of the participant did understand the nature of the technology better.

Questions Four: Understanding of Cloud computing

This questions helps the study to test the level of understanding of the technology by the participants, the project will use this data to back its finding in order not to generalize but to present the findings as samples that may invoke the need to build a strong background for useful responses. The question got a 100% percent responses from the 53 participants.



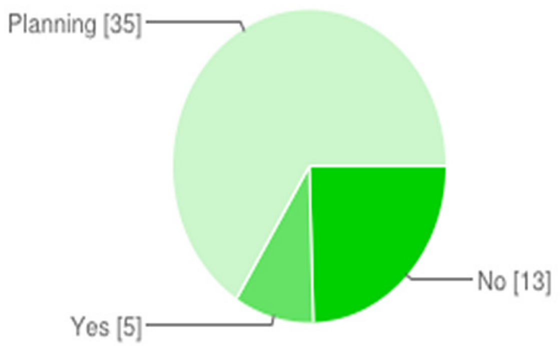
No Understanding of cloud computing	0	0%
Little	13	25%
Average	40	75%
Above Average	0	0%

The findings have shown a significant outcome having 0% of participants who have no knowledge of cloud computing. 75% of the correspondents have shown that they understand the basics about the technology in which 40 out of 53 participants indicates that they have average knowledge of cloud computing, which is a big boost towards the research results, as it will enable the study to obtain a better ends to the study. It has become necessary to know how they got the knowledge about the technology, the findings below seeks for the answer.

Question Five: Cloud Adoption status among participating company

Having said, they understand the technology, this question is designed to further test and confirm their claims, the graph below shows some of the results.

Is your enterprise currently using any of the cloud services?



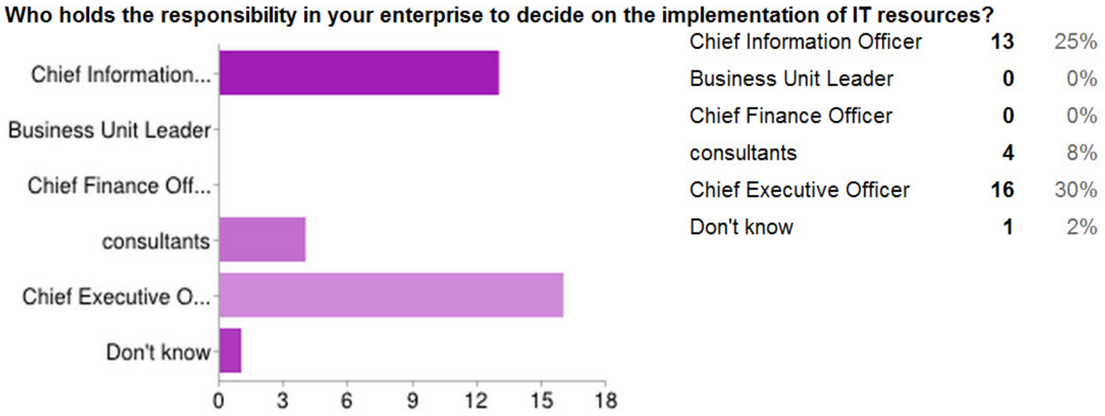
No	**13**	25%
Yes	**5**	9%
Planning	**35**	66%

Analysis

The results in the chart above indicates that 66% of the 53 participants stated that the organization they belong has not adopted any of the cloud computing services but are planning to and 5% indicates that they are currently using the cloud services already. And that makes a total of 71% out of the 75% that claimed earlier in the question four findings. The analysis indicates almost no-differences from the earlier claim which means the potential of a valid results is iminent.

Question Six: Decision makers

The study believed that SMEs decision makers should be at the forefront of the project, therefore this question however was suppose to be designed as an initial study before the interview stage. The interview raised a questions in the mind of the interviewer, which led to the insertion of the question into the questionnaire in order to test if the observations carried out before the interview was the right move. The question intends to find out who makes decisions that affects technological development in Small and Medium-sized companies.


Who holds the responsibility in your enterprise to decide on the implementation of IT resources?

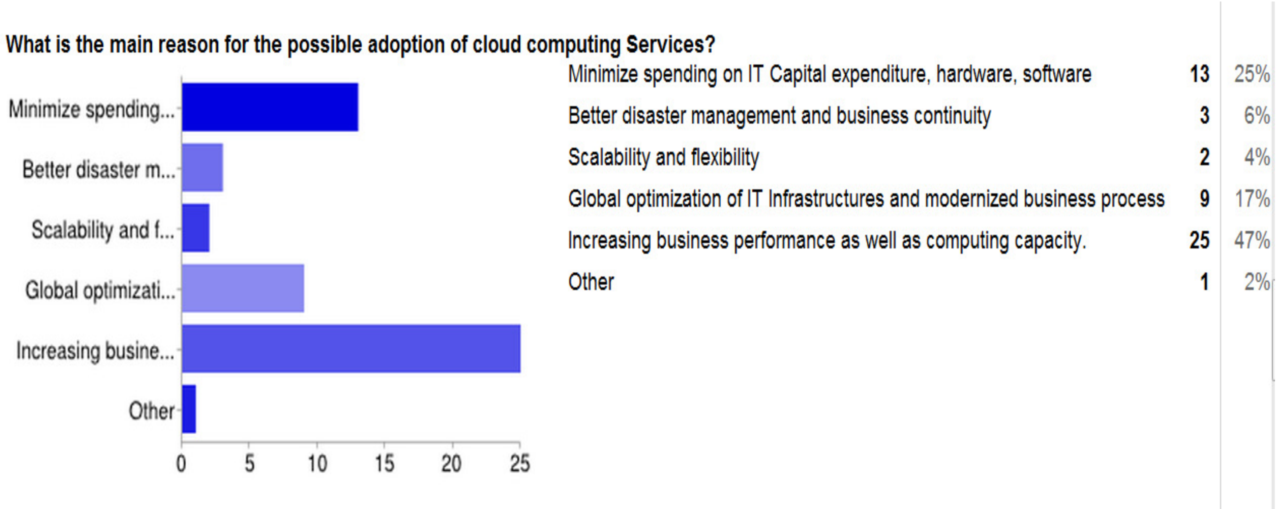
Chief Information Officer	**13**	25%
Business Unit Leader	**0**	0%
Chief Finance Officer	**0**	0%
consultants	**4**	8%
Chief Executive Officer	**16**	30%
Don't know	**1**	2%

Analysis

The results according to the chart presented here can reveal that 30% of the 33 responses indicate that CEO is responsible for making strategic decisions regarding implementation of IT resources in the company. 25% of the respondents believed that the company's CIOs own the responsibilities of making IT implementation decisions. 4% percent outsources their IT decision making to consultants. The overall result from the responses indicating that CEO is the key decision maker suggests that most of the participated SMEs do not have separate personnel to manage their IT division.

Question Seven: Reasons for adoption of Cloud Services

Having established the participant's level of understanding of the technology, this question is developed to see if they understand the essence of cloud computing and their response will determine the faith of the question that follows. Their understanding of the purpose of the may be one of the determinant of awareness of the type of concerns surrounding the technology.



What is the main reason for the possible adoption of cloud computing Services?

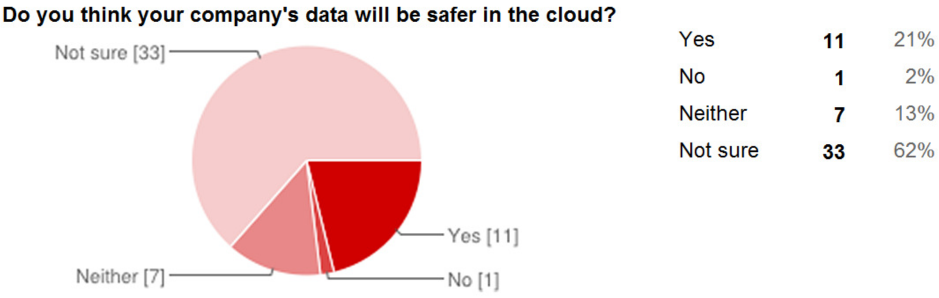
Minimize spending on IT Capital expenditure, hardware, software	13	25%
Better disaster management and business continuity	3	6%
Scalability and flexibility	2	4%
Global optimization of IT Infrastructures and modernized business process	9	17%
Increasing business performance as well as computing capacity.	25	47%
Other	1	2%

Analysis

53 people answered this question out of which 25 of them making 47% of the respondents adopt cloud services because it increases business performance as well as improved computing capacity and 25% believed that minimizing IT spending on capital expenditure is their main reasons. The result in this scenario shows that one of the main driver of cloud computing is improving business performance while increasing computing capacity which in the study context indicate a good understanding of the purpose of the technology which is also good for the study..

Question Eight: Security

The question is developed to investigate how the participants feel about securing data in the cloud against securing in-house data.



Do you think your company's data will be safer in the cloud?

Yes	11	21%
No	1	2%
Neither	7	13%
Not sure	33	62%

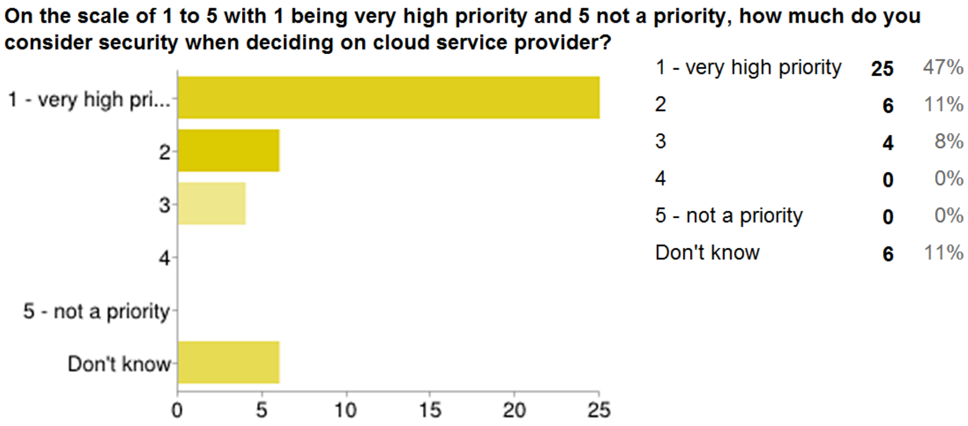
Analysis

The questions got 52 responses from the questionnaire out of which 33, that is 62% of those that answered question are not sure if the technology is safer in the cloud or better on premises. 21% percent of the respondent however did believe that their data is safer on the cloud and 2% disagreed to that stating that their data is not safer in the cloud. 13% of the respondent believed that their data is not safe both on-premises and off-premises.

The result suggests that majority of the responses either does not really understand the security context here or believed that their data is either safe or not safe in both environments. A good number of responses however prefer their data on the cloud rather than in-house.

Question Nine: Importance secured IT environment

This question is intended to see the perception of the correspondent concerning the importance of security of data and information to their organisation. The question is designed to enable the study gain the views of the participants over the importance of security in the cloud environment.



On the scale of 1 to 5 with 1 being very high priority and 5 not a priority, how much do you consider security when deciding on cloud service provider?

1 - very high priority	**25**	47%
2	**6**	11%
3	**4**	8%
4	**0**	0%
5 - not a priority	**0**	0%
Don't know	**6**	11%

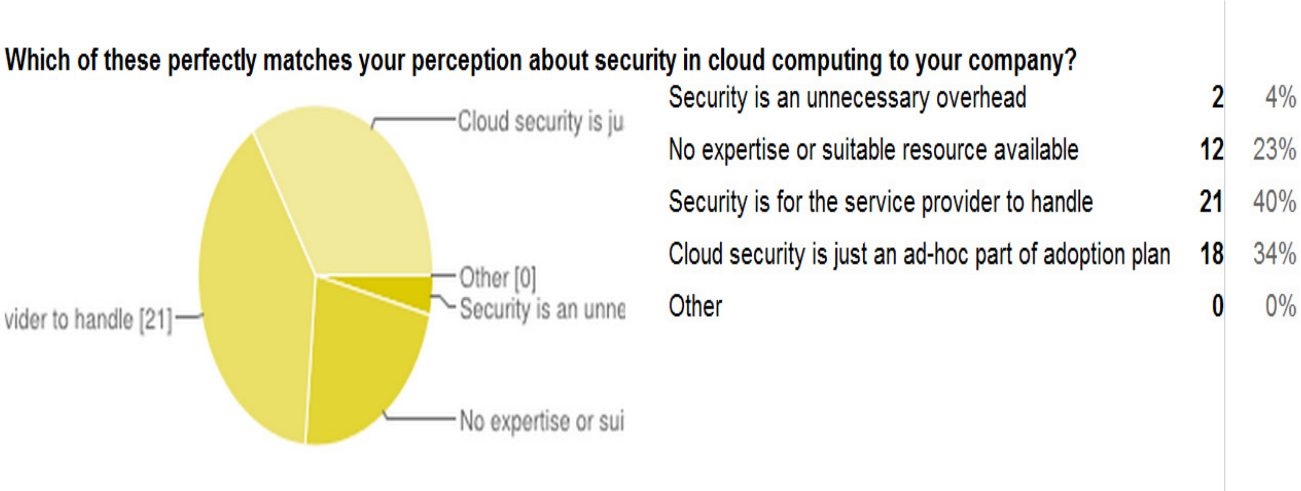
Analysis

41 participants answered this question out of which 47% percent agreed that security is a very high priority in deciding the adoption of the technology. 11% of the correspondent for some

reason does not know if the it security is a priority or not. The results suggest security of data and information as a very important issue for the organisation.

Question Ten: Relevance of security measures

The question is developed to test the participants thought or insight on the importance of security measures in the cloud environment.



Which of these perfectly matches your perception about security in cloud computing to your company?

Security is an unnecessary overhead	2	4%
No expertise or suitable resource available	12	23%
Security is for the service provider to handle	21	40%
Cloud security is just an ad-hoc part of adoption plan	18	34%
Other	0	0%

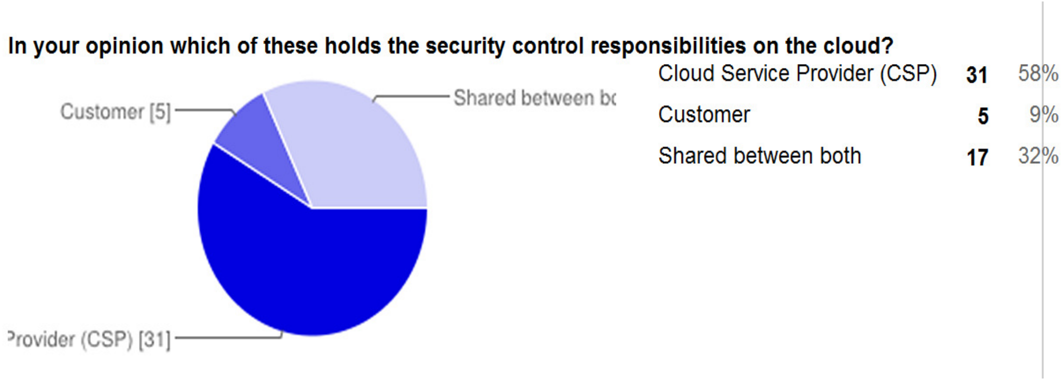
Analysis

While 4% of the 53 responses sees security as an unnecessary overhead expenses, 40% of the responses believed that security measures is not part for them to decide but CSPs. A reasonably large number of responses, 34% believe that security measure is a mare ad-hoc plan. 23% indicates that the security measure requires functional expertise.

The overall result indicates that the responses are either not interested or unconcerned about cloud security control in the cloud environment.

Question eleven: security control Responsibility

The questions is to enable the study find out participants perception about who holds the security control of cloud computing. The question was inspired from the observations while undertaking the interview.



In your opinion which of these holds the security control responsibilities on the cloud?

Cloud Service Provider (CSP)	31	58%
Customer	5	9%
Shared between both	17	32%

Analysis

The results indicates a little over half of the 53 responses, 58% strongly believe that security control in the cloud environment is the responsibility of the cloud service provider while 32% agreed that it is better shared. 9% of the responses indicate that the responsibility is that of the customer.

5.3 **Summary of Results**

The data sources, the interview and questionnaire indicate similarities in

- Responses received from the interview with a CEO and CIOs indicate that the participated have basic understanding of the technology which is a good sign for the study.
- The Interview shows a great sign that the participated SMEs are concerned with security situation of the technology with almost the entire participant stressing strongly on the issue. Similarly, the participants of the questionnaire indicate their fear of security.
- However, both sources perceptions of security in the cloud shows some of participants of the questionnaire indicating that cloud computing security control is either an ad-hoc plan or irrelevant aspect of the company can reveal that regardless of their fear, participating SMEs are either not concerned, over relied upon cloud provider or attached little or no importance to the security issues. Particularly, the interview with CEO of ASD motors indicates similar perception indicating that security control should be no much of importance to the user of the cloud since the data centre is under the control of the cloud.

- The interview indicates that three out of the participated interviewee concede that the responsibilities of cloud security control in the cloud environment solely belong to the Cloud Service Provider. Only 1 did admit that it is a shared approach. Similar findings were obtained from the questionnaire results.

- The background study revealed that the cloud provider rarely have dedicated security personnel for their data centre as the cloud security control is not part of their important businesses (Polemon, 2011). To confirm this in a similar finding from the perspective of the participated SMEs, primary research results also revealed some concerns about lack of knowledge regarding internet security. The interview with the CIO of IT consultancy firm gave the information that due to lack of funds SMEs finds it difficult to get services of security expert.

6.0 CHAPTER SIX: DISCUSSION

The project has leant so much from the primary and secondary research in the process of carrying out this study. This chapter discusses in a broader and explanatory perspective of findings from the background. The primary study is tested on the background finding in other to confirm its credibility to enable the study give reasonable conclusions.

The study learnt and did demonstrate a strong understanding of the technology, it attempted to describe the technology from the perspectives of different authors with purpose of identifying more holistic approach to the technology that enables the reader understands the technology with ease. In the process of carrying out the background study of cloud computing security, privacy and trust, the project learnt in chapter two that the security control responsibilities within cloud environment can’t be faulted on either cloud service provider or businesses respectively with both cloud vendors and business not agreeing to be responsible for cloud security control. To confirm these findings the primary study of SMEs from the sources, interview and survey gave strong backing on the belief that the responsibilities of the security control is the duty of the vendor. Like the secondary survey few of the participants agreed to the sharing approach of security control.

Majority of SMEs responded in the primary research that cloud control responsibilities are the duties of CSPs, while quite a reasonable number agreed it’s a shared responsibility. Similarly, the secondary findings could spot the same results but in this case, majority of cloud computing providers claimed that control responsibilities are for the customers to handle as against the views of the customers. Some customers in the study however deed concede in the previous study carried out by redshift in 2011 and Polemon respectively that the cloud control responsibility should be a shared approach to cloud handling.

The study also showed that the trend in security concern are not one of those overhyped media stories but a reality, as the primary and secondary findings can clearly show that regardless of the level of attentions attracted from the cloud experts, regulatory bodies such as Cloud Security Alliance (CSA) and other professional organisations, security and data privacy as well as trust in the cloud environment remains the major threats concerning the technology.

The attitude observed through the extensive study of existing work including surveys as well as the primary study of companies CIOs and CEO through interviews, shows that customers of the cloud expresses relaxed nerves over the security responsibility concerns due to the believe that cloud providers are securing their data, and that becomes a worry for the study in the sense that the study will have to source for information through different source that will strongly back the claims of each of the perceptions by participated SMEs.

6.1. **Cloud Security, Privacy and Trust a concern for SMEs**

This study could confirm that the survey finding from the review of literature indicating fears and concerns over cloud security is a reality as almost all of the participants of the primary study agreed that security is a major concern of the technology. The study did not just confirm but also revealed that the level of concerns over this issue is low as some participants overly rely on the providers of the services for security control. Cloud provider on the other thought did reveal that the cloud security control only receives 10% of the cloud business funding.

6.2. **Cloud security control responsibilities**

The study main aim was to identify if SMEs are the owner of the cloud security control responsibility. Study of the literature review did show that majority of cloud service providers pay little attention to the aspect of securing cloud data and majority also agreed that they do not have dedicated personnel for that purpose. This however could not be generalized as some small number of the cloud service providers was happy to share the cloud security control responsibility.

The secondary study can also reveal that some cloud providers like IBM did conceive the idea of shared control responsibilities as against the results from the Survey conducted by Polemon. IBM developed a structured framework of how these control is shared between cloud customers and the cloud vendors. **Figure 2** in chapter two is used by IBM to describe the level of control between cloud customers and vendors. **Figure 3** respectively describe the control level of each service model for the i.e. SaaS, IaaS, PaaS. The primary research presented similar results with the secondary findings. Majority of the participants for the interview did strongly believe that the security control responsibility should be the function of the cloud service provider.

With both the cloud provider and users pointing fingers at each other as observed from the three data sources it will be difficult to ascertain who should control what environment even when some providers believed that it is a shared responsibility, with some already drawn up framework to split control domain.

6.3. **Relevance of cloud security control SMEs**

The study from the Interviews and the questionnaire discovered that participating SMEs have various perceptions towards cloud security control in the cloud. A number of SMEs that answered the questionnaire perceived security control as an ad-hoc plan. Similarly the study on cloud service provider as discussed in Chapter two of this project also reveal how majority of service providers perceived security a non-core part of their business. Interviews with some of CIOs also enlighten the study on their attitude towards the security issues regarding the technology.

This bulk passing attitude between service providers and users did not however stop security experts from coming together under the auspices of the Cloud Security Alliance (CSA) in their quest to develop compliance standard and requirements within the cloud community.

Scenario such as this makes the study to realise that for SMEs to understand their responsibilities proper, they may have to deeply understand the different forms of security and privacy risks that exist within the cloud environment.

Evidence of lack of understanding of cloud security and privacy risk regarding to the cloud environment was revealed in the questionnaire findings as a reasonable number of participants believed that their company lacks the needed expertise to address cloud security strategy.

6.4. **Who is guarding the cloud?**

It is important to understand that cloud computing involves giving away the control of Data Centre to a third party. Cloud computing environment as the study have learnt involves two major players, those who owns the cloud and those who use the cloud. The study learnt that majority of cloud vendors fully disassociates themselves from the cloud security control and the same applies to the cloud users. The study also learnt that cloud environment extends from the cloud data centre that controls all of the components that have to do with the cloud to the users who mainly have ‘user’ controls over the virtualized applications, platforms and infrastructure controlled by the provider. Although it looked like a shared environment but the virtualized resources aren’t save and needs to be secured and control by those who have access to the back-end, the providers, authentication controls could be seen as a shared responsibility. It is observed that the technology due to its embryonic nature still have no agreed standard and therefore at this stage, no specific

7.0. CHAPTER SEVEN: CONCLUSION

The study is focused on cloud security and privacy and trust, identifying the nature of cloud security control responsibility in the cloud environment involving SMEs, cloud provider and the cloud. Primary and secondary data sources were used in the study. For the primary data the researcher adopted a semi-structured face-to-face interview and online questionnaire. Sampling of the interview and questionnaire participants was based on the observation from the background study. Google form and Google spreadsheet was used for the questionnaire data collection. Having more than one data sources, data triangulation was used to analyse the data with the aim of synchronizing each of the results for the purpose of answering the research question.

Based on the results of the primary and secondary data sources, the study learnt that cloud computing despite the enormous cost saving, operational and business computing promises and reasonably high adoption statistics; there are security concerns over data control ownership as well as data locations issues hovering over it. The study learnt that In Cloud computing, applications and data are hosted in the cloud, consumers rarely understand the location of their data, when asked, and they always point at cloud service providers. Neither will cloud providers for security reasons provide such information easily. Some specialist will argue that as custodians of confidential information; customers need to know the location of their data all the time. The reasons of which the study could understand were due to the non availability of cloud security standard or viability of data protection act of different region across border.

Lack of understanding of the impact of security threat, combined with fears over viability of cloud regulations and compliance by some cloud customers and cloud experts as identified during this research and from the reviewed literature is a major problem in ascertaining the location of customer's data and who is safeguarding the data. Even with that, most CIOs of SMEs seems to be more excited and therefore concentrates more on the positive side which is the benefits and almost ignore all the negativity associated behind those beneficial promises of cloud computing therefore unconcerned about the ownership of security control of cloud environment.

The major understanding from the project was that there are basically three levels of cloud security control responsibilities at the moment, the provider as a controller, the customer as a controller and a shared security control environment. The researcher learnt that cloud service provider did not admit to be the main handler of the cloud security responsibility and same as the cloud customers. The shared environment emanates from the belief of some businesses and cloud provider that security responsibility in the cloud should be a shared affair rather than a one sided approach.

Critically evaluating views of the majority of cloud users over relying on the cloud provider for cloud security control, vice versa could be interpreted as a complete back-to-end protection approach which in other words means the cloud provider controls every bit of the cloud security environment i.e. from the users end to the providers ends.

In reference to the background studies, specifically the IBM distribution of responsibility model, researcher could understand that cloud security responsibility can be viewed and shared by both parties, i.e. cloud providers and the cloud customers. The cloud provider as the owner of the ‘cloud’ i.e. data centre and the full control of the distributed virtual infrastructure, platform and applications is responsible for the backend security watch while the authentication control concerning user information be kept confidential.

The study could understand that there are efforts underway to combat these fears hovering over the technology. Different bodies associated with the technology such as the CSA and other experts are discussing and acting to develop cloud computing security standard. There is no single standard at this stage of the life of the technology concept. While, that is in progress, concerns over the differences in cross border jurisdiction are other worries mostly to countries with no data protection laws.

In conclusion the questions of ‘who is guarding the cloud’ remains an open questions as no single entity could be identified due to revolving nature of cloud computing. Experts are busy rolling out new ideas in the quest for a safer cloud as well as building standards. The study however identified three major entity of cloud security control environment which are the front-end user, the back-end vendor and the shared control environment.

7.1 Recommendations

The project was designed around CIOs and personnel with good IT knowledge in Small and Medium-size Enterprise comprises of different sectors. The study due to time constraint decides on sampling this sector into small number of participants. And based on the findings, SMEs overly relies on cloud providers in the case of security control and therefore are unconcerned basically about the issue.

However, in the absence of cloud security standard, it is recommended at this stage that SMEs in order to mitigate the cloud security and privacy risks audit the credibility of different cloud provider’s security policy before deciding on which provider manages their data.

7.1.1. Improving the Research

The study could be improved by an extensive study the strength and weaknesses of cloud provider’s policies. These could be implemented through deep involvement of cloud providers. Such may enable the project to provide a platform on which SMEs can possibly audit cloud providers credibility.

Furthermore, though cloud computing is not yet a fully standardized concept, the project could have in absence of cloud security standard at this stage try to develop a generic cloud security framework or guide for cloud computing environment including security services rendered over the internet that may be favourable for SMEs and cloud providers to . Despite the fact that lots of concerned organisations, individuals, government agencies have an on-going activity to contain these issues; there is a general belief that the effort is not enough. These may give the reader the opportunity to differentiate between cloud providers in terms of services and what to look out for in Service Level Agreements.

The study can also be improved by including a thorough investigation and examination of the general cloud environment looking at the kind of security control entity and identify how the three identified cloud control responsibilities i.e. vendors, users, and the shared environment can be critically explain in order to broaden and educate the study.

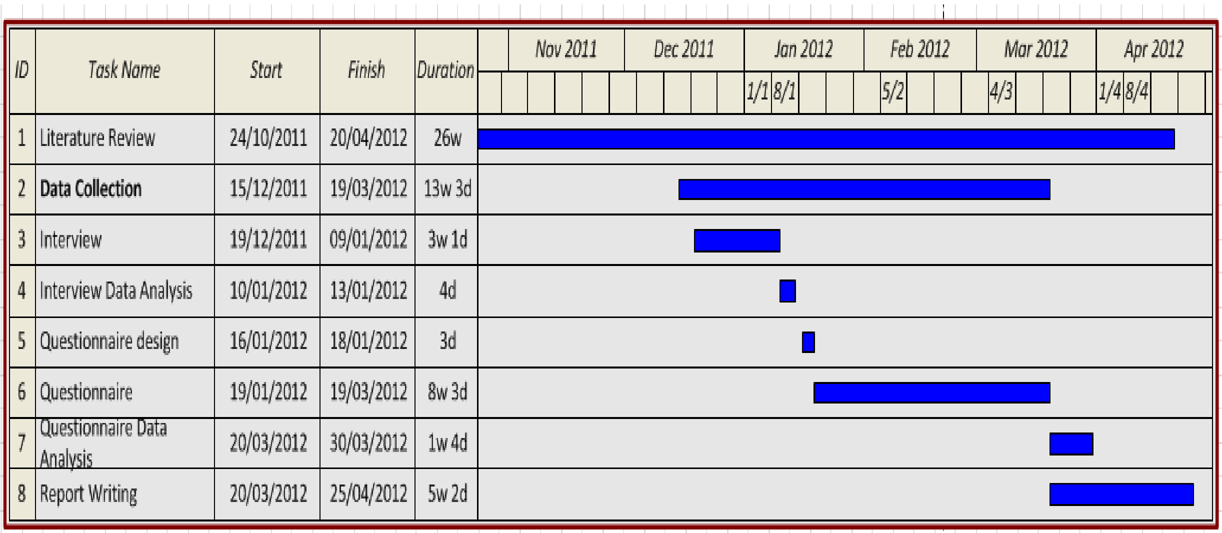
8.0. CHAPTER 8: PROJECT MANAGEMENT

The initial project plan was design for the project to finish by 12 of March, 2012. This however is not the case with the author as the processes were distorted by some anticipated problems. Delays in getting responds from the data collection participants were the major problems encountered.

This section is a reflection on the critical chapters in the project, their successes and difficulties encountered in the process of carrying out the tasks.

8.1. Revised Gantt chart

The revised Gantt chart is developed from the project diary showing the actual time spent on the project.



ID	Task Name	Start	Finish	Duration
1	Literature Review	24/10/2011	20/04/2012	26w
2	**Data Collection**	15/12/2011	19/03/2012	13w 3d
3	Interview	19/12/2011	09/01/2012	3w 1d
4	Interview Data Analysis	10/01/2012	13/01/2012	4d
5	Questionnaire design	16/01/2012	18/01/2012	3d
6	Questionnaire	19/01/2012	19/03/2012	8w 3d
7	Questionnaire Data Analysis	20/03/2012	30/03/2012	1w 4d
8	Report Writing	20/03/2012	25/04/2012	5w 2d

Figure 5: Project revised Gantt chart.

The revised Gantt chart carefully developed out of a proper review of the initial plan which made the author to move some days i.e. weekends out of the project plan to enable the author attend to some other academic activities.

Before the start of the project, the author spent some time trying to understand the project topic in depth. Adjustment had to be made in the process. The initial target for the project was too broad that requires the author to narrow it down to some researchable questions.

The literature review as seen in the Gantt chart was dragged on till almost the end of the report writing for the reasons that it continuously informs the study about any new literature entry about the project topic.

Data collection tasks were the main chapter that experienced an unrealistic time plan in respect of the initial project plan. The chapter consumed more time due to untimely responses from the targeted participants. Contact made by the author to the identified subjects to participate in the interview suffered so much delay. None response from about a half of the subjects contacted for the led the author to redesign the project diary to fit with responses that are readily available.

The questionnaire suffered the same lapses because some of the contacted subjects did not response to the invitation, this however did not stop the author to send links of the online questionnaire to the responses already got. This step was adopted in order meet up with the time allocated to the tasks. The project got responses from the rest of the subject later in the project when the author was almost closing the questionnaire.

The questionnaire would have gotten a higher response but due to time constraints and work on other aspects of the project, the author has to close the questionnaire for data extraction and analysis.

Appendix A.

University of Portsmouth

Information Sheet: 19/12/2011

Cloud Computing, Security, privacy and trust in the cloud.

RESEARCHER: Nuhu Audu, Student of Business Information Systems, University of Portsmouth, United Kingdom.

The study asked for your are invited to participate in this study, the following information explain why the research is being carried out and what your participation involve, please don't hesitate to ask me if anything that is not clear or if you want more information.

The purpose of this tudy is to find out from the perspective of Small and Medium-size Enterprise their concerns about cloud security, privacy and trust regarding who is responsible for security control between cloud customers and cloud providers. The information will be used to determine the reliability of other survey carried out by research companies.

You are invited to take part in a survey. The study typically involves answering an online survey.

If you chose to take part a 'consent form', is included on the second page of this document, which I would be grateful if you complete it and return to me by e-mail.

You are still free to withdraw from the interview at any time and without giving reason.

Anything you tell us will be kept confidential. My procedure for handling, processing, storage and destruction of data are compliant with the Data protection Act 1998.

- Data will be collected from the survey will be stored on Google spreadsheet.
- I will be the custodian of the data
- Identifiable data will only be viewed by Nuhu Enemaduku Audu
- The data will be deleted from Google doc. at the end of the study
- Direct quote might be used but these will not be attributed to any individual.

Appendix B.

Consent note

If when you have read the following paragraph, you consent to interview, please copy and paste the paragraph into your reply. Thank you.

I understand and agreeing to participate in this research I am giving my consent for the information provided by me to be used in the ways described in the Information sheet. My Name and personal information (including my address and online personas) will remain confidential and will not be communicated further nor published in the research. I have the right to withdraw from the Interview at any time.

Appendix C

Interviewer: Nuhu Audu
Interviewee: Anonymous **Position:** CIO
Company: Microfinance Bank
Industrial Sector: Banking
Date: 21/12/2011 **Time:** 11:32am

Introduction:
My name is Nuhu Audu, a final year student of Business Information Systems (University of Portsmouth, United Kingdom. The purpose of the interview is to obtain data regarding the position of businesses in the cloud computing, security, privacy and trust in the cloud

Interview questions

1. What is your understanding of cloud computing?

Response:
Contracting IT resources to an external Data Centre.
subscription

2. Using any cloud services?

Response:
YES
E-mail services (MTN)

3. What is your perception on the benefit of cloud computing?

Response

Lesser annual IT expenses
Lacks internal expertise
Access to official documents from anywhere.

4. What will discourage you from adopting the services

Response

Poor Internet connection
Lack of trust in online transactions

5. What is your perception about securing the cloud?

The providers
Security mechanism
Expertise
It's part of the subscription cost

5B. Followed up Question

Do you believe cloud service provider should be responsible for cloud security control then?

The company's data centre is for the company to control
The cloud is the responsibilities of service provider
BUT: keeping user information safe should be our responsibilities.

Appendix D

Interviewer: Nuhu Audu
Interviewee: Anonymous **Position:** CEO
Company: ASD Motors
Industrial Sector: **Retail**
Date: **29/12/2011** **Time:** **14**:00pm

Introduction:
My name is Nuhu Audu, a final year student of Business Information Systems (University of Portsmouth, United Kingdom. The purpose of the interview is to obtain data regarding the position of businesses in the cloud computing, security, privacy and trust in the cloud

Interview questions

1. What is your understanding of cloud computing?

Response:
Access to applications
Online storage
Pay monthly

2. Using any cloud services?

Response:
No.
Internal Data centre (BPM).

3. What is your perception on the benefit of cloud computing?

Response

working away from office
Save money on hardware
Easy access to modern software
Managing companies data

4. What will discourage you from adopting the services

Response

Lost information
Online theft

5. What is your perception about securing the cloud?

Service providers and the users
Nothing over the internet is safe

5B. Followed up Question

Do you believe cloud service provider should be responsible for cloud security control then?
It should be a shared responsibility
Buying things online was always at my own risk

Any comment?

Appendix E

Interviewer: Nuhu Audu
Interviewee: Anonymous **Position:** CEO
Company: Quanteq Technology
Industrial Sector: Retail
Date: 5/01/2012 **Time: 13**:00pm

Introduction:
My name is Nuhu Audu, a final year student of Business Information Systems (University of Portsmouth, United Kingdom. The purpose of the interview is to obtain data regarding the position of businesses in the cloud computing, security, privacy and trust in the cloud

Interview questions

1. What is your understanding of cloud computing?

Response:

Online storage (Skydrive)
Platform
Applications
On-demand

2. Using any cloud services?

Response:
Planning

3. What is your perception on the benefit of cloud computing?

Response

Easy entry
Save money on capital expenditure
Easily scalable
Irrelevance of geographical location

4. What will discourage you from adopting the services

Response

Security
Data privacy

5. What is your perception about securing the cloud?

'mostly' service provider
Advice adoptees on securing their own ends

5B. Followed up Question

Do you believe cloud service provider should be responsible for cloud security control then?

Partly

Any Comment?

Appendix F

Interviewer: Nuhu Audu
Interviewee: Anonymous **Position:** CIO
Company:
Industrial Sector: Retail
Date: 9/01/2012 **Time: 15**:00pm

Introduction:
My name is Nuhu Audu, a final year student of Business Information Systems (University of Portsmouth, United Kingdom. The purpose of the interview is to obtain data regarding the position of businesses in the cloud computing, security, privacy and trust in the cloud

Interview questions

1. What is your understanding of cloud computing?

Response:

Online storage
Software
On-demand

2. Using any cloud services?

Response:
NO
In-house data centre (accounting software and email)

3. What is your perception on the benefit of cloud computing?

Response

Save money on capital expenditure
Frequent access to modern IT infrastructure
Improved productivity

4. What will discourage you from adopting the services

Response

Internet never a secured environment.
Weak IT standard
Insufficient IT knowledge

5. What is your perception about securing the cloud?

Cloud provider

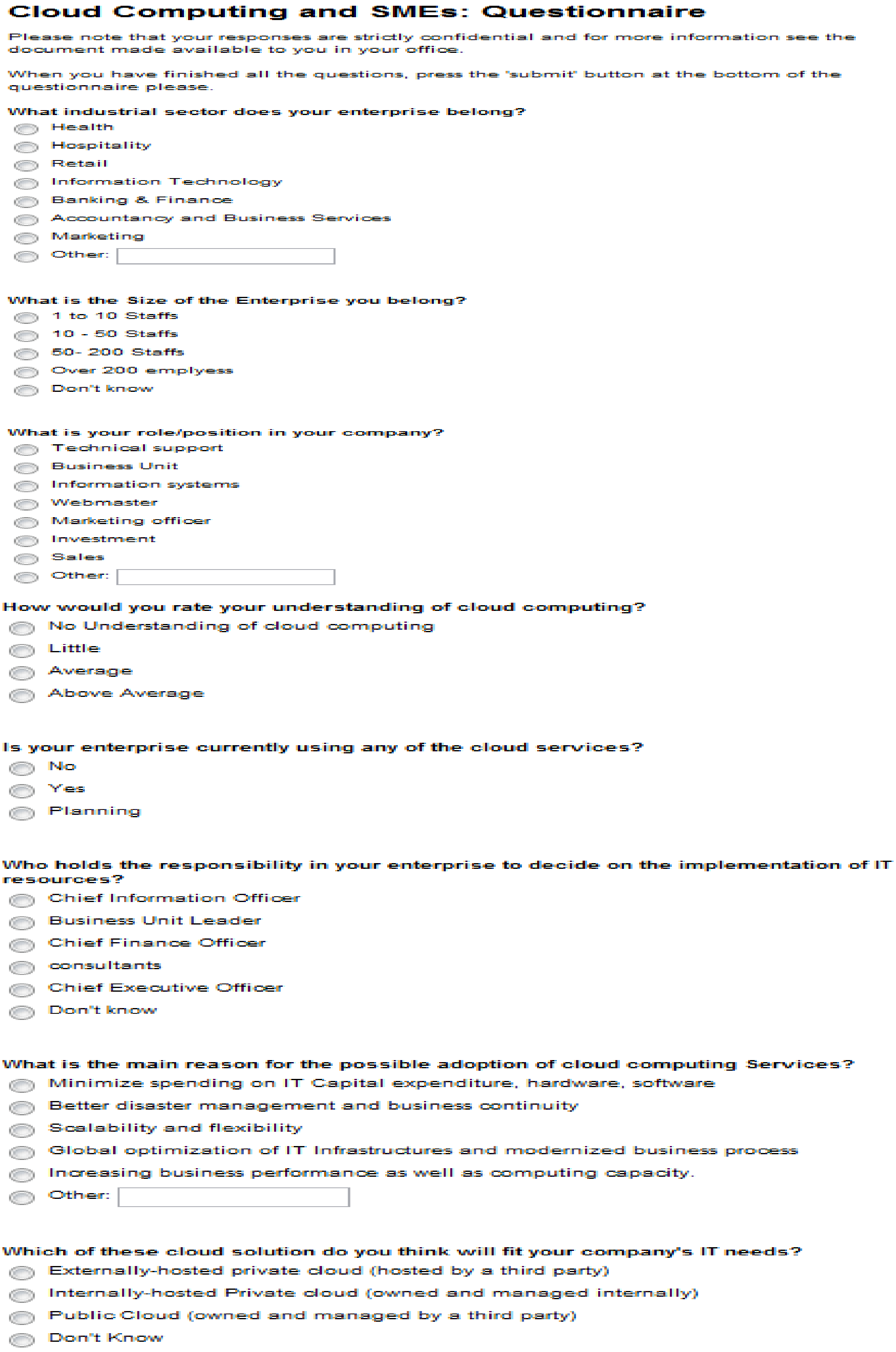
5B. Followed up Question

Do you believe cloud service provider should be responsible for cloud security control then?

Yes

Any comment?
'do not know if the country have any data protection law, even if they do, no enforcement'

Appendix G



Cloud Computing and SMEs: Questionnaire

Please note that your responses are strictly confidential and for more information see the document made available to you in your office.

When you have finished all the questions, press the 'submit' button at the bottom of the questionnaire please.

What industrial sector does your enterprise belong?

○ Health
○ Hospitality
○ Retail
○ Information Technology
○ Banking & Finance
○ Accountancy and Business Services
○ Marketing
○ Other:

What is the Size of the Enterprise you belong?

○ 1 to 10 Staffs
○ 10 - 50 Staffs
○ 50- 200 Staffs
○ Over 200 emplyess
○ Don't know

What is your role/position in your company?

○ Technical support
○ Business Unit
○ Information systems
○ Webmaster
○ Marketing officer
○ Investment
○ Sales
○ Other:

How would you rate your understanding of cloud computing?

○ No Understanding of cloud computing
○ Little
○ Average
○ Above Average

Is your enterprise currently using any of the cloud services?

○ No
○ Yes
○ Planning

Who holds the responsibility in your enterprise to decide on the implementation of IT resources?

○ Chief Information Officer
○ Business Unit Leader
○ Chief Finance Officer
○ consultants
○ Chief Executive Officer
○ Don't know

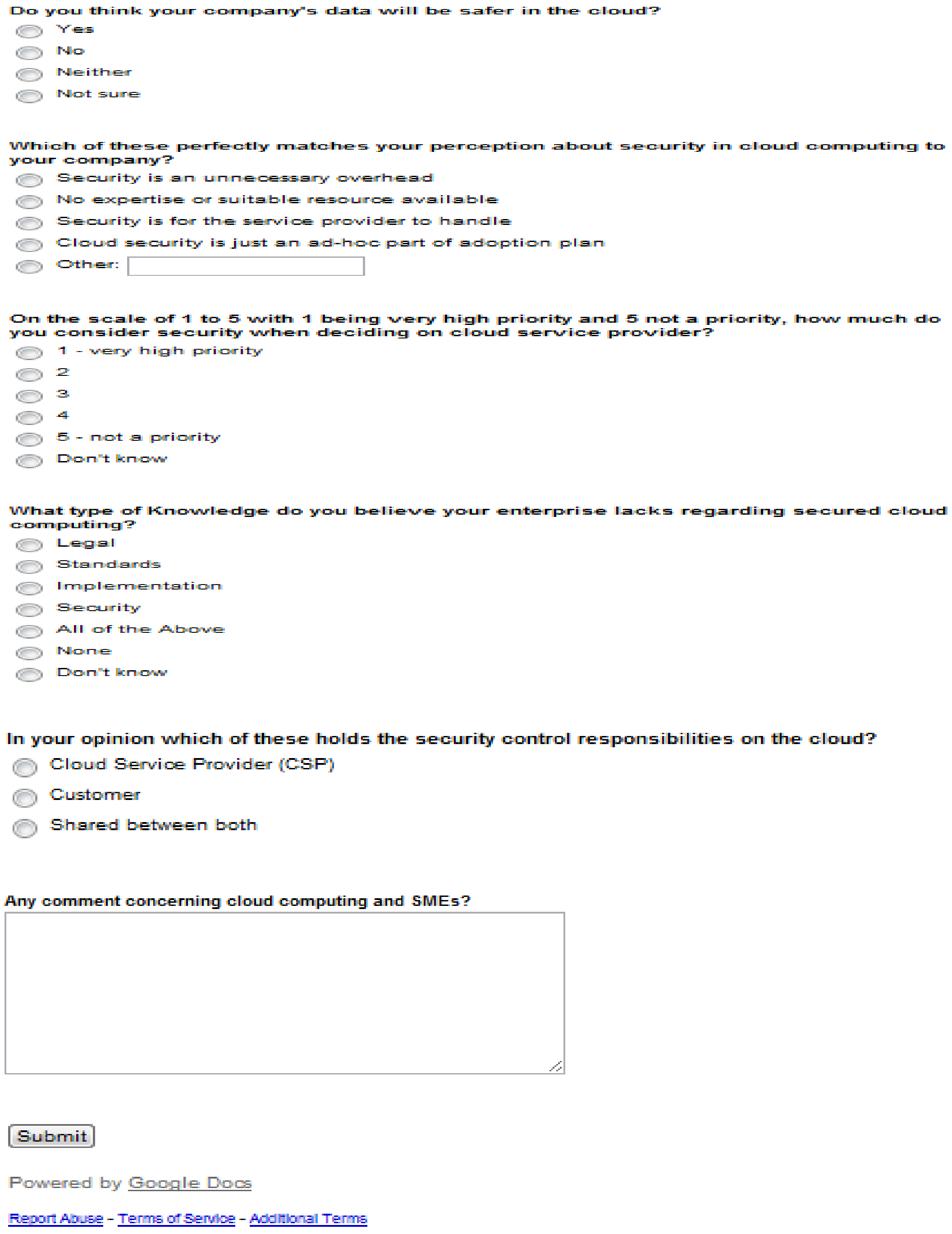
What is the main reason for the possible adoption of cloud computing Services?

○ Minimize spending on IT Capital expenditure, hardware, software
○ Better disaster management and business continuity
○ Scalability and flexibility
○ Global optimization of IT Infrastructures and modernized business process
○ Increasing business performance as well as computing capacity.
○ Other:

Which of these cloud solution do you think will fit your company's IT needs?

○ Externally-hosted private cloud (hosted by a third party)
○ Internally-hosted Private cloud (owned and managed internally)
○ Public Cloud (owned and managed by a third party)
○ Don't Know

Appendix H



Do you think your company's data will be safer in the cloud?

○ Yes
○ No
○ Neither
○ Not sure

Which of these perfectly matches your perception about security in cloud computing to your company?

○ Security is an unnecessary overhead
○ No expertise or suitable resource available
○ Security is for the service provider to handle
○ Cloud security is just an ad-hoc part of adoption plan
○ Other:

On the scale of 1 to 5 with 1 being very high priority and 5 not a priority, how much do you consider security when deciding on cloud service provider?

○ 1 - very high priority
○ 2
○ 3
○ 4
○ 5 - not a priority
○ Don't know

What type of Knowledge do you believe your enterprise lacks regarding secured cloud computing?

○ Legal
○ Standards
○ Implementation
○ Security
○ All of the Above
○ None
○ Don't know

In your opinion which of these holds the security control responsibilities on the cloud?

○ Cloud Service Provider (CSP)
○ Customer
○ Shared between both

Any comment concerning cloud computing and SMEs?

References

Armbrust, M. (2010). A view of cloud computing. Practice 53 – (4) 50-58.

BBC (2011). Sony chief Howard Stringer says firm acted quickly. Retrieved December 22 from BBC News Business: http://www.bbc.co.uk/news/business-13435386

Bbc. (2011). Amazon apologies for cloud fault one week on. Retrieved December 12, from BBC: http://www.bbc.co.uk/news/business-13242782

Case Studies (2012). Solutions: Retrieved April 7, 2012 from Amazon Web Services website: http://aws.amazon.com/solutions/case-studies/

Cloud Security Alliance (2011). Security Guidance for the critical areas of focus in cloud computing . CSA - (3.0) 1-178.

David, M., & Sutton, C. D. (2011). Social Research: An Introduction (2nd Ed.). London: SAGE Publication.

e-government (2011). Journal of E-Governance: Guidelines on Security and Privacy in Public Cloud Computing, 34 (), 149-151.

Frey, J.H & S.M.Oishi (1995): *How to Conduct Interviews by Telephone and in Person.* London: Sage.

Gilbert, F. (2011) Cloud Computing legal issues: data location. Retrieved March, 15 from SearchCloudsecurity: http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-legal-issues-data-location

Golden, B.(2010). Data Compliance and cloud computing: Key Questions. Retrieved 20 February from CIO: http://www.cio.com/article/612063/Data_Compliance_and_Cloud_Computing_Collide_Key_Questions?page=1&taxonomyId=3024

Greene, J. C., Caracelli, V. J., & Graham, W. D. (1989). Toward a conceptual framework for mixed-method evaluation designs: Educational Evaluation and Policy Analysis, 11(3), 255-274.

Kevin, M. (2010). Above Clouds: Managing Risk of Cloud Computing [Electronic version]. Cambs: IT Governance.

Khorshed, T. et al (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Elsevier (28), 833-851.

KPMG. (2010). From Hype to Future: KPMG's cloud computing survey. Netherland: Advisory

Martin, J., (2010) Should you move your small Business to the cloud?. Retrieved Novembe, 25 from PCWorld:http://www.pcworld.com/businesscenter/article/188173/should_you_move_your_small_business_to_the_cloud.html

McAfee, A. (2011). What every CEO Needs to know about the cloud. Havard Business Review. (no volume No)124-132.

McDonald, T., K. (2010). Above the Clouds: Managing Risk in the world of cloud computing. [electronic version]. Cambridgeshire: IT Governance Publishing.

Myerson, J., M., (2011). Cloud Services: Mitigate risks, maintain availability. Retrieved January 2012 from IBM: http://www.ibm.com/developerworks/cloud/library/cl-cloudservicerisks/

National Institute of Standard and Technology. (2011). 800-144: Guidelines on Security and Privacy in Public Cloud Computing. USA: Jansen W. and Grance Timothy

National Institute of Standard and Technology. (2011). 800-145: The NIST Definition of Cloud Computing. USA: Mell, P. and Gance T.

Ponemon Institute. (2011). Security of cloud computing Providers Study (unknown number). USA: Ponemon Institute.

RedShift research. (2011). Adoption, Approaches, and Attitudes: The future of cloud computing in the Public and Private Sector. USA: redShift Research

Ryan, M. D. (2011). Cloud Computing Privacy con our doorstep. Viewpoints 54 (1). 36-38.

Samson, T. (2011, December 7). Survey: Consumerization of IT a big driver to the cloud. Retrieved from infoworld: April 7, 2012 from InfoWorld: http://www.infoworld.com/t/cloud-computing/survey-consumerization-it-big-driver-the-cloud-181191

Savage, M. (2012). CSA at RSA 2012: International cloud computing security standards needed. Retrieved 12, March 2012 From SerachCloudSecurity: http://searchcloudsecurity.techtarget.com/news/2240118583/CSA-at-RSA-2012-International-cloud-computing-security-standards-needed

Subashini, S., and Kavitha V. (2011). A survey on security issues in service delivery models of cloud computing. Elsevier (34), 1-11.

Sultan, N. A. (2011). Reaching for the 'Cloud': SME can manage . Elsevier (34), 272-278.

Tashakkori , A., Teddlie, C. (2003). Handbook of Mixed Methods in Social and Behavioural Research [Electronic version]. California: Sage Publication, Inc.

Velte T. et al (2009). Cloud Computing: A practical Approach [Electronic Version]. USA: McGraw-Hill

Wilshusen, G., C. (2011). Information Security: Additional Guidance needed (12-130T). Washington: GAO.