Cloud Computing Security Issues

Entsar Mansour & Fathia Lahwal

Abstract

In the last three decades, the concept of computation has changed from centralized (client-server not web-based) to distributed systems and recently users are coming to the Cloud Computing "virtual centralization". Cloud computing is where data, software applications, computer processing power, can be accessed from cloud on line resources. On the one hand, an individual user can access data and applications from any device connected to the internet. What is more, data maintenance and the service is provided by the vendor which means the customer/client is unaware of where the data is, what processes are running or where the data is stored. So, logically, the customer/client has no ability to control over it. The internet is fundamental as the communication media of the cloud computing. This poses a substantial security concern for cloud computing. Guaranteeing the security of data is difficult as they provide numerous services such as Virtualisation, Utility computing, Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) Each of these services have their own issues of security, the vendor of cloud computing has to provide some guarantee in service level agreements (SLA) to convince the client that security issues have been considered and measures have been taken to ensure an adequate degree of security. The SLA has to illustrate diverse levels of security based on the various services to allow the client to understand the policies of the security which are being implemented. This project identifies issues related to cloud computing that should be considered by security practitioners. Three types of cloud computing issues are examined: integrity, availability, and confidentiality, and inspect the techniques that can be employed to counter them.

ACKNOWLEDGEMENTS

We would like to deeply thank the various people who, during the several months in which this lasted, provided us with useful and helpful assistance. I would like to express my deepest gratitude to my supervisor, Dr. Maria Kavanagh, and my second supervisor Anil for his an excellent support, advice, guidance and time. His support was crucial to my studying until completing this project. It was a great pleasure and precious experience working with him and all the staff at STRL...❀❀❀

Most important, to my loving husband *Abdlulbast* for his understanding and taking care of everything while I have worked on this thesis ...❀❀❀

My sons who put up with a string of goes to university, during weekends, and more working hours...❀❀❀

To all of my family in Libya, my father "*Mansour*", mother "Fathemah", sisters and brothers, thank you for your continued support and unwavering belief in me...❀❀❀

Finally, I would like to say thank you to my government for giving me this opportunity and their funding throughout my graduate studies...❀❀❀

Contents

List of Abbreviations

ARPANET	Advanced Research Projects Agency Network
2FA	Two Factor Authentication
CIA	Confidentiality, Integrity and Availability
CRSF	Cross Site Request Forgery
DPA	Data Protection Act 1998
HMAC	Hash based Message Authentication Code
HPC	High Performance Computing
HTTP	Secure Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IaaS	Infrastructure as a service
Paas	Platform as a service
SaaS	Software as a service
SHA1	Secure Hash Algorithm
SSL	Secure Socket Layer
XSS	Cross Site Scripting
SLA	service level agreements
CSA	Cloud Security Alliance
ISACA	Information Systems Audit and Control Association
IDC	International Data Corporation
IT	Information Technology
NIST	National Institute of Standards and Technology
EC2	Elastic Compute Cloud
S3	Simple Storage Services
CIO	chief information officer
PC	Personal computer
IBM	International Business Machines
HB	Hewlett-Packard storage
USB	Universal Serial Bus (USB)
U.S.	United Stat
TCG	Trusted Storage standards
TLS	Transport Layer Security
TPM	Trusted Platform Module
VM	Virtualisation Machine
TNC	Trusted Network Connect
DoS	Denial of service
CEO	chief executive officer
HIPAA	Health Insurance Portability and Accountability Act
PCI	Peripheral Component Interconnect
PVI	Private Virtual Infrastructure
AWS	Amazon Web Services
SSH	Secure Shell
IP	IP address (individual IP or block)
CIDR	Classless Inter Domain Routing
SAS	security assessment services
PIR	Private Information Retrieval
DLP	data loss prevention

List of Figures

List of Tables

Chapter 1: Introduction of Cloud Computing Ssecurity issues

Objectives to:

A. Overview of Cloud Computing Security Issues.

B. Provide the Motivation and Problem Statement

C. Give Research Aims and Objectives

C. List Research Questions

D. Outlines the Dissertation.

---

1. Introduction

The notion of Cloud computing is the most popular in IT today. It is already being used via tens of millions of users in diverse manifestations, involving services of free email, such as Hot Mail, Yahoo Mail, Gmail, etc.; and applications of free office productivity, such as Amazon Web, Google Apps; and several subscription-based software as a service (SaaS). The expression ‘cloud’ in computing means a ‘remote data centre’. It has a two-part definition [102][103][104]. The first is the ability to access the Internet by using a Web browser to computing resources that are administered remotely and dynamically allocated and de-allocated regarding the user requirements. Secondly, is the payment for computing resources for the actual use. What is more the internet is fundamental as the communication media of cloud computing. This poses a substantial security concern for cloud computing. assurance of the security of data is difficult as they provide numerous services such as Virtualisation, Utility computing, Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) Each of these services have their own issues of security, the vendor of cloud computing has to provide some guarantee in service level agreements (SLA) to convince the client that security issues have been considered and measures have been taken to ensure an adequate degree of security. The SLA has to illustrate diverse levels of security based on the various services to allow the client to understand the policies of the security which are being implemented. This project identifies issues related to cloud computing that should be considered by security practitioners. Three types of cloud computing issues are examined: integrity, availability, and confidentiality, and inspect the techniques that can be employed to counter them.

1.2. Motivation and Problem Statement

The aim of this project is focused on the security issues in Cloud Computing systems. Although the cloud computing concept gains more popularity, the security of cloud computing has many unresolved issues related to integrity, availability, and confidentiality of data and computing.

The definition of Cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, and services) that can be rapidly provided and released with minimal management effort or service provider interaction"[4]. Three model Applications of cloud computing as cloud service delivery comprise Software as a Service, (SaaS) Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) Cloud Security Alliance (CSA) [36].

In addition, cloud computing frees organizations from the need to buy and maintain their own software and hardware infrastructure as proposed by Levitt [5]. According to Erdogmus [6] there are two key business drivers in relation to cloud computing: (a) simplification of software delivery and (b) economics [7]. Furthermore Leavitt proposes that cloud computing offers additional benefits of technical features including easy scalability and high availability, in addition to direct access to IT resources, providing faster services [9].

On the other hand, there is much "buzz" on the cloud computing benefits, there has been growing alarm as to whether cloud computing is secure [10]. Hayes raises concerns about security, privacy, and reliability [11]. Regarding privacy, there is the probability that cloud computing might lead to "commingling of information assets with other cloud customers, including competitors" ISACA [12]. Viega predicts that code and data existing in environments of cloud computing will become more targets to hackers [68].

Related to reliability of cloud, [13] some dispute that few non-cloud IT infrastructures are as strong as the cloud computing service. However, organizations are still concerned about the availability of recent outages from Google and Amazon.

Gatewood proposes that cloud computing vendors‟ ideas “might not be fully developed or include records management rules-based control” [14]. The Cloud Security Alliance avoids the conception of cloud computing as a black box Cloud Security Alliance [36]. The recommendation of Information Systems Audit and Control Association (ISACA) is organizations need to perform risk assessment and business impact analyses as part of governance initiative of cloud computing [12]. As famed by Leavitt organizations are currently evaluating both the rewards and risks of cloud computing [7]. Essentially, the underlying the direction of this project is onthe statement by Nelson that “it is feasible that within the next 5 years, more than 80% of the world’s computing and data storage could occur in the Cloud” [91]. Likewise, International Data Corporation (IDC) which estimates that the income of worldwide IT cloud services will raise at yearly rate of 26% from $17.4 billion in 2009 to $44.2 billion in 2013.[92]

This project will examine these security issues related to integrity, availability, and confidentiality of data and computing., and discover practical protocol of cloud computing security

1.2.1. Research Aims and Objectives

The ultimate aim of this project is to explore a novel technique for cloud computing security based on requirements of confidentiality, integrity, and availability. To achieve this goal, the following research issues are considered:

1. Conducting a comprehensive literature review to understand cloud computing security issues.

2. Analysis of cloud computing security issues, which is considered to be the main feature to identify the issues as classified into three requirements of security (availability, integrity, confidentiality) as reported in selected literature (for more details see chapter 2).

3. Identification and analysis tools, approaches or methods that already exist and are used to make cloud computing more secure , available , integrated, and confidential.
4. Establish a related solution of the above mentioned issues
5. Develop a protocol for the recommended method

1.3. Research Questions

Security issues of cloud computing are defined in this project as the business impact considering/ net mission, the possibilities that a particular information systems vulnerability and threat source will exploit [93]. This project contains research questions as follow:

1) What are the major challenges of cloud computing security?
2) What are the security threats?
3) What are the security issues that must be considered for cloud?
4) What are the security techniques to protect data or sensitive information?
5) What solutions have been done for cloud computing issues that meet the requirements CIV (confidentiality, integrity, availability)

1.4. Dissertation Outline

The following describes the proposed outline of the author's Master Dissertation. The actual outline may vary, since at the moment, it is not clear how strongly the Dissertation will concentrate on the cloud computing security issues and finding good solutions for these issues.

1.4.1. Chapter outlines:

Chapter 1: Introduction for Cloud Computing Security

This chapter gives an overview of the dissertation, including motivation and problem statement, research objectives, research question and dissertation outline

Chapter 2: Overview for Cloud Computing Security and its Application

This chapter gives an overview of Cloud Computing Security issues and provides definition, structure and some Implication of Cloud Computing Security.

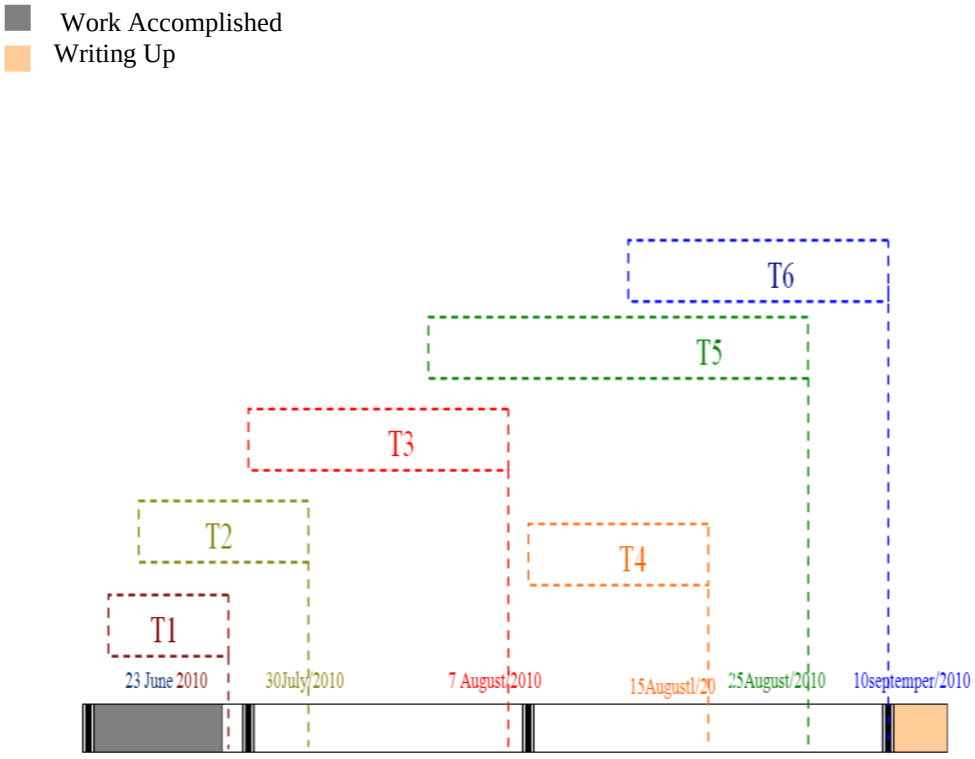
Chapter 3: Research Methodology

This chapter provides design of research methods, and development of research tools.

Chapter 4: Data Analysis and Discussion of Results

This chapter presents the data analysis and discussion of results. in addition , this chapter includes conclusions and recommendations for future work

1.4.2. Time Chart Dissertation Outline



T1: Overview regarding cloud computing security issue.

T2: Full understanding and specially Description about security issues of cloud computing.

T3: more investigate about security issues of cloud.

T4: Compare between different approaches of cloud computing.

T5: Developing approaches.

T6: Data collection and Analyse the results.

Chapter 2: Review of Cloud Computing Security Issues

Objectives to :

A. Overview of Cloud Computing Security Issues.

B. Exemplify Security threats.

C. Provider Example of Cloud Security Implication and Other Operations Relating to Security.

---

2. Background

There are diverse types of computing that led to the development of Cloud Computing. Grid Computing in the early 1990's was famous as the peer-to-peer networking; allowing virtual computers to structure a network to achieve very large tasks [100]. Subsequent Grid Computing, Utility Computing started in 1961. This idea died after a couple of years was then brought back in 1998 by Hewlett Packard. The idea of an "intergalactic computer network" was proposed by J.C.R. Licklider, who was responsible for the improvement of Advanced Research Projects Agency Network (ARPANET) in 1969. His vision was everybody in the world to be interconnected and be able to access data and programs from anywhere at any location.

Utility Computing is known as an on demand service, where customers access their own data via the internet or private lines. Some say Utility Computing developed into "Cloud Computing".[101] The Autonomic Computing is a new term which came before "Cloud Computing". The word "Cloud" of Cloud Computing represents the internet. The Cloud is the network joined with the computing infrastructure.

2.1. What is Cloud Computing?

Cloud computing is the next stage of development of on-demand information technology services, cloud computing based on virtualized resources. It provides different services which are based on different capabilities services such as Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS), Virtualisation, grid and Utility computing. The definition of cloud has been discussed by 20 different authors; definitions of cloud computing are as follows:

"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLA" [14].

According to National Institute of Standards and Technology (NIST), cloud computing is a model used for enabling suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, and services) which can be quickly provisioned and released through service provider interaction or minimal management effort. This cloud model encourages availability and is collected for essential characteristics, models deployment, and various service models [15].

Cloud computing indicates a rising model of computing where data in large machine centres can be dynamically provisioned. These are configured and reconfigured to distribute services in scalable methods, for wide requests from scientific research to e-mail to video sharing [16]. It is usually expressed as a single entity although cloud computing can includes numerous components at once: cloud applications, cloud platform, cloud infrastructure and the provision of cloud infrastructure as a service, both storage and resource are components such as Amazon's Elastic (EC2) and S3 service [17]. This infrastructure allows clients to construct the infrastructure themselves, in addition to containing the rapid expansion of their infrastructure, which is based on network requirements. A Cloud platform is the provision of software stack or a computer platform as a service, such as salesforce.com or Google's App engine. A Cloud application is web services that run on an upper level over a cloud infrastructure or platform which is available to the customers or organization's users. They can contain applications which are more popular such as Google Docs as a set of office applications, and video on YouTube's as hosting applications.

Providers of Cloud offer different services to individuals, corporations, small or big companies and government agencies. Cloud computing is used for clients employing sharing and storing of information, and database management. In addition, deploying Web services can range from processing huge databases, for complex scientific problems, and to use cloud to manage and offer access to medical records [7]. The incredible processing capacity level of data and information which is available in the cloud the petabyte scale allows new approaches to analysis data [18]. Clients may use cloud computing to store their documents and e-mail. Large groups of scientists and companies can use the huge computing power which is available to insert another dimension to their recent IT infrastructure [16].

Cloud computing opens up the opportunity of a main cloud provider such as Google so that they could finally become the world's primary computer [19]. Cloud computing speaks for a computing resource and centralization of information - quite opposite to the images that address evokes, and several, individuals, companies, and government agencies are already frequent or constant users. Already unknowing clients are taking benefit of the cloud throughout Web-based on-line data storage service and software applications, such as YouTube, Flicker, and Google [20].

The conception of cloud computing is not only to change the infrastructure of organizations, but also how they do business. As federal CIO Vivek Kundra has stated, ".....it's a fundamental change to the way our government operates" [16]. Accordingly, the government of federal has already started to apply cloud computing in their IT strategies [21]. In addition, the Obama Administration has interest in the large –scale use of cloud computing for processing and government storage [22]

This focus going on the electronic provision of information via the Obama Administration would take the government closer to the social expectations of several citizens. Now the majority government of information is digital, and clients want to access it electronically [23]. A 2008 study found 77.4% of users seeking services or government information regularly by using Google or any commercial search appliance [24]. Although, providing ever rising amounts of communication, government information, and services on-line increases serious issues about equality between people with limitation of technological means to contact e-Government [25].

According to Dikaiakos, the vision of 21st century is accessing the services of internet by light weight portable devices, instead of accessing it by a traditional Desktop PC. Cloud computing as technology has allowed individual users, companies or organisations or any enterprise to host their services without worrying about supporting services and IT infrastructure. Cloud computing comes from existing technologies which are not new such as Distributed Computing, Centralised Computing, Utility Computing. On the other hand what is new is that it integrates all the above to move them from a processing unit to virtualisation centre [26], [27].

The facilities of cloud computing start at a company by moving Capital to Operational Expense[29]. Amazon (EC2,S3),Google App, IBM Blue Cloud, HD Cloud Assure, Microsoft Azure, all of these services are available in the market of cloud computing [28].

2.1. Why is it significant?

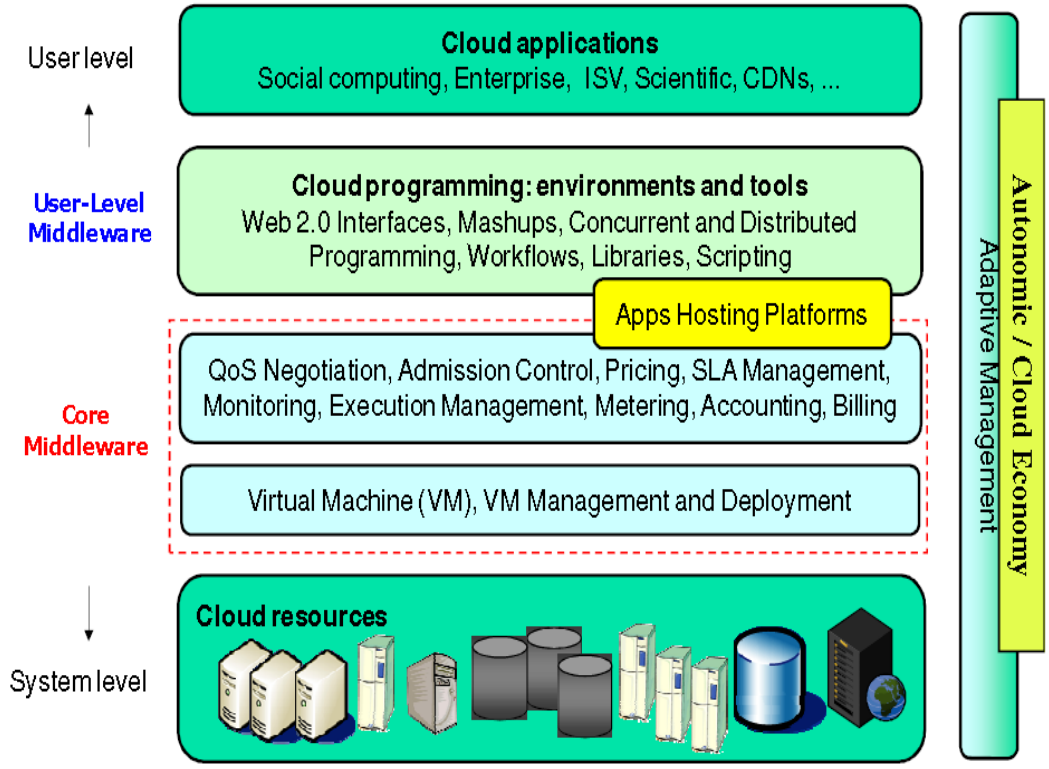
Cloud computing offers IT organizations with a diverse model of operation; many advantages of cloud such as the maturity of networks, web applications, and the increasing interoperability to provide IT services of computing systems. Cloud provides particular services and applications and this expertise allows them to manage maintenance, backups, disaster recovery, upgrades, and failover functions. As a result, customers of cloud services can see the rising of reliability, even as costs rise due to economies of scale or other factors. With cloud computing, companies can observe current needs and make modifications of capacity to increase or decrease, find spikes in demand to avoid paying for unused capacity through slower times. Beside the potential of lower costs, universities and colleges gain the flexibility of quick response to requests for new services when purchasing them via the cloud. Cloud computing encourages and provides IT organizations to increase standardization of processes and protocols. So that the many parts of the cloud computing model can be efficient and interoperate. Another key benefit of cloud computing is scalability for higher education, especially for research projects which require vast amounts of processing capacity and storage for a limited time. Some organisations have built data centres close to sources of renewable energy, such as hydroelectric facilities and wind farms, cloud computing affords access to these providers of "green IT." Finally, cloud computing allows university and college IT providers to make the costs of IT apparent. So IT services consumption can be matched to those who pay for such these services [30].

2.3. Cloud Computing Architecture

Figure (1) shows the design of a service-oriented layer of Cloud computing architecture. Core middleware capabilities with physical Cloud resources form the foundation for delivering IaaS. The aims of the user level middleware layer provides PaaS capabilities. The top layer User level focuses on application services (SaaS) via making use of services provided through the lower layer services. PaaS/SaaS services are provided and developed often by 3rd party service providers [34].

2.3.1. User-Level Middleware

This layer contains Web 2.0 Interfaces (IBM Workplace, Ajax) as software frameworks which help developers to create rich, cost effective browser user interfaces on which are based applications. Also the layer provides composition tools and programming environments which help applications in the creation, deployment, and execution in Clouds.



Resource : [98]
Figure (1) Layered Cloud Computing Architecture

2.3.2 Core Middleware

The platform level services implemented by this layer provide a runtime environment allowing capabilities of cloud computing to application services built by using User-Level Middlewares. Core services at this layer consist of Billing, Accounting, Dynamic SLA Management, management, Pricing and Execution monitoring. The services operating at this layer are those such as Google App Engine, Amazon EC2, and Aneka [31].

2.3.3. System Level

The computing power is installed with hundreds to thousands of servers in Cloud computing [33].There are huge physical resources (application servers and storage servers) which power the centres of data at the System Level layer. These servers are clearly managed via the higher level virtualization [32] toolkits and services that allow sharing of their capacity between servers virtual instances. These VMs are isolated from another that leads to achieving fault tolerant behaviour, and the isolated security context environments is supplied by a group of data centres[35]

2.4. Characteristics and Attributes of the cloud

There are various views on the description and number of the cloud's key Characteristics and attributes. There are five characteristics according to NIST which are comparable to Gartner's Five Attributes of Cloud Computing [36].

***NIST*: On-demand self service; Gartner: Service based**

A client can unilaterally provision computing capabilities, such that network storage and server time, automatically without entailing human interaction by each service's provider.

***NIST:* service orientation** is a specific focus of the Gartner definition, within considerations of the significance of service level descriptors and abstraction to a service.

***NIST:* Broad network access; Gartner: Uses Internet Technologies**

Capabilities are available over the internet and accessed throughout standard mechanisms which encourage use via heterogeneous thick or thin customer platforms (e.g., laptops, PDAs, and mobile phones). Standard mechanisms and protocols for interacting with the service.

***NIST:* Resource pooling; Gartner: Shared**

The computing resources providers are pooled to serve multiple clients that use a multi-tenant model (NIST), with diverse physical and virtual resources which are dynamically assigned and reassigned regarding to customer demand. The user is unaware where the exact location of the provider but might be able to specify location with a high level of abstraction (e.g., data centre, country, or state) and the customer may or may not have managed over where a service runs (NIST). Models of resources contain memory, processing, network bandwidth, storage, and virtual machines.

NIST: **Rapid elasticity; Gartner: Scalable and Elastic**

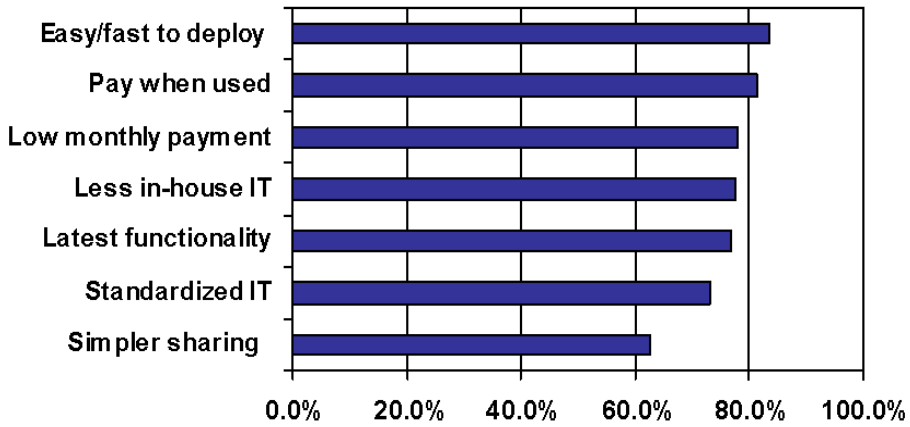
Capabilities can be elastically provisioned and rapidly and, this is automatically in some cases, to rapidly and quickly scale up released to quickly scale down, services must be able to scale resource provisioning quickly and automatically to meet changing needs. To the customer, the availabilities of capabilities for provisioning it, appears to be unlimited and can be purchased at any time in any quantity.

NIST: **Measured Service; Gartner: Metered by Use**

Cloud systems optimize resource and automatically control use via leveraging a metering of capability at a few levels of suitable abstraction to the kind of service (e.g., bandwidth, processing, storage, and active user accounts). Usage of resource can be controlled, monitored, and reported providing transparency for both consumer and the provider of the utilized service [36].

2.5. Cloud Computing advantages:

Several of the advantages of cloud computing has over traditional distrusted programming as shown it the figure (2). Many of the advantages that Cloud Computing paradigm has over traditional distributed programming paradigms are due to its capability to implement locally, close to the system outputs to be processed or near data to be analysed. It is desirable to many individuals and companies to use and benefit from the cloud.



Resource: [IDC]
Figure (2): Advantages of cloud computing

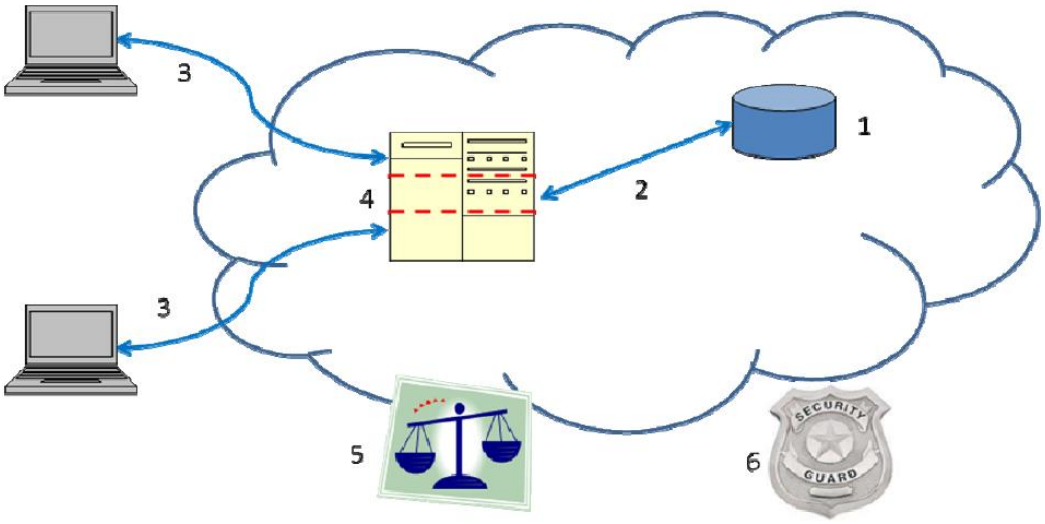
It is easy to deal with the increasing demand of resources by allowing the required resources from any provider of Cloud service. Equally, for any reduction of demand that leads to a cut down on the resource via not letting, is extra from the Cloud service provider. The rental of the resources can be put in a best way as “Pay-as-you-go”, i.e. the customers have to pay for the service.

Once the user stops using a service, the payment stops. Portability is another advantage of data with Cloud Computing. Also, clients of Cloud Service no longer have to be worried about constantly installing updates or repairs as this is taken care of via the Cloud Service provider. As the client’s data can be accessed anytime and anywhere throughout the Cloud, the client does not have to take other storage devices even as small as a USB drive [37]. So it can be summarised the advantages of cloud computing as follows:

1- Reduced costs
2- Resource sharing is more efficient
3- Management moves to cloud provider
4- Consumption based cost
5- Faster time to roll out new services
6- Dynamic resource availability for crunch periods

2.6. Critical Areas for cloud computing security

The Cloud Security Alliance (CSA) [36] has developed a seventy six page security guide (Security Guidance for Critical Areas of Focus in Cloud Computing V2.1) which identifies several areas for issues in cloud computing [38]. Cloud environment is a new model that cannot be well protected via traditional security approaches. From this comprehensive document, there are six specific areas that are selected from the cloud computing environment where software implementing TCG specifications and equipment can provide substantial security improvements [39]. Figure (4) illustrates the relationship between these areas in the cloud.



Resource: [107]
Figure (3): Areas for security issues in cloud computing

(1) Data at rest, (2) Data in transit,

(3) Authentication, (4) Separation between customers,

(5) Cloud legal and regulatory issues and (6) Incident response.

2.6.1. Securing Data at Rest

Cryptographic encryption is the greatest practice and in several U.S. states and other countries worldwide, it is the law of securing data at the cloud provider. Fortunately, manufacturers of hard drives are shipping self encrypting drives which implement the TCG's Trusted Storage standards [26]. Drives of Self-encrypting constructed encryption hardware into the drive, providing automated encryption with lower cost or performance impact. Software encryption can be used as well, but it is less secure and slower because the key of encryption can be copied off the machine with no detection.

2.6.2. Securing Data in Transit

Encryption techniques must be used in transit for data. Furthermore, authentication and integrity protection guarantee that data goes where the client wants it to go and without being modified in transit. It must use protocols such as SSL/TLS here. The difficult part is strong authentication, as illustrated next.

2.6.3. Authentication.

Authentication of User is the primary basis of access control, keeping the attack outside while allowing authorized users in with a minimum of fuss. Access control and authentication in the cloud environment are more important than another because cloud and all its data are accessible to everyone over the Internet. The TPM can provide powerful authentication rather than username and passwords. TCG's IF-MAP standard allows real-time communication among the cloud provider and the client about authorized users and another security issues. When a customer is reassigned or fired, the user's identity management system can inform the cloud provider in real-time. So the user's cloud access can be revoked or modified in seconds. When the fired user tries to login into the cloud, they can be immediately disconnected. The Trust of Computing allows authentication of customer PCs and another devices, that is critical to ensuring security of cloud computing.

2.6.4. Separation Between Customers

One of the clearer cloud issues is separation among a cloud provider's users (who might be competing companies or hackers) to avoid unintentional or intentional access to the sensitive information. Usually a cloud provider would use a hypervisor and virtual machines (VMs) to separate clients. TCG technologies can provide important security developments for a virtual network and VM separation. In addition, the TPM can provide hardware that base VM integrity and verification of a hypervisor. The TNC standards and architecture can provide security and powerful network separation [40].

2.6.5. Cloud Legal and Regulatory Issues

To verify that a cloud provider has powerful practices and policies that address regulatory and legal issues, each user must have their own experiences of regulatory and legal issues to examine cloud provider practices and policies to make sure of their adequacy. The issues to be included are data security, compliance, export, data retention, auditing, legal discovery, and destruction. For data deletion and retention, The TPM access techniques and trusted Storage can play a key role of limiting access to data.

2.6.6. Incident response

As part of expecting the unexpected, clients need to plan for the probability of cloud provider user misbehaviour or security breaches. An automated notification or automated response is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification allows the integration of diverse security systems and provides notification in real-time for incidents and user misbehaviour [40].

2.7. The Major Challenge of Cloud Computing Security

Moving security software from original operating system into an isolated virtual machine offers diversity challenges of difficult research. The most important high level challenges of cloud computing security are shown below [42]:

2.7.1. ***Performance systems***: are concerns for the real-world. Typically, the security is only useful if the impact of performance is acceptable to the administrators and users that will be working with the systems result. The potential resulting from pursuing this new architecture of security software will be far outside of the challenges which are described above. By protecting critical security of software, trust can be restored by building blocks for securing both desktop systems and servers.

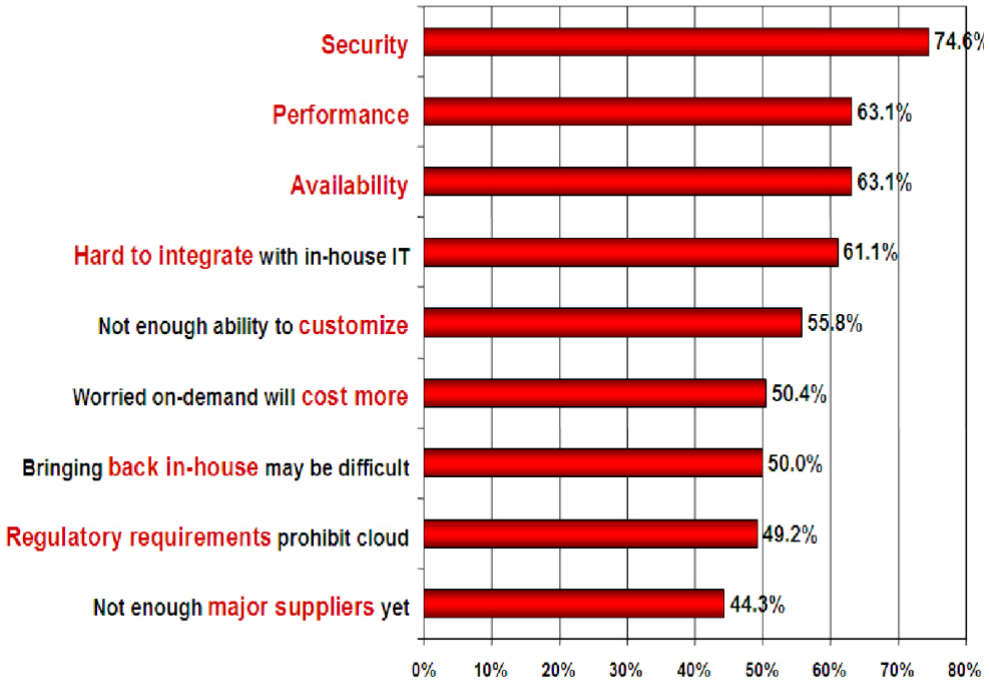
2.7.2. Accessing the information: In a traditional background, the security software might access all of this information by using the interfaces which is provided by the operating system. In new settings, these interfaces do not exist. So it must build both the mechanism and the interface to access for each piece of information which is needed [41].

2.7.3. Knowing when to access this information: it is as critical as being able to access it. When operating inside the monitored operating system the tools of security can easily place execution hooks during the system to collect notification of significant events such as file creation or new process execution. In new settings, there is no way which has been established to perform active monitoring among virtual machines.

2.7.4. Access level to information: that will be at low-level, so the need is to link the semantic gap to remove useful information from low level bytes.

2.7.5. New attacks: new kind of attacks is a concern through new architecture. For instance, data which is generated within the entrusted virtual machine that leads to introduce the

opportunity of a data driven buffer to overflow attacks against the security tools. This needs more understanding of security tradeoffs associated with new architecture [41][42]



Resource: [42]
Figure (4): challenges of cloud

2.8. Cloud Computing Security Threat

A diversity of sinister sounding security hazards can occur in cloud computing based distributed systems. For example, the cloud computing literature warns of brainwashing, hijacking, subversion, and implanting. To make sense of the diverse threats of cloud computing security, it is useful to apply some broad classifications. Six threat categories can be identified according to STRIDE [43]:

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privileg

2.8.1. Spoofing identity: Is illegally accessing via using another user's authentication information, such as username and password. In the case of **s**poofing identity attacking there are generally three forms that an attack can take:

- Authentication
- Protect secrets
- Do not store secrets

2.8.2. Tampering with data: That contains the malicious modification of data. Cases include unauthorized changes made to continual data, such as held in a database, the alteration of data as it flows over an open network between two computers, and Internet. Attacks by Tampering with data typically take one of five forms:

- Authorization
- Hashes
- Message authentication codes
- Digital signatures
- Tamper-resistant protocols

2.8.3. Repudiation: Repudiation threats are connected with users who reject performing an action with no other parties having any way to prove otherwise. For instance, a client performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non repudiation indicates to the ability to counter repudiation threats of a system. For example, a client who purchases an item might have to sign this item upon receipt, this make the vendor able to use the signed receipt as evidence which the client did receive the package. An attack by Repudiation will generally take one of three forms:

- Digital signatures
- Timestamps
- Audit trails

2.8.4. Information disclosure*:* It contains the disclosure of information to people who are not expected to have access to it. For instance, the ability of an impostor to read data in transit among two computers, or the ability of clients to read a file to which they were not given permission or granted access. In the case of Information disclosure attacking there are generally four forms that an attack can take:

- Authorization
- Privacy-enhanced protocols
- Encryption
- Protect secrets

2.8.5 Denial of service (DoS :) attacks reject service to valid clients such that, making a Web server temporarily unusable or unavailable. That has to protect against certain types of denial of service threats simply to improve system reliability and availability. Attacks by denial of service typically take one of five forms:

- Authentication
- Authorization
- Filtering
- Throttling
- Quality of service

2.8.6 Elevation of privilege: In this category elevation of privilege threats contain many situations in which an attacker become piece of the trusted system itself and has effectively penetrated the entire system, it is a dangerous situation indeed. An attack by Elevation of privilege will generally take one of three forms:

- Digital signatures
- Timestamps
- Audit trails

2.9 Cloud computing security issues

What are the security issues that are preventing companies from taking benefit of the cloud? Several studies, for example IDC's 2008 Cloud Services User Survey [43] of IT management, mention security as one of many challenge of cloud users.

This section contains three security issues. The Cloud Security Alliance's initial report [45] includes a different type of taxonomy based on 15 diverse security domains .The main three concerns of the security are:

- Availability
- Confidentiality
- Integrity

2.9.1. Availability

Availability refers to ensuring the information processing resources, unavailability may occur as a result of malicious action. A key importing point of cloud computing is for the client to have 100% uninterrupted availability. For large vendors, maintaining 24/7 up time is essential to their business, as consumers need this amount to enhance their missions significant efforts. However, outages of companies probably occur, and can be costly for the customer [82].

In a recent research of California University, Berkley followed the availability of several vendors of cloud and recorded about four major outages throughout the first four months in 2008. The reasons of these outages are due to overloads on the systems that leads the system to fail. In fact the issue in these cases refers to the vendor of cloud being a single provider, thus a single failure leads the company to failure [46], and the customers of cloud were unconcerned or unaware that the vendor had no back-up or redundancy mechanisms in place. During a period no more than 60 days, Apple Mobile Me, Amazon S3, Citrix, and Google Gmail, all reported periods or outages of unavailability between 2 to 14 h; in March 2009, and about 22 h were losing of Microsoft Windows Azure [47]. The estimated value of market $100 billion by 2011 [48], the outage cost of these companies can reach millions of dollars, without mention of another costs which are caused by lacking confidence via these organizations associates and own customers.

Natural disasters and unexpected events can affect the services of cloud and cause it to be become unavailable. For instance, in June 2009, one lightning strike on data centres of Amazon.com EC2 caused the loss of the service of cloud about 4 h. This was the third time in the last 2 years, and was a wide-spread outage [49]. On the other hand the vendor of cloud should be able to compute the demand from its services, in fact, this calculation based on the Request or its customers' services. This incorrect science has the potential of error which can lead to over capacity of cloud. Once the capacity of cloud reaches greater than 80%, cloud servers and local computers will "thrash" via constantly exchanging data among disks and computer memory. This leads computers to become unresponsive. If the design of the cloud is lacking enough slack resources to control a situation where over capacity happens, the whole cloud can fail [50]. The control to reduce this risk "is that when clouds reach their capacity limit, they could be architected so that applications can request no more computing capacity. They could gracefully degrade each application's usage, which could prohibit the application from working, but allow the cloud itself to remain functional". [82], [105].

Any outage based throughout overcapacity will have costs (both reputation and financial) to the client. For assessing bids of cloud services, the specialists federal procurement would need a deep understanding of the impacts and risks of even a minute's outage and what would be an acceptable range of downtime on a site-wide basis before a contract be awarded. Another risk of availability is how the priority of customers on the cloud is determined should the entry of overcapacity be reached. If the capacity starts to approach the 80% threshold and confronting some performance or services is necessary, the vendor will be protecting their own services and pass the poverty service to their clients. This risk refers to the need of the client to understand the cloud capacity and how their account will be managed. It is not easy, as a capacity of cloud's reserve is not clear, and data are not public by major cloud providers for competitive reasons. One pointer may be the usage of electrics via a vendor which t is one indication of the amount of technology used in their cloud. [51]. Variability in performance plays a risk to the users of cloud, as they will request a service which is predictable and reliable which will meet their service level requirements.

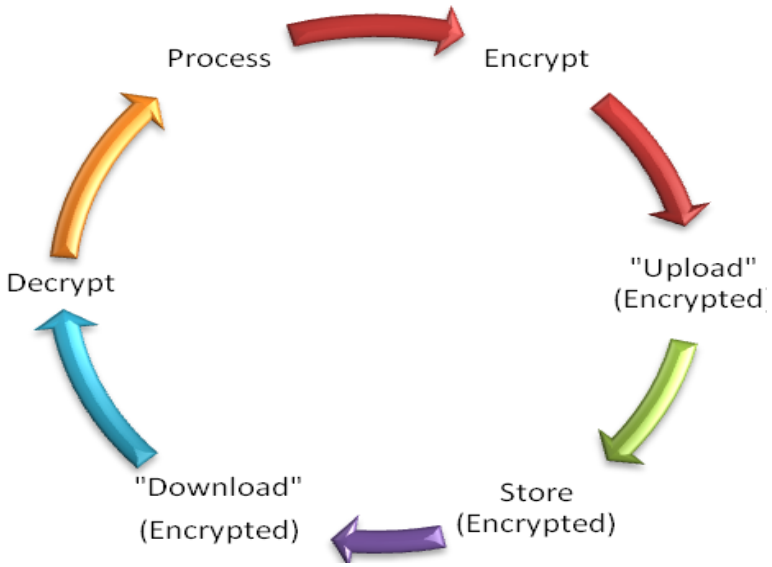
As cloud computing becomes major, corporations and popular and management entities become clients, that will naturally lead to the services becoming goals of malicious attacks via hackers. Cloud vendors will need to understand the issues which are presented by those. The vendors who can gather a number of complicated services to rejection attacks [52]; this risk was comprehended currently via Twitter and Face book [53]. Dependence on these outsourced vendors could have resulted in a major disconnection of communication inside, across, and with federal agencies. So the impact of this outage of federal users until now is not assessed. Another regard is the availability of the cloud vendor itself. If the vendor is subsumed via another vendor or goes out of business, the availability, safety, and custody of the data it had stored might be in question. In 2008, The Linkup of the cloud vendor rudely ceased operations with notice to its 20,000 clients. According to CEO Steve Iverson, "at least 55% of the data was safe [54].

2.9.2 Confidentiality

The main aim is to preserve the confidentiality of the database on the cloud. When confidentiality is achieved the entire cell is protected. The definition of a cell's confidentiality is to maintain when no user that does not have access to the cell is able to decrypt it.

Also it can be defined as the scope of a key is the number of cells in the database that the key can decrypt. A user may receive multiple keys to decrypt all her cells. Then her scope is the sum of all her keys [55].

Confidentiality refers to ensuring that information is not disclosed to unauthorized persons. Typically, the handle of confidentiality is through the usage of technologies such as access Control and Encryption. It still can be encrypted, but what happens for a large data set? This data has to be assembled or sent in the Cloud. Thus the data must be decrypted, complete the operations required, and then re-encrypt the data and resend to the Cloud. Any data left unencrypted at any stage in the transfer process or in the storage discloses it to unauthorized discovery. Unauthorized disclosure is the reverse of any compliance requirements or good security, such as HIPAA or PCI.



Resource [36]

Figure (5): Lifecycle of Encrypted Data

Security indicates confidentiality, integrity and availability, which create major issues of cloud vendors. Confidentiality indicates to who stores the encryption keys data from company A, to company B which stored in an encrypted format, that must be kept secure from unauthorized persons of B; therefore, the customer company must own the encryption keys.

John Krautheim researcher from the University of Maryland [57], also mentions the security and confidentiality issue about Cloud Computing. Krautheim designed the Infrastructure of Private Virtual of cloud security. So users require security over their information, and providers need more security of their own server over the fabric. The level of agreement among the client and provider is very important, because both of them are providing the responsibilities of each party. To observe the security of these parties Krautheim created LoBots.[56] This server provides a continual observing of the cloud communicates and environment to the PVI factory that allowed them to be aware of special situations. (PVI) through this service Krautheim wished to increase security while lowering the cost of ownership of IT infrastructure.

2.9.3. Integrity

Integrity of the cloud infrastructure is ensured through the use of Trusted Computing. In addition, we advocate the seamless extension of control from the enterprise into the cloud

through the powerful combination of high-assurance remote server integrity, and cryptographic protocols supporting computation on cipher text. With this approach, content is protected in a manner consistent with policies, whether in the enterprise or the cloud. Yet, because the protection mechanisms support computation, it is possible for all cloud participants to mutually benefit from the cloud data in a controlled manner. Hence, there is business intelligence advantages derived from operating in the cloud that simply don't exist otherwise. The ability to get smarter through use of the cloud is the key differentiator that will sufficiently alleviate privacy fears to ensure widespread adoption [105].

Integrity refers to all data received and should only be sent or modified by "legitimate" senders, it contains a number of fields that are critical to avoidance or mitigating the risks which affect the accuracy of information managed. Data quality, data validity, and security, speak to the system's operations; integrity is difficult to assess the validity of second generation of data. The processes and decisions involved in deciding which vendor to use and how the system is managed are equally relevant. It also addresses cost and schedule management, as well as performance and program efficacy. All of these are always a challenge for contract management processes and federal acquisitions.

Any information housed via a cloud infrastructure must maintain its accuracy, its integrity with the context to be of value to the client. The provider of cloud must ensure that all protections are taken to guarantee that data in the cloud storage has not been changed or corrupted; this will be not a safe assumption without a defined SLA. Recently, a provider of cell phone which stored data of customers (such as, contact lists, personal text messages, etc.) the provided cloud in a Microsoft subsidiary became unavailable when the provider missing that data. Clients wait days to be informed of that risk, with no guarantee that data might be restored.

Although, there is the level of data integrity, the timeline to restore, and the extent of data recovery [58] and the question of responsibility and liability appears. If the problem occurs, who would be responsible or liable for the problem, remediation and ensuing results? Could responsibility be determined based on the infrastructure? Without detailed knowledge of SLAs, these issues will not be easy for both government and the vendor to resolve. Due to a lack of

law of challenging case and federal policy, who owns information once it is remanded to a cloud's care is not apparent.

For instance, if a federal or soldier employee posts to a federal blog housed in a cloud, the terms of service among the cloud and the agency would decide who owns and controls their information. If the user is unaware of those terms and that information is breach, who would suppose that liability? This shows interesting implications of the double edged of sword that is the balance among free expression, verifiability, information accuracy, and accountability. All of these lead to threat of government although outsourcing such as IT technology. When outsourcing happens, it will become very important that the contract language reflect the needs and requirements of this language and is focused on the agreement of service level which include details measurements of performance and standards [59]. To provide assurance on the privacy and security for both services and data must integrate the requirements of the government's risk management plan.

2.10. Multiple Levels of Security

2.10.1. Host Operating System: Administrators with a business have to access the management plan that requires the use of multi factor authentication to obtain access to purpose constructed administration hosts. These administrative hosts are systems which are specifically designed, built, hardened and configured, to protect cloud management plan of all that are audited and whose access is logged. When the user no longer has a business need to access his management plan, the access to the hosts, privileges and relevant systems are removed.

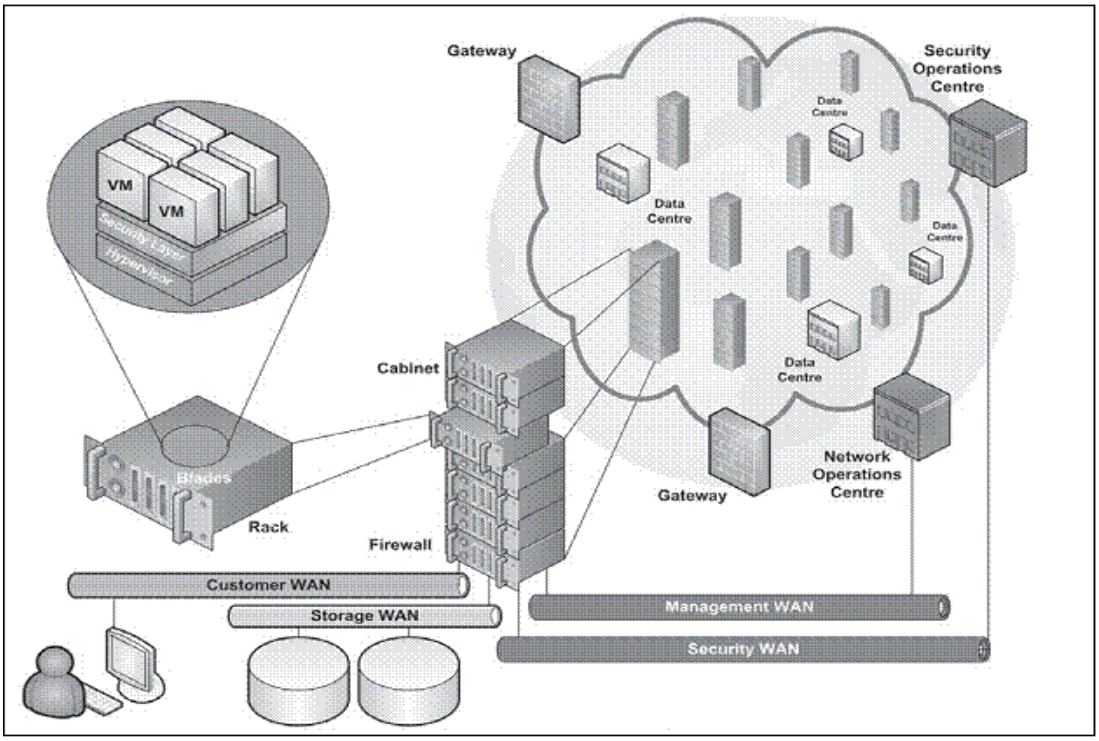
2.10.2. Guest Operating System: Virtual instances are fully controlled via the client. Customers have administrative control or complete root access over services, accounts, and applications. Amazon AWS is unable to go to the guest and does not have access rights to client instances. AWS proposes a basic set of security measures which include: clients should disable password which gives basic access to their hosts, and use some form of multifactor authentication to win access to their instances (or at a least certificate based SSH Version 2 access). In addition, clients should utilize a privilege escalation method by logging on a per customer basis. For instance, if the guest operating system is Linux, after freezing their request, they must employ certificate based SSHv2 to contact the virtual instance and disable remote root login, use both ‘sudo’ for privilege escalation and command line logging. In order users

should create their own key pairs to assurance that they are exclusive, and not shared with AWS or with other customers. [99]

***2.10.3. Firewall**:* Amazon EC2 offers full Firewall solution; this necessary inbound firewall is configured in a default reject mode, clients of Amazon EC2 must clearly open all ports which required allowing inbound traffic. The traffic might be restricted via all of service port, protocol, and via source IP address (Classless Inter Domain Routing (CIDR) or individual IP block). The firewall can be construed in groups permitting diverse classes of cases to have different rules. For instance, in the traditional case there are three level web applications. The application servers group would have port 8000 only accessible into the web server group. The web servers group would have port 443 (HTTPS) and/or port 80 (HTTP) open to the Internet. The database servers group would have port 3306 (MySQL) only open into the group of application server. All of these groups would allow administrative access on port 22 (SSH), except only from the client's corporate network. High level secure applications can be deployed by using this expressive [99].

2.11. Security Implications

According to Sloan, he has exposed the complicated technologies of cloud computing in which he discusses the challenges posed of security of cloud computing. According to him, security components might be added to the security Layer and be delivered as security as a service. To make sure CIA (Confidentiality, Integrity and Availability) of the information, the service provider should test stringent access controls, encryption schema, and scheduled data backups [1]. The architecture of security of cloud computing is shown below in figure (6).



Resource [67]

Figure (6): cloud computing security Architecture

There are various clouds available in the markets that are lead enterprises to start using diverse clouds for diverse operations. Finally there will be a situation where the cloud integration services that require a different approach of security implication [2].Organisation need to confirm where the assurance comes from [3].

Although the basic components of security have been identified the requirement of security varies with respect to the business needs and domain. Cloud Security Alliance has identified 15 domains of cloud computing as shown above in the table (1).

Domain 1: Cloud Computing Architecture framework
Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal
Domain 4: Electronic Discovery
Domain 5: Compliance and Audit
Domain6: Information life cycle Management
Domain 7: Portability and Interoperability
Domain 8: Traditional Security, Business Continuality and Disaster Recovery
Domain 9: Data centre Operation
Domain 10: Incident Response, Notification and Remediation
Domain 11: Application Security
Domain 12: Encryption and Key Management
Domain 13: Identity and Access Management
Domain 14: Storage
Domain 15: Virtualization

Resource [36]

Table (1): domains of cloud computing

While many people have touted virtualization as the solution to today's computer security problem, closer inspection reveals that it is not quite that easy. In fact, when designed or deployed poorly, virtualization can negatively impact security. This is because using virtualization means adding more software to your computer, which means more opportunities for vulnerabilities. Furthermore, as data centres consolidate their servers, it is possible to now have multiple systems separated by software instead of an air gap. The end result could be quite damaging to security.

Fortunately, the picture is not all bad. When designed and deployed properly, virtualization can be very useful for security and, a related topic, overall system management. Getting it right is not always trivial. As part of this project, we consider what it means to get it right, and suggest some strategies for getting the most security benefit from a virtualization platform. The key goal here is to ensure sufficient isolation between virtual machines to prevent malware from crossing this boundary. Since the area of cloud security is vast and lacking to standards clearly defined, cloud security needs to understand the dangers and compare them with benefits [61]. For instance, the database service which is provided by Amazon S3 is lacking flexible authorisation granular security [60] .

2.12. Security Components

2.12.1. Encryption

To ensure the information privacy hosted in cloud, this information might be encrypted which can be decrypted at client level via key. This is reliable if the data can be quickly decrypted at the level of client, this require high processing power. The multi-core processors will lead to provide integration of information [63].Researchers of IBM have cracked a problem of homomorphism encryption that has led to enhanced cloud computing via enabling providers to analyse data without compromising them [62]. In reality, even the service providers are unable to distribute high levels of security. For example, both HTTPS and HTTP can be used via Google services. Although via default service using HTTPS that is SSL encrypted, it can sometimes go back to HTTP which is unencrypted. This leads attackers to observe traffic of network and capture the credentials of a specific user. Whilst Google is not allowed to use https by default, but the setting of cloud may be changed to use https [64].

2.12.2. Intrusion Detection/prevention Systems

Providing security of cloud computing requires more than authentication using confidentiality and passwords throughout data transmission Vieira and Schulter suggested a solution of intrusion detection in cloud computing[65]. The solution includes two kinds of analysis which was knowledge analysis and behavioural analysis. In knowledge analysis security policy attack and violations patterns were analysed to prevent or detect intrusion. In behavioural analysis, the data taking out techniques were used to a server deviation of behaviour or recognize expected behavioural.

2.12.3. Antivirus

Antivirus scanning is one of many types of security components, it can be done to reduce the hazard of malicious activities on cloud computing. It is an expensive operation, but which has the benefit of many advantages. Furthermore, the power of cloud computing is more than anti-virus techniques which can be employed and lead to be more efficient. The challenge at this point is linking the gap amongst virus signature release and the threat release [66]. Though the operation of antivirus scanning is expensive, it should be repeated by the release of new virus signatures.

2.12.4. Firewall

Firewall might be implemented as a virtual machine image which running in hardware level "out of band" or in its own processing partition, firewall management channels [67].

2.13 Security Threat

The communication among consumers and cloud services can be secured by using SSL. Usually users ignore the warning which can be occurring via attackers. Google has illustrated such sort of exploitation in cloud base services. Other than that, a fault of indexing system design in Zoho has caused security vulnerability where one client can read other client's documents. Also there are another CSRF and XSS attacks which were successful to make cloud vulnerable to attack [44].

In SaaS model of cloud computing, the developer should suppose that intruders have complete access to the client. Anyone can buy the software from cloud which lack source codes, they can be access to binaries via exploiting the vulnerabilities. So there should be a verification method to verify a client needs earlier than execution [68].

2.15. Authentication and Access

There are diverse authentication mechanisms for various services. The most commonly used methods are User Request Token, Open Authd, and open id. Usually Open Authd, and open id mechanism are in normal PCs. Google and Yahoo utilize User Request Token method for authentication while Amazon AWS utilizes a custom mechanism which similar to the open Auth and open id mechanism, in addition, the program using HMAC-SHA1 algorithm [69].2FA (Two Factor Authentication) is another authentication mechanism that needs two proof or identities which the user knows (PIN and Password) (Mobile Phone, Smartcard, Hardware Token). While this mechanism is more secure than other sorts of authentication, smartcards or handling tokens could potentially be a load to users. In this scenario, smart phones or mobile phones can act as a proof only if software makes tokens similar to the hardware tokens that are installed on it [68].

2.16. Data Security

The organisation or individual using cloud computing must maintain their data by sponsorship even if the providers back up data for the organisation. This will help incessant access to their own data even at the great situations such as a disaster at data centres or data providers going bankrupt etc [45]. Mowbray has proposed a consumer based privacy manager to eradicate the fear of the data loss or leakage privacy of cloud computing. This project has presented a scenario of salesforce.com that can endure a security threat; diverse ways of stealing sales data where intruder information can gain knowledge that is based on the unencrypted data. The threats involve the set of personal information and getting unsuitable access to the information. On this scenario a collection of requirements was derived that contain sensitive data and the minimization of personal data which maximised the security protection of data in cloud. The general architecture of client based privacy of data manager has been depicted [70].Other than that, Wang suggests that the model of public verifiability is compulsory and can be used where the third party audits the data with no central user's time to assure the data security [71].

2.17. Tempting Target for Cybercrime

The internet is always a target of attack and malicious activities. The cloud computing proffers a target for cybercrime for diverse reasons. To maintain of data integrity, several providers want 100% of client's data to be located in cloud computing that means if it is compromised 100% of data is available to attackers. That leads providers such as Amazon and Google to have existing infrastructures to redirect cyber attacks, but this is not the case for all providers. The cloud architecture connects with multiple compromise and entities where any of the weakest links could cooperation with all another linked entities [1]. The cloud computing community is watching services analysis of the cloud activities constantly to prevent and detect any newly malicious activities and injected viruses. Active participation of several organisations and individuals in this community will aid them to restrain the malicious activities which are more effective [8].

2.18. Benefit to Risk Ratio

Viega intrduces a scenario of a software industry where developers would not have great control of IT infrastrucure[68]. In this scenario IaaS would take advantages from the communiction among local machine and the cloud is encrypted so that man in the centre cannot stop the traffic. This would be a vast cost saving for the business. The attackers of SaaS model have less information i.e., the software binaries is quite justified inhaving an unassuming application security program. The cost effective for several organisations is to rent someone to do cheap testing of security and skip the cost of training developers on cloud computing security to review their work and best practices [68].

2.19. Legal Issues IT

Industry's current focus on cloud computing payable to a global recession and the 'credit crunch'. The solution legal issues of cloud computing with regard to sourcing arrangements are DPA (Data Protection Act 1998), tasks of database rights and confidentiality. For Example, in the technique ofstoring a large volume of data in cloud, the servers could extend across the world. It is arguable whether the information agree actually can be given in this unclear situation. Correspondingly there are intricacies over confidentiality and database rights as well [77].

It is possible to use cloud computing in the UK with a low risk manner and and a legal compliant. This would need modification in the operating model that could corrode the benefits of cloud computing only if not considered at early stage and if operational mangement or contractual is not accurately adopted, it could be important to raise of operational risk [77].

Properties	Amazon EC2	Google AppEngine	Microsoft Azure	Manjrasoft Aneka
Service Type	IaaS	IaaS – PaaS	IaaS – PaaS	PaaS
Support for (value offer)	Compute/Storage	Compute(web applications)	Compute/Storage	Compute
Value Added Provider	Yes	Yes	Yes	Yes
User access Interface	Web APIs and Command Line Tools	Web APIs and Command Line Tools	Azure Web Portal	Web APIs, Custom GUI
Virtualization	OS on Xen Hypervisor	Application Container	Service Container	Service Container
Platform (OS & runtime)	Linux, Windows	Linux	.NET on Windows	.NET/Mono on Windows, Linux, MacOS X
Deployment Model	Customizable VM	Web apps (Python, Java, JRuby)	Azure Services	Applications (C#, C++, VB, ...)
If PaaS, ability to deploy on 3rd party IaaS	N.A.	No	No	Yes

Soures: [107]
Table (2):Cloud Computing Solutions Feature Comparison

2.20. NEW Trend

The core issue of the cloud is that with the advent, the provider of cloud has some control of users' data. To sort this issue there are many solutions that aim to provide tools which support the recent capabilities of the cloud, although limiting cloud provider control of data, also enabling users to benefit from cloud data during enhanced business [82].

2.20.1. Information-centric security

In order to extend control to data of the cloud for any enterprises, that lead to shifting protecting data from the outside (applications and system which use the data) to protecting data within. This approach of protecting data and information itself called information-centric security [78, 79,80] differently terminology used. This self-protection needs intelligence to be put into the data itself. Data requires being self defending and describing, regardless of its environment. Consequence data should be encrypted and packaged with a tradition policy, and after being accessed, data has to consult its policy and try to recreate a secure environment by revealing itself and using virtualization but only if the environment is verified as dependable (using Trusted Computing). Information-centric security is extension of the trend toward stronger, finer, and further usable data protection [81].

2.20.2. High-Assurance Remote Server Attestation

The lacking of transparency is disappointing to businesses moving their data into the cloud. Data owners hope to know how their data is being handled at the cloud, and guarantee their data is not being leaked or abused. Clients should be satisfied with cloud providers by using manual auditing procedures such as that of SAS-70. An approach of this problem is based on Trusted Computing. Imagine if a trusted monitor installed at a layer of the cloud server can monitor the operations of the cloud server. The trusted monitor can provide the data owner, in this case that certain access policies have not been ignored. To ensure integrity of the monitor, in addition Trusted Computing allows secure bootstrapping of monitor to run beside applications and operating system. This monitor can enforce perform monitoring tasks and access control policies to produce a “proof of compliance” “statement of compliance” produced via the monitor. Then the data owner gets proof of compliance that leads to verifying that the cloud server has obeyed the access control policies and correct monitor code is run [81, 82].

2.20.3. Privacy-Enhanced Business Intelligence

A diverse approach to retain control of data is to require the encryption of all cloud data. The limit of encryption data use is a problem. Typically indexing and searching the data becomes problematic. For instance, when the data stored in clear text can efficiently search a document by specifying a keyword. It is unfeasible to do it with traditional encryption schemes. In this case cryptography may offer new tools to solve these problems. Cryptographers have currently invented multipurpose encryption schemes which allow computation and operation on the cipher text. For example, searchable encryption allows the data owner to calculate a capability from its secret key (see [87], [82], [86], [85], and [83]). A capability encodes a search enquiry, which leads cloud to use this capability to choose which documents match the search enquiry. Another basic cryptographic such as Private Information Retrieval (PIR) [84] and homomorphic encryption [88] perform computations of encrypted data exclusive of decrypting. So these techniques of cryptographic nature might open up new potential ways of cloud computing security.

Although a large amount of research is needed to make cryptographic tools more sufficiently practical for cloud, they present a good opportunity for a clear differentiator for cloud since these protocols allowed users of cloud to benefit from other data in a controlled manner. In particular, encrypted data allows irregularity detection which is important from a business intelligence standpoint. For example, a cloud payroll service may provide total data about execution time of payroll that allows clients to identify inefficiencies of their own processes with the agreement of participants. Furthermore, if the cloud service provider is made powerful with some ability to search the encrypted data, the propagation of cloud data that lead to enable better insider threat detection (e.g. detecting activities of user outside of the norm),also better data loss prevention (DLP) (e.g. throughout detecting strange content).[82].Regarding the privacy aspect of cloud computing, it can be applied cryptography to offer tools to other security problems of cloud. For example, proofs of irretrievability (e.g., [90], [89]) the storage server can illustrate a packed together proof which exactly stores all client’s data.

Chapter 3: Research Methodology

Objectives to:

A. Propose and Develop the Design of Research Methods

B. Provide the Development of Research Tools

C. Investigate the Possibility of Data Collection and Data Analysis

3.1. Introduction

The aim of this study is to collect enough quantitative information on cloud computing security issues to find out a clear information gap between different issues, and about how it is developing and people's opinions of it to provide some understanding in to the state of certain aspects of cloud computing security issues. This chapter presents the research objectives for the study and describes the methodology employed which can be understood as a set of procedures or guidelines in problem solving, development is well arranged and make sure that the aim of project is achieved. The following activities have been carried out for this project:

- Design of project methods
- Development of project research tools
- Data Collection
- Data Analysis and Discussion of Results
- Conclusions and recommendations for future work

Dissertation activities will be described in details as following.

3.2. Development of project research tools

In order to collect data on the cloud computing security, one technique have been used in the current project, which is a questionnaire that has been used to fill a clear information gap about how it is developed and people's perspectives of it in different issues to make sure of CIA (Confidentiality, Integrity and Availability) of the information, (see Appendix 1). The questionnaire is not a statistical analysis of developments, but aims to collect enough quantitative information to make comparisons between different issues to provide some understanding into the state of certain problems of cloud computing in security.

The main source shaped the content of the questionnaire used in the present study came from reviewing the User's views on cloud computing security carried out by Curtis+ Cartwright for

the cloud computing for research [98]. This study has been very carefully structured. Topics have been selected on the starting point of issues identified as of particular interest to target this project. Questions were prepared in consultation with experts in cloud computing for research and issues.

The high return rate of questionnaires (75 per cent) were immediately analysed to find clear information about how it is developed and people's opinions of cloud computing security in different issues to make sure of CIA (Confidentiality, Integrity and Availability) of the information.

3.3. What techniques were reviewed?

The primary research was used to dispute or confirm results with local trends. There are several types of primary research which could be used such as:

Analysis*:* include collecting data and organizing it in some manner based on the criteria which develop. It is useful to find some pattern or trend.

Interview: Interview face to face or as a small group question and answer session. It will provide a set of information from individuals or a small number of people and this is useful to get knowledgeable opinion or an expert on a subject.

Survey: Survey is a form of questioning that is more inflexible than interviews which include large groups of people. It will provide a limited quantity of information from a large group of people which is useful to know how the population thinks.

Observation: involves taking notes about events in the world. This provides the insight about specific occurrences or people or locales, which is useful to learn more about an event without the viewpoint of an interview.

Questionnaire: is a form of questioning that is more flexible than interview which is used for gathering specific information from people.

3.4. Why they were not used

The questionnaires were picked as the main primary research technique of this dissertation, Because the primary fact it is the best known of the research instruments used for gathering specific information from people to support another preliminary research technique. Secondary fact, another technique such as analysis, interview, survey, observation all of these technique are not suitable for this research topic, and short time of Master dissertation. For example an interview is not easy to find free time with professional people to do an interview and the arrangement for many people to do an interview takes a long time, which is not suitable for a Master project. Although this is useful to get knowledgeable opinion or an expert on a topic, and for observation technique the student is not able to do this because the issues of security of cloud computing might occur in Virtualisation Machine or vendor which spread to different places in the world, and the student would be unaware of where the data is, what processes are running or where the data is stored. To do that requires 24/7 observation from the team, this task takes a long time and needs high level experience. One person may not be able to do that, also no body know when or where problems may happen in a thesis. In addition, this topic is relatively new and few publications exist on cloud computing security issues and do not provide enough information to do analysis techniques as primary research. So that is why the questionnaire was chosen as primary research to confirm or dispute results with local trends and enhance literature review of this topic.

3.5. Why questionnaire picked as the main primary research technique

3.5.1. Advantages of Questionnaire

Questionnaires are the best known of the research tools used for gathering specific information from people, and they can be used in conjunction with other techniques such as the literature review as preliminary research. Beside there are many advantages to use questionnaire that is why questionnaire picked as the main primary research technique. Some advantages of questionnaire are below:

1- Questionnaire is familiar to the majority people. Practically everyone has had some experience and in general does not make people apprehensive.

2- Questionnaire is very cost effective when compared to another methodology such as face-to-face interviews or samples or observations. This is true for studies including different geographic areas and large sample sizes. Questionnaire becomes more cost effective for increase of research questions as well.

3- Questionnaire is easy to analyze. Data entry can be simply done with various computer software packages.

4- Questionnaire reduces bias. There is uniform question and without middle-man bias. The researcher's own opinions with no influence the respondent to answer questions in a confident manner. There are no visual or verbal evidences to influence the respondent.

5- Questionnaire is less intrusive than face-to-face or telephone surveys. When a respondent receives a questionnaire by mail, it is easy to complete the questionnaire in his own time rather than other research methods, the respondent is not interrupted by the research tool.

3.5.2. Disadvantages of Questionnaire

1- One major disadvantage of questionnaires is the possibility of small response rates, which is not good of statistical analysis. That leads to reduce the confidence in the results. The rate of response varies widely from one questionnaire to another (10% - 90%).

2- Another disadvantage of questionnaires is the inability to explore responses.

3- Questionnaire does not include any visual cues. The lack of personal contact will lead to different effects depending on the sort of information being requested. But a questionnaire requesting accurate information that will possibly not be affected via the lack of personal contact. A questionnaire probing sensitive attitudes or issues may be lead to difficulties.

4- When the questionnaire is completed and returned via mail, it can be assumed that the respondent is the same person who completes the questionnaire. In fact this may not be the case. But numerous times questionnaires get handed to other peoples for

completion. For a diversity of reasons, the respondent may not be the same person who answered the questionnaire. It is a confusing error in questionnaires.

5- Finally, questionnaires are not suited or do not work for a few people because of problems of reading skill. People avoid written questionnaires for misuse.

3.6. Brief discussion on questionnaire design

For ethical reasons, at the early planning stage it was decided that permission would always be obtained in writing from all study participants whose details and responses were recorded, to use the data gathered for reporting in this project. The questionnaire of this dissertation used a mixture of different methods, which include e-mail and telephone communications or visits and was chosen to clarify broad aims of the main study. The task of questionnaire design is not an easy matter and underlines the idea about this research. So the main aim of the questionnaire of this dissertation is to a) get as many responses as possible b) to be accurate and usable. To maximise the rate of response, the questions of this questionnaire designed so that the most important items were in the first half of questionnaire; this will ensure getting the most significant data from non finishers, because many people do not complete questionnaires. In general the questionnaire start with easy questions to encourages respondents to carry on with it. The questions ordered from the general to the particular and from factual to abstract questions. The questionnaire was sent and received by email that made clear how and when responses must be returned and also includes what the study is about, and who is running it.

3.6.1. Why the questions were chosen

There are different types of questions that can be used in questionnaires. Such as Open Format Questions and Close Format Questions, the questions of Open Format Questions that give audience or responses an opportunity to express their opinions. Closed format questions include

multiple choice answers. These multiple choices could be in even or odd numbers. So the questions of this questionnaire were designed as close format questions such as Dichotomous questions that offering two answer choices(Yes or No), Multiple choice s type of questions offering three or more answer options, and that can easily calculate statistical data and percentages. Preliminary analysis can also be performed with ease. Also this type can be asked to different groups at different intervals. In addition the main key of these questions is getting the accurate data to support the result of the literature review depends on the questions which are asked relevant to objectives and the research question of cloud computing security issues.

3.6.2. Eliminate those questions on the questionnaire which are not relevant to the research question

The majority of these questions as demonstrated in Appendex1 were relevant to the research question and objectives of this dissertation, only two of these questions were not related to the research question. the first question: How much experience do you have with Cloud computing?, the answer of this question did not relate to the objective and research question of cloud computing security issues, the answer just demonstrated the level of experience of cloud computing as new term without mention of security and security issues of cloud computing. This question should be eliminated on the questionnaire. Also question number four: What are your reasons for using Cloud Computing? The answer of this question just shows which big reasons lead people to use cloud computing without any indication of the security of cloud computing, although this question may be easy to answer and encourage people to answer sequence questions. It was not significant for this project, that is why it must be eliminated on the questionnaire.

3.6.3. Demonstrate how the primary research adds and validates the conclusions from the literature review

The result of primary research adds good evidence and enhances the conclusion of the literature review, so both the questionnaire and literature review support each other about which is the

best solution for information security on cloud computing by ensuring all of these confidentiality, integrity, and availability to improve cloud security.

3.7. Data Collection

Planning and arrangement of visits and contacts to different sites that were involved in this study. The purpose is to collect data of interest to specialists and researchers in cloud computing security issues .The project chose three approaches to fill the questionnaires, which depended on the people and where they are. The first approach was contacted with several members of research lab by an e-mail and was conducted with many higher education teachers and their ICT class tutors who are interested (filled and sent back again). Each questionnaire was send by email in, Libya, Australia and UK. Finally, phone calls were made to clarify some unclear questions.

In addition, the project chose the distribution approach of copies of printed questionnaire was conducted with one department in De Montfort University at Software Technology Research Laboratory (STRL). It was a to be filled by pen printed copy of questionnaire to avoid intimidating the group members as a tool for gathering this type of information. This approach was very useful to get close with the responses and easy to get the data. Telephone approach as well has been used in some cases when needed to gather the information or clarify unclear questions.

3.8. Data Analysis and Discussion of Results

In order to understand the security issues on cloud computing, the project focuses on understanding the existing views of cloud security on technology usage and information

requirements on different aspects of cloud computing by analysis of the questionnaire that was laid out in five sections as follows:

1 Users' skills for cloud computing: the extent to which users felt equipped to develop and use cloud computing provided will be examined;

2 Issues facing of cloud computing usage: which provides views of issues that face user practitioners on technology usage and information requirements;

3 Solution of cloud computing: protocols of developing of cloud computing techniques and tools support will be looked at;

The goal of the client needs analysis to find out the requirements of the user. In many projects with heavy investments in technology and learning materials, the user needs analysis as a well identified phase in a project lifecycle and the results of the analysis strongly influence the subsequent development of the process. Therefore, this project outlines a number of respondents and identifies them by organization type. The questionnaires received 25 responses from the 30 questionnaires that have been sent and together they build up a picture of development in some key areas of cloud computing security.

3.9. Conclusions and recommendations for future work

The analysis of the questionnaire on different aspects of cloud computing will be allowed to draw the final conclusion to fill a clear information gap about how it is developing and people's opinions of it in security issues and what is the difference between them. Then the results of this study will be allowed for formulation of a number of future works and recommendations for main study.

Chapter 4: Data Analysis and Discussion of Results for Future Work

Objectives to:

A. Provide the Summary 0f Present Study

B. Describe the Experimental Investigation Conducted

C. Present the Results With the Contributions Made in this Research

D. Discuss Directions for Future Work.

4.1. Introduction

This chapter presents the analyses of the study in cloud computing security issues using relevant quotations to be applied to the results. This chapter analyses responses on different aspects of cloud computing each survey contains many items in different parts (UK, Libya, and Australia side).

4.1. Users' skills for cloud computing

Which will be examined the extent to which users felt equipped to develop and use cloud computing provided.

4.1.1. How much experience do you have with Cloud computing?

□None □Minimal □Moderate □High

Table 4.1: Experience of cloud computing

Answer options	None	Minimal	Moderate	High
Response count	10	8	5	2
Response percent	40%	32%	20%	8%

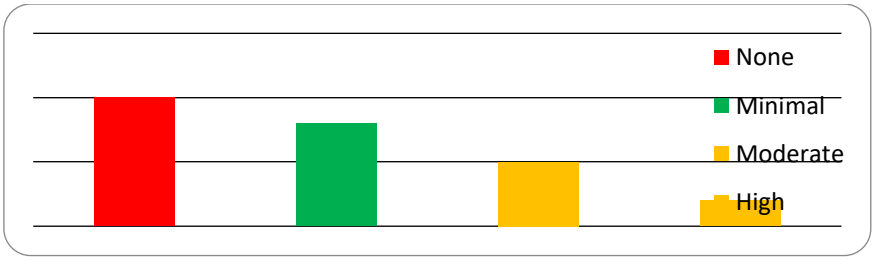


Figure 4.1: Experience of cloud computing

Respondents had between no experiences to two years experience by using AWS. The majority of respondents as shown in the chart had absolutely zero previous experience with Cloud computing, the reason for that because cloud computing it is still new term of technology. Some of them had low experience might be just reading about the diverse offerings from Amazon or another cloud or hear about it or attending one of their events. Only a small number of respondents had good experience about cloud computing. STRL are members of the Advanced Computing for Software Engineering Department here at De Montfort University, who have experience with Cloud computing especially with Amazon Web Services. This was critical to getting up as they were familiar with the AWS interface and they know what to expect in terms of system performance, behaviour, and even provided software tools to configure improve virtual cluster.

4.1.2. Do you think Cloud computing is beneficial?

Table 4.2: Use of cloud computing

Answer options	Yes	No	Other
Response count	17	2	5
Response percent	68%	8%	20%

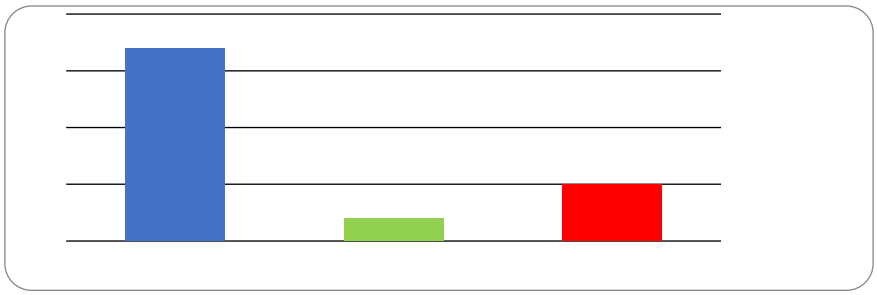


Figure 4.2: Use of cloud computing

The answer of this question is shown in the chart. Several interesting responses found cloud computing very useful because cloud has many benefits. In fact the majority of respondents decided cloud was very useful if they have experience with cloud or have good background. On the other hand some respondents decided cloud was not useful, and some other responses choose the last option cloud who had no idea about cloud computing.

4.1.3.What difficulties have you encountered when using the Cloud (for example Google documents)?

□ Cost of using the service □Accessibility □Services □Usability

Table 4.3: Biggest difficulties of cloud computing

Answer options	Cost	Accessibility	Services	Usability
Response count	2	7	3	12
Response percent	8%	28%	12%	48%

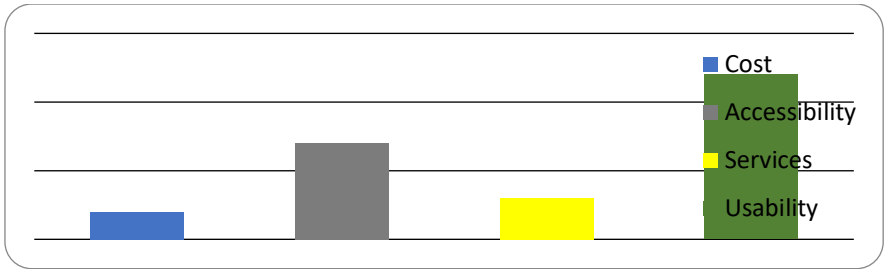


Figure 4.3: Biggest difficulties of cloud computing

The majority of respondents found getting started was a difficulty, though others particularly indicated it was easy to get up and running over cloud Amazon. Other barriers mentioned involve: cost, compared to accessibility, and services. “The biggest difficulty was possibly figuring out how to configure a computer to connect to EC2and to set up access credentials. But, it was not in fact that difficult. I found good instructions online after that I found a couple of useful extensions on the Firefox browser which made it easy to connect to S3 and EC2 to manage and launch instantly. In general, I think that it took about one day”. Only some of respondents found it difficult to access this cloud and to use the services which are offered from this cloud. The result of the survey as shown in the figure 4.3.

4.2. Issues facing cloud computing usage:

This provides views of issues that are facing user practitioners on technology usage and information requirements;

4.2.1. What are your reasons for using Cloud Computing?

Table 4.4: Reasons behind cloud computing

Answer options	Response count	Response percent
Increasing capacity of computing and business performance	4	16%
Avoiding capital expenditure in SW, HW, IS, IT	9	36%
Developing business into the Cloud	3	12%
Adding redundancy to increase resilience and availability	2	4%
Scalability and Flexibility of IT resources	6	24%
others	5	20%

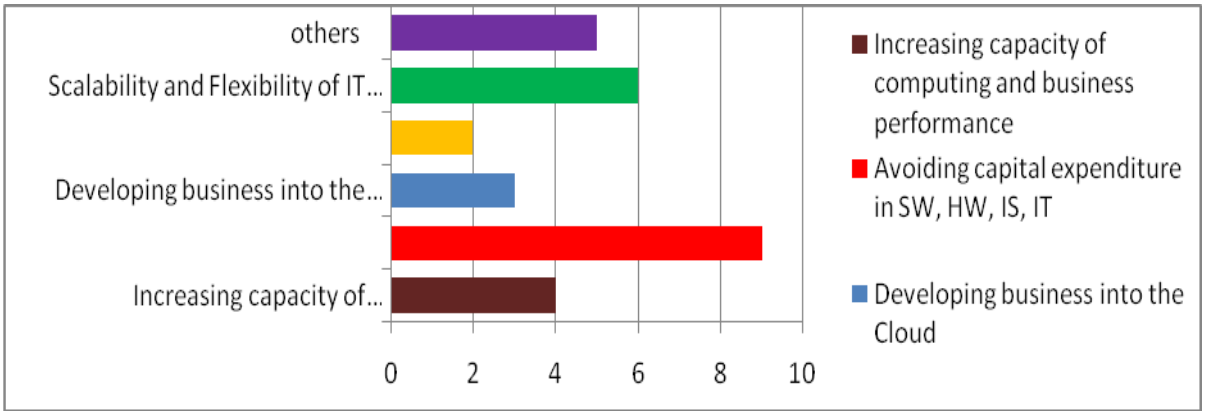


Figure 4.4: Reasons behind cloud computing

Numerous interesting responses were received in answer to this question. The majority of responses choose avoiding capital expenditure in software, hardware, and IT to support information security via outsourcing services/ infrastructure/platforms. Various responses selected Scalability and Flexibility of IT resources, and increasing capacity of computing and business, other than deciding on adding redundancy to increase resilience and availability. So the answer was different regarding background and motivation to deal with cloud computing.

4.2.2. What are your main concerns for cloud computing?

Table 4.5: Main concerns of cloud computing

Answer options	Not important	important	very important	Response count
Privacy	0	10	14	24
Availability of data and/or services	1	8	14	23
Integrity of data and/or services	1	9	13	23
Confidentiality of shared data	2	9	12	23
Loss of control of data and/or services	5	10	10	25
Inconsistency between regulations and trans national laws	2	10	10	22
Repudiation	4	5	11	

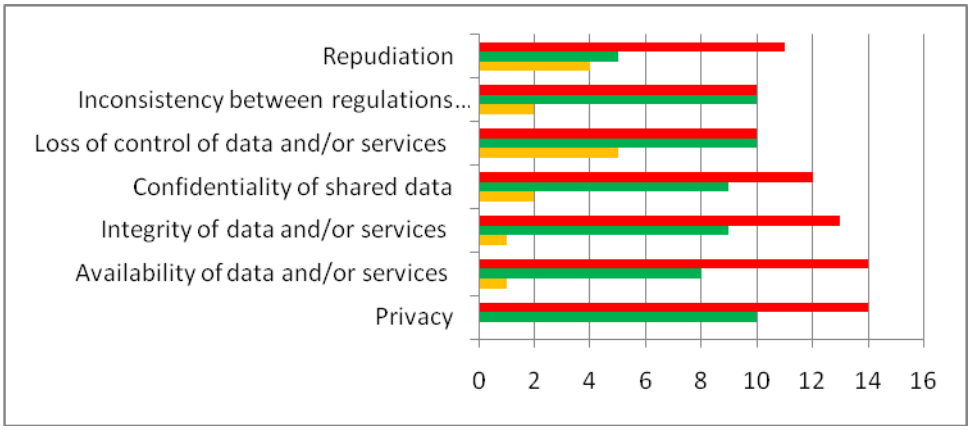


Figure 4.5: Main concerns of cloud computing

The majority of response focused their concerns in Availability of data and/or services and privacy. In order the integrity of data and/or services, and confidentiality of shared data as of most concern. Other options of answer take different numbers as shown in the Figure 4.5.

4.2.3. Which solution do you believe is the most suitable for ensuring confidentiality, integrity and availability of Cloud Computing?

Table 4.6: Good solution of cloud computing

Answer options	Response count	Response percent
Private cloud (owned, managed internally)	3	12%
public (owned, managed via an unrelated business)	4	16%
Federation of clouds provided by various sources (partner, private, etc).	9	36%
Partner cloud (owned, managed via trusted)	8	32%
Other	1	4%

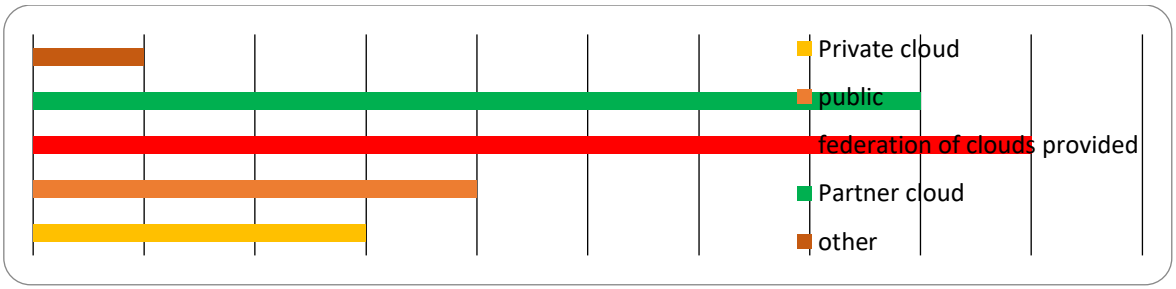


Figure 4.6: Good solution of cloud computing

Several of the responses considered the federation of clouds provided by various sources (partner, private, etc) as a good solution and suitable for a CIA. In order the partner cloud (owned, managed via trusted) as a good solution as well, another answer selected different sectors such as public and private cloud as shown in the Figure 4.6.

4.3. Solution of cloud computing security issues

This will be looked at protocols of developing of cloud computing techniques and tools support;

4.3.1. Do you think current level of security is good enough for cloud computing?

□No □Yes □other

Table 4.7: Security good enough for cloud computing

Answer options	No	yes	other
Response count	18	5	2
Response percent	72%	20%	8%

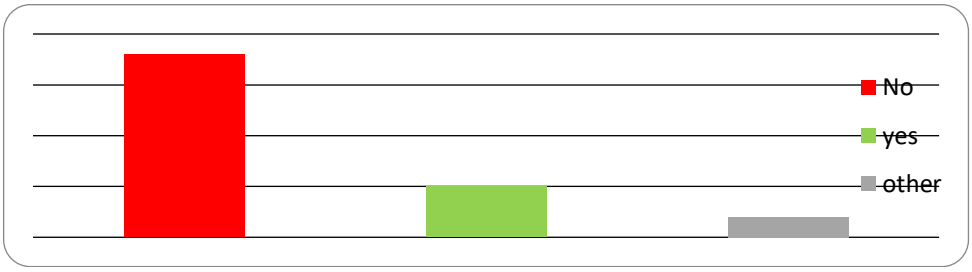


Figure 4.7: Security good enough for cloud computing

The majority of responses decided that the security of cloud computing is not good enough , that is mean the security need more improve to make user more satisfy about security to protect their sensitive information, some of them thinking the security good , the result of this question appear it the Figure 4.7.

4.3.2. Do you think it is possible to make cloud available 100% of the time?

Table 4.8: possibility to make cloud available 100%

Answer options	No	Yes	Other
Response count	11	8	6
Response percent	44%	32%	24%

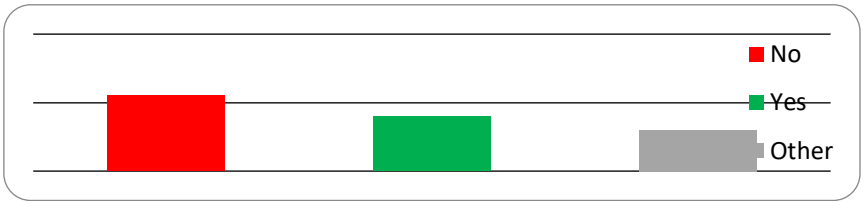


Figure 4.8: possibility to make cloud available 100%

In fact the result of this question came as the research expected; the availability of cloud computing is impossible to become 100%. Some respondents decided yes cloud computing might become available as the Figure 4.8 illustrates this result.

4.3.3. Overall, what do you think of the integrity of cloud computing (the ability of the Cloud to manage risks that affect the accuracy of information managed)?

□ Unsatisfactory □ Satisfactory □ Excellent

Table 4.9: Is cloud computing security integrity or no?

Answer options	Response count	Response percent
satisfactory	6	24%
Unsatisfactory	15	60%
Excellent	9	36%

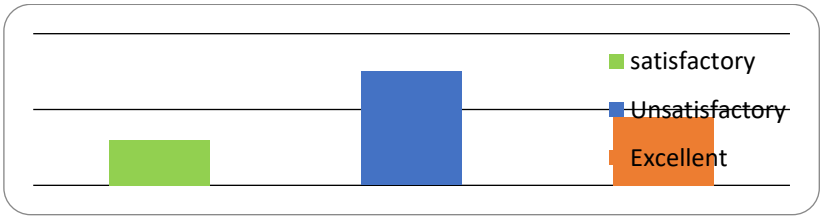


Figure 4.9: Is cloud computing security integrity or no?

The big number of responses of this question choose the cloud computing security did not have integrity, some of them selected yes cloud security does have integrity, others no idea about integrity. The Figure 4.9 shows this result.

4.3.4. Which one of these cryptographic techniques could improve the confidentiality of cloud computing?

□ Homomorphic encryption

□ Private information Retrieval

□ Other

Table 4.10: Cryptographic techniques of cloud computing

Answer options	Response count	Response percent
Homomorphic encryption	12	48%
Private information Retrieval	9	36%
Other	4	16%

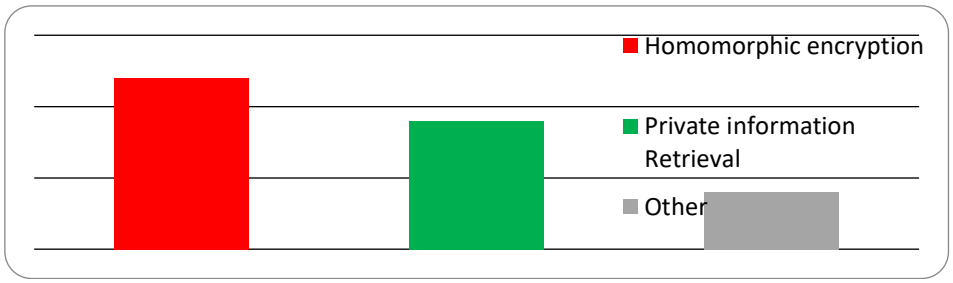


Figure 4.10: Cryptographic techniques of cloud computing

The Figure 4.10 shows the result of this question, several of responses thinking one of the most cryptographic techniques which could be a good solution of confidentiality of cloud computing was homomorphic encryption that could be make confidentiality of cloud good enough. Some of them prefer the private information retrieval as good cryptographic techniques improve confidentiality of cloud computing security, another response indicated no idea.

4.4. Conclusion

In conclusion of thisdissertation , it is apparent that the cloud computing security itself is in evolving stage and the security implications are not complete. Still the leaders of cloud computing security providers such as Google, Amazon,etc are facing many security issues and are yet to stabilise. To achieve complete solution for legal issues is still an unsolved question. With this stage of issues in cloud computing security, a decision to adopt cloud security in an organisation should be made only based on the benefits to risk ratio.The techniques of SLA coprative with cyrpotghres and trusted computing work together will find these as a good solution of security issues and will improve the security of cloud computing.

4.5. Recommendations for Future Work

The results of this study have led the researcher to formulate a number of future work and recommendations for main study. The techniqes of SLA coprative with cyrpotghres and trusted computing work together are a good solution of security issues and will improve the security of cloud computing. These are:

1) Working with tools of Service Level Agreement (SLA) to support security of cloud computing , and

2) Work Trusted Computing with cyrpotghres will increas integrity and confidentiality

References

[1] Kaufman, L. M, ”Data Security in the World of Cloud Computing.” *IEEE Security and Privacy*, vol 7, no 4, pp.61-64, 2009.

[2] Kim, W. “Cloud Computing :Today and Tomorrow.”*Journal of object technology,* vol 8, no 1, pp.65-72, 2009

[3] Grossman, R. ”The Case for Cloud Computing.” *ITPROFESSIONAL*, vol 11, no 2, pp. 23-27,2009.

[4] Mell, P. & Grance, T. *“*The NIST definition of cloud computing.” Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc 2009.

[5] Leavitt, N. “Is cloud computing really ready for prime time?” *Computer,* vol *42* ,no 1, pp.15-25, 2009 Retrieved from IEEE Xplore Digital Library: http://ieeexplore .ieee.org. libproxy. uoregon.edu /stamp/stamp.jsp?arnumber=04755149

[6] Erdogmus, H. (2009). “Cloud Computing: Does nirvana hide behind the nebula?” *IEEE Software*, vol *26,* no 2,pp. 4-6, 2009. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee .org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04786942

[7] Leavitt, N. “Is cloud computing really ready for prime time?” *Computer* ,vol 42, no 1,pp. 15-25, 2009 Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04755149

[8] Hawthorn, N. “Finding Security in the Cloud.”*Computer Fraud & Security* vol 10, pp. 19-20.2009.

[9] Ryan, V. “A place in the cloud.” *CFO,* vol *24,* no 8,pp. 31-35.2008

[10] Rash, W. “Is cloud computing secure? Prove it.” *eWeek,* vol *26,* no 16),pp. 8-10, 2009.

[11] Hayes, B. “Cloud computing.” *Communications of the ACM,* vol *51,* no.7,pp. 9-11, 2008.

[12] ISACA. (2009). “Cloud Computing: Business benefits with security, governance and assurance perspectives*”.*

[13] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009) “ Above the Clouds: A Berkeley view of cloud computing.”

[14] Gatewood, B. "Clouds on the information horizon: How to avoid the storm." *Information Management (15352897)*, vol *43*, no 4,pp. 32-36, 2009

[15] Peter Mell, Tim Grance , "Effectively and Securely Using the Cloud Computing Paradigm" *NIST, Information Technology Laboratory,* vol 10, pp. 7, 2009

[16] Wyld, D. (2009). " Moving to the cloud: an introduction to cloud computing in government E-Government Series. : IBM Center for the Business of Government"

[17] Youseff, L., Butrico, M., & Da Silva, D. (2008). "Toward a unified ontology of cloudcomputing." *Paper presented at The Grid Computing Environments Workshop* at GCE2008, Austin, Texas.

[18] Hand, E. (2007) "Head in the clouds." *Nature,* vol 449,pp. 963.

[19] Anderson, C. (2008). "The end of theory: The data deluge makes the scientific method obsolete." *Wired* (February 27, 2009 Retrieved June 12, 2009 from http://www.wired.com/science/discoveries/magazine/16-07/pb_theory.

[21] Beizer, D. (2009). "USA.gov will move to cloud computing" Retrieved April 15, 2009, from http://www.fcw.com/Articles/2009/02/23/USAgov-moves-to-the-cloud.aspx.

[22]Obama, B. (2009). "January 21" Retrieved May 1, 2009, fromhttp://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.

[23] Kubicek, H. (2008). "Next generation FoI between information management and Web 2.0." Paper presented at the 2008 *International Conference on Digital Government Research*,Montreal, QC.

[24] Burroughs, J. M.(2009) "What users want: assessing government informationpreferences to drive information services." *Government Information Quarterly*, vol 26,pp.203−218,.

[25] Bertot, J., Jaeger, P. T., Shuler, J. A., Simmons, S. N., & Grimes, J. M. (2010) "Reconciling government documents and e-Government: Government information in policy,librarianship, and education." *Government Information Quarterly*, vol 26, pp. 433−436.

[26] Dikaiakos, M., D. Katsaros, et al. (2009) “Cloud computing: Distributed Internet Computing for IT and Scinentific Research.” *IEEE Internet Computing* vol 13, no5, pp. 10-13.

[27] Weiss, A. (2007). “Computing in the Clouds.” *COMPUTING* pp.16.

[28] Kaufman, L. M..(2009) “ Data Security in the World of Cloud Computing.” *IEEE Security and Privacy* vol 7, no 4, pp. 61-64.

[29] D. And M. Creeger. (2009)“computing 2cloud computing: An Overview.”*Distributed Computing* vol 7 pp.5.

[30] William, “7 things you should know about the cloud computing” *EDUCAUSE*, available from: http://creative commons.org/Licenses/by.nc.nd/3.0/.

[31] Aneka X. Chu et al. (2007): “Next-generation enterprise grid platform for e-science and e-business applications.” *Proceedings of the 3rd IEEE International Conference on e-Science and Grid Computing*.

[32] J. E. Smith and R. Nair. (2005) *Virtual Machines: Versatile platforms for systems and processes.*

[33] R. Buyya and M. Murshed. (2002) “GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing.”*Concurrency and Computation: Practice and Experience*, vol 14, pp.13-15), Wiley Press, Nov.-Dec.

[34] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I.Brandic.(2009) “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.” *Future Generation Computer Systems*, vol 25 no 6, pp. 599-616, Elsevier Science, Amsterdam, The Netherlands, June.

[35] R. Buyya1, R. Ranjan2 and R. N. Calheiros, “Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities”

[36] Cloud Security Alliance . “Security Guidance for Critical Areas of Focus in cloud computing.”Retrieved Nov 25, 2009, from http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[37] A. Sharma ,and K.Shrivastava "Privacy – Reason Enough to Reconsider a Cloud Service" 2009

[38] A Security Analysis of Cloud Computing: (http://cloudcomputing.syson.com/ node/ 1203943

[39] Cloud Security Questions? Here are some answers (http://cloudcomputing.sys-con.com/node/1330353)

[40] Trusted Computing Group Cloud Computing and Security A Natural Match www.trustedcomputinggroup.org April 2010

[41] T.J Betcher, "Cloud Computing: Key IT related Risks and Mitigation Strategies for Consideration by IT Security Practitioners". Feb 2010

[42] Chow et al., "Cloud Computing: Outsourcing Computation without Outsourcing Control", *1stACM* Cloud Computing Security Workshop, November 2009.

[43] F. Swiderski and W.Snyder , "Threat Modeling", *Microsoft Press*, 2004 The STRIDE Threat Model

[44] S. Mansfield-Devine, S. (2008). " Danger in the clouds." *Network Security* vol 12 pp.9-11, 2008.

[45] Abraham, D. (2009). "Why 2FA in the cloud?" *Network Security*, vol 9, pp.4-5, 2009.

[46] Armburst, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2009)."Above the clouds: a Berkley view of cloud computing" (Retrieved June 12, 2009,from http://radlab.cs.berkeley.edu/).

[47] Hoover, J. N. (2009). "GSA backs away from federal cloud CTO appointment" RetrievedJune 9, 2009, from http://www.informationweek.com/news/showArticle.jhtml?articleID=217800386.

[48] Klems, M. (2008). “Merrill Lynch estimates “cloud computing” to be $100 billion market” (Retrieved March 14, 2009, from http://markusklems.ulitzer.com/node/604936).

[49] Miller, E. (2009). “The Verterans Administration goes Web 2.0” Retrieved June 11, 2009,from http://blog.sunlightfoundation.com/taxonomy/term/Facebook/.

[50] Greenberg, A. (2009). “If the clouds burst” Retrieved June 11, 2009, from http://www.forbes.com/2009/06/04/cloud-computing-nist-intelligent-technology-cloud-computing.html

[51] Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. “Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing.” *First Monday*, vol 14, pp.5.2009.

[52] Armburst, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2009).“Above the clouds: a Berkley view of cloud computing” (Retrieved June 12, 2009, from http://radlab.cs.berkeley.edu/.

[53] Ortutay, B. (2009). “Twitter service restored after hacker attack”, *The Baltimore Sun* Retrieved from http://www.baltimoresun.com/technology/bal-twitter-outage-0806,0,2941226.story.

[54] Brodkin, J. (2008). “Loss of customer data spurs closure of online storage service”, *The link up*, Retrieved March 14, 2009, from http://www.networkworld.com/news/2008/081108linkup-failure.html?hpg1=bn.

[55] Krishna P. N. Puttaswamy, Christopher Kruegel, and Ben Y. Zhao “Silverline: Toward Data Confidentiality in Third-Party Clouds” *Computer Science Department*, UC Santa Barbara

[56] *Cloud Computing*. (n.d.). Retrieved October 14, 2009, from TechEncyclopedia: http://www.techweb.com/encyclopedia?term=Cloud+Computing&x=0&y=0

[57] Brown, B. (2009, 06 10). “5 Cool Cloud Computing Research Projects.” Retrieved 09 2, 2009, from *NETWORKWORLD*: http://www.networkworld.com/news/2009/061009-cloud-computing-research-projects.html?page=2

[58] Cubrilovic, N. (2009). “Letting data die a natural death” Retrieved October 13, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2009/10/11/

[59] Chen, Y. -C., & Perry, J. “Outsourcing for e-Government: managing for success. Public Performance and Management Review”, vol 26, no 4,pp. 404−421, 2003

[60] Brantner, M., D. Florescu, et al. (2008). “Building a database on S3, ACM.”

[61] Greene, T. “ Cloud security fears cast shadow at RSA” , *Network World* vol 26, pp.16.2009.

[62] Saran, C. “Cryptography breakthrough could secure cloud services.” *Computer Weekly*pp.20, 2009

[63] Hewitt, c. “ORGs for scalable, robust, privacy-friendly client cloud computing.” *IEEEInternet computing* vol 12 no 5, pp. 96-99.2008.

[64] Herrick, D. (2009). “Google this!: Using Google apps for collaboration and productivity”, *ACM.*

[65] Vieira, K., A. Schulter, e al.(2009). “Intrusion Detection Techniques in Grid and cloud computing Environment.”

[66] Walsh, P.J. “The brightening future of cloud security.”*Network Security* vol 10, pp. 7-10.2009.

[67]”Sloan, K.(2009). “ Security in virtualised world.” *Network Security* 2009 vol 8, pp.15-18.

[68] Viega, J. (2009). “Cloud computing and the common man.” *Computer*, vol42, no 8, pp. 106-108. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=05197438]

[69] Christensen, J. (2009). “Using Restful web-services and cloud computing create next generation mobile application”, *ACM.*

[70] Mowbray, M. And S. Pearson (2009). “A client-based privacy manager for cloud computing,” *ACM.*

[71] Wang, C., Q . Wang, et al. (2009). “Ensuring data storage security in cloud computing.”

[77] Joint, A., E. Baker, et al.(2009). “Hey, you, get off of that cloud?” *Computer Law and Security Review: The International Journal of Technology and Practice* vol 25, no 3, pp.270-274.

[78] An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199

[79] EMC, Information-Centric Security. http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf.

[80] ESG White Paper, The Information-Centric Security Architecture. http://japan.emc.com/collateral/analyst-reports/emc-white-paper-v4-4-21-2006.pdf.

[81] R.Chow, P. Golle, M. Jakobsson, R. Masuoka, J.Molina, E. Shi and J. Staddon“Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control” PARC Fujitsu Laboratories of America

[82] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. “Public Key Encryption with Keyword Search.” In *EUROCRYPT*. 2004.

[83] Boneh, D and Waters, B. Conjunctive, “Subset, and Range Queries on Encrypted Data.” In *The Fourth Theory of Cryptography Conference* (TCC 2007), 2007.

[84] Chor, B., Kushilevitz, E., Goldreich, O., and Sudan, M. “Private Information Retrieval.” *J. ACM*, vol 45, no 6, pp. 965-981.1998.

[85] Shen, E., and Shi, E, “Cryption Systems.” In TCC. *Waters, B. Predicate Privacy in En* 2009.

[86] Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, A. “Multi-Dimensional Range Query over Encrypted Data.” *IEEE Symposium on Security and Privacy*. 2007.

[87] Song, D., Wagner, D., and Perrig, A. “Practical Techniques for Searches on Encrypted Data.” *IEEE Symposium on Research in Security and Privacy*. 2000.

[88] Gentry, C. Fully “Homomorphic Encryption Using Ideal Lattices.” *STOC*. 2009.

[89]Waters, B. and Shacham, H. “Compact Proofs of Retrievability.” *ASIACRYPT*. 2008.

[90] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Z., Peterson, and Song, D. “Provable Data Possession at Untrusted Stores.” *CCS*. 2007.

[91] Nelson, M. “The cloud, the crowd, and public policy.” *Issues in Science & Technology*, Vol *25*, no 4, pp. 71-76. 2009. Retrieved from Academic Search Premier Database.

[92] IDC. (2009a). “IDC‟s new IT cloud services forecast: 2009-2013.” Retrieved from http://blogs.idc.com/ie/?p=543

[93] Stoneburner, G., Hayden, C. & Feringa, A. (2004). “Engineering principles for information technology security (a baseline for achieving security),” Revision A. *NIST Special Publication 800-27 Rev A.* http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf[Accessed: 2/8/2010].

[94] “Risk categories.” (n.d.). *Disaster Recovery Journal*. Retrieved from http://www.drj.com/index.php?option=com_glossary&func=view&Itemid=297&catid=35&term=Risk+Categories[Accessed: 19/7/2010].

[95] “Grid Computing.” (n.d.). Retrieved October 14, 2009. Available from: http://www.techweb.com/encyclopedia?term=grid%20computing

[96] “Utility Computing.” (n.d.). Retrieved October 14, 2009, http://www.techweb.com/encyclopedia?term=Utility+Computing&x=25&y=11[Accessed: 9/8/2010].

[97] Mohamed, A. “A History of Cloud Computing.” , from *ComputerWeekly*, 15, 2009. Available from: http://www.computerweekly.com/Articles/2009/03/27/235429/a-history-of-cloud-computing.htm[Accessed: 9/8/2010].

[98] Hammond., M. Hawtin., R. Gillam., L. Oppenheim, Cloud computing for research, 2010. available from : http://www.curtiscartwright.co.uk[Accessed: 8/7/2010].

[99]Amazon Web Services: Overview of Security Processes *November 2009*. available from Ahttp://aws.amazon.com/security [Accessed: 9/7/2010].

[100]*Grid Computing*. (n.d.). Retrieved October 14, 2009, from TechEncyclopedia: http://www.techweb.com/encyclopedia?term=grid%20computing

[101] Brown, B. (2009, 06 10). *5 Cool Cloud Computing Research Projects*. Retrieved 09 2, 2009, from NETWORKWORLD: http://www.networkworld.com/news/2009/061009-cloud-computing-research-projects.html?page=2

102] Erica Naone: "Computer in the Cloud", MIT Technology Review, September 18, 2007

[103] J. Nicholas Hoover and Richard Martin: "Demystifying the Cloud", InformationWeek Research & Reports, pp. 30-37, June 23, 2008.

[104] Won Kim. "Cloud Computing: Today and Tomorrow," Journal of Object Technology, January/February 2009.

[105] Identifying the security risks associated with governmental use of cloud computing

[106] Vecchiola., C. Pandey., S. and Buyya., R. (unapplicated) High-Performance Cloud Computing: A View of Scientific Applications.

Appendix 1

1- How much experience do you have with Cloud computing?

□None □Minimal □Moderate □High

2- Do you think Cloud computing is beneficial?

□Yes □No □Other

3- What difficulties have you encountered when using the Cloud (for example Google documents)?

□ Cost of using the service □Accessibility □Services □Usability

4-What are your reasons for using Cloud Computing?

□ Increasing capacity of computing and business performance

□ Avoiding capital expenditure in software, hardware, information security, information technology support, by outsourcing services /platforms/ infrastructure.

□ Developing business into the Cloud

□ Adding redundancy to increase resilience and availability

□ Scalability and Flexibility of IT resources

□ Others (please specify)

5- What are your main concerns for cloud computing?

□Privacy

□Availability of data and/or services

□ Integrity of data and/or services

□ Confidentiality of shared data

□ Loss of control of data and/or services

□ Lack of liability of providers in case of security incidents

□ Inconsistency between regulations and trans national laws

□ Repudiation

6-Which solution do you believe is most suitable for ensuring confidentiality, integrity and availability of Cloud Computing?

□ a federation of clouds provided by various sources (partner, private, etc)

□ Private cloud (owned, managed internally)

□ Public (owned, managed via an unrelated business)

□ Partner cloud (owned, managed via trusted)

□ other (please specify)

7- Do you think current level of security is good enough for cloud computing?

□No □Yes

8- Do you think it is possible to make cloud available 100% of the time?

□ No □Yes

9-Overall, what do you think of the integrity of cloud computing (the ability of the Cloud to manage risks that affect the accuracy of information managed)?

□ Unsatisfactory □ Satisfactory □ Excellent

10- Which one of these cryptographic techniques could improve the confidentiality of cloud computing?

□ Homomorphic encryption

□ Private information Retrieval

□ Other

Thank you for taking the time to complete the questionnaire.