UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Mohit Kinger

Enterprise Cloud Security Guidance and Strategies for Enterprises

Master's Thesis (30 ECTS)

Supervisor(s): Andro Kull

Raimundas Matulevičius

Tartu 2017

Enterprise Cloud Security Guidance and Strategies for Enterprises

Abstract:

Today an estimated 72% of enterprises use at least one cloud application or a percentage of their I.T infrastructure in the cloud. Research shows that 56% of the decision makers in technology are investigating more ways of leveraging the cloud. This makes it important to understand the different usage plans in cloud service models, business drivers and investments. This thesis measures the myriad benefits of using cloud applications, and the effect of cloud computing on business performance. As will be seen in the thesis, cloud computing offers a flexible, affordable as well as proven platform for the provision of business and IT services via the internet. Cloud computing provides companies with the rare opportunity of strengthening their efficiencies in service delivery, management streamlining, and the aligning of IT services with the ever changing business needs. In more ways than one, cloud computing provides solid support for business functions, alongside increasing the capacity for the development of new as well as innovative services. A non-exhaustive review of the existing literature revels that the security challenges faced by enterprises during cloud adoption and interoperability have to be addressed before the implementation of cloud computing. In this thesis, we provide a detailed overview of the key security issues in the realm of cloud computing and conclude with the recommendations on the implementation of cloud security.

Keywords:

Cloud computing ,Cloud security ,IT services.

CERCS: P170, Computer science, numerical analysis, systems, control

Ettevõtte pilve teenuse turvalisuse soovitused ja strateegia

Lühikokkuvõte:

Hinnanguliselt 72% ettevõtetest kasutavad vähemalt ühte pilves olevat rakendust või on mingi osa nende IT infrastruktuurist pilves. Uurimistööd näitavad, et 56% tehnoloogia valdkonna otsustajatest uurivad erinevaid võimalusi pilvelahenduste kasutamiseks. Eeltoodu tõttu on oluline mõista erinevaid pilveteenuste kasutusvõimalusi, ärivajadusi ja investeeringuid. Antud magistritöö hindab paljusid kasutegureid, mida pilverakenduste ja pilvearvutuse kasutamine pakub äritegevusele. Pilvearvutus pakub paindliku, taskukohast ja end tõestanud platvormi ärilahenduste ja IT lahenduste loomiseks. Pilvearvutuse kasutamine pakub ettevõtetele harukordset võimalust muuta teenuse pakkumist tõhusamaks, juhtimist sujuvamaks ning viia IT teenused vastavusse pidevalt muutuvate ärivajadustega. Pilvearvutuse kasutamine pakub rohkem kui ühe võimaluse ärivaldkondade usaldusväärseks toeks ning ühtlasi tõstab võimekust luua uusi ja innovaatilisi teenuseid. Olemasoleva kirjanduse mittetäielik analüüs toob esile selle, et enne ettevõtetes pilvelahenduste ja pilvearvutuse kasutuselevõttu on väga oluline pöörata tähelepanu kaasnevatele turvalisuse väljakutsetele. Antud magistritöös on detailselt käsitletud peamisi pilvandmetöötluse valdkonna turvalisuse probleeme ning töö järeldusena pakutakse välja soovitusi pilve turvalisuse juurutamiseks.

Võtmesõnad:

Arvuti pilveteenused , Pilveturvalisus , IT Teenused.

CERCS: P170,arvutiteadus, arvutusmeetodid, susteemid, juhtimine (automaatjuhtimisteooria)

Table of Contents

1 Introduction

Cloud computing is currently the basis of internet usage as web services among them emails, social networks, media streaming sites, and search engines are hosted in the cloud [1]. The cloud essentially refers to the voluminous collections of servers that run coordinated software that make the host's disposable to a large extent. According to [2]cloud computing offers a flexible, affordable as well as proven platform for the provision of business and IT services via the internet. Cloud computing is becoming increasingly popular in the corporate sector as companies appreciate the immense value of the ease of deploying and scaling cloud resources, within their business processes, services, as well as applications that can be available in real time regardless of the location of the user. Cloud computing provides companies with the rare opportunity of strengthening their efficiencies in service delivery, management streamlining, and the aligning of IT services with the ever changing business needs. In more ways than one, cloud computing provides solid support for business functions, alongside increasing the capacity for the development of new as well as innovative services.

Research from a study carried out by [3] [4]shows that both public and private cloud models are popular among individuals and corporates. Some examples of the public cloud models include software as a service (SaaS) clouds. Specific cloud services under SaaS include the IBM Lotus Live. Other public cloud modules include Amazon's Platform as a service (PaaS) [2].The Figure:1 from a research carried out by [5] shows how enterprises are using public cloud applications.

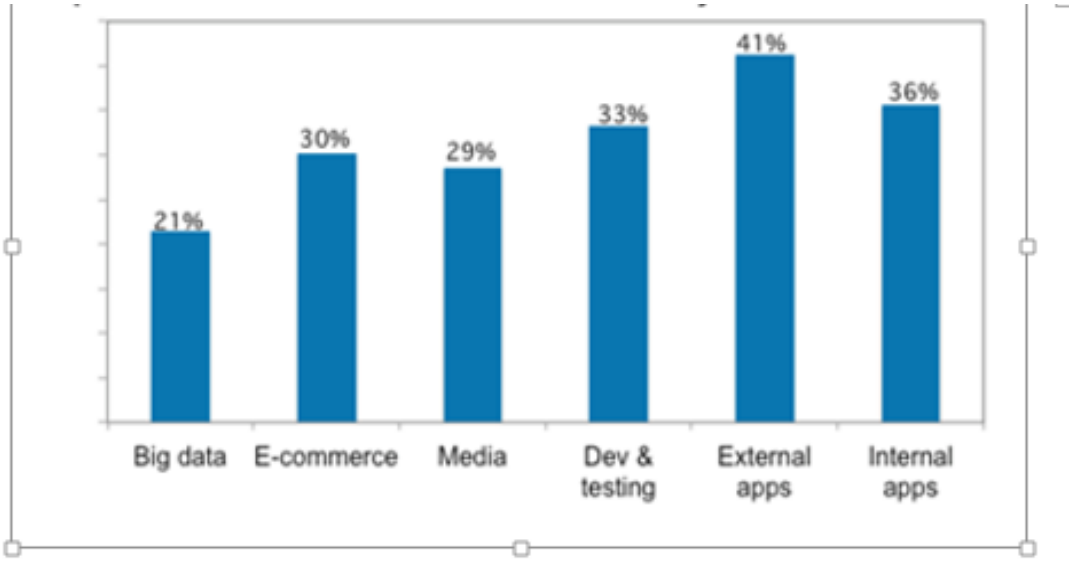

Figure 1. Cloud Usage in Enterprises [5]

Unlike the public modules, private cloud modules are owned by private companies and have similar benefits as the public cloud modules with additional advantages of increased flexibility as well as control. Aside from this, the private clouds can offer reduced latency during peak traffic. Organizations embrace and appreciate both the public and private cloud modules through the integration of the said modules to create hybrid clouds [4]. The hybrid clouds are designed specifically to meet particular business as well as technological requirements as they assist in the optimization of privacy and security with less IT costs. As seen in the Figure:2 below, the various applications of private cloud computing increased between 2014-2015 [4].

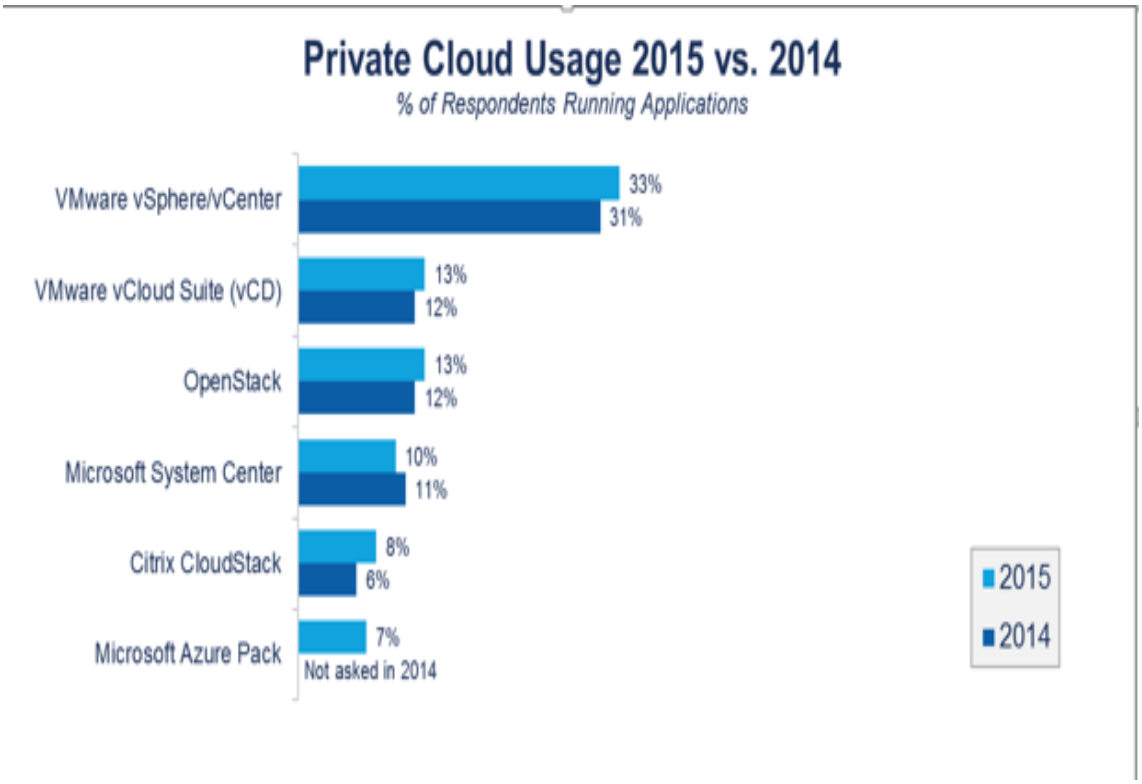

Figure 2. Use of Private Cloud [4]

While the benefits of cloud computing are irrefutable, so is the needs to implement stringent security measures for cloud services. Security experts have analysed the aspects of computing security, with respect to the cloud to assess the extent to which proposed defences can address cloud specific attacks [1]. The experts agree that to benefit from the efficiencies enabled by cloud computing, enterprises have to implement cloud computing security strategies to be void of malicious attacks that can translate into heavy losses.

A non-exhaustive review of the existing literature reveals that the security challenges faced by enterprises during cloud adoption and interoperability have to be addressed before the implementation of cloud computing [3] [2]. A review of the security challenges indicates that organizations such as Google and Apple consider security as a paramount challenge that needs to be solved. This is attributable to the fact that even with the strongest implementation of security measures malicious people always have weaknesses to exploit. As such the identification of the security issues and the subsequent solution updates to curb the challenges are paramount in the use of cloud computing services. The Figure: 3 below from Intel research [3] shows the security vulnerabilities that enterprises are exposed to. In this thesis, we provide a detailed overview of the key security issues in the realm of cloud computing and conclude with the recommendations on the implementation of cloud security. A high level and advanced classification of the thesis is carried out to examine the extent of could attacks. Specifically, the thesis will organize the literature on cloud security into five categories: colonial denial of service, data integrity and availability, infrastructure compromise, collocation confidentiality breach and data confidentially. As will be seen in the thesis while the realm of cloud computing has made great strides, there are shortcomings as far as cloud defences are concerned.

This will be evidenced by the different perspectives given by published research.

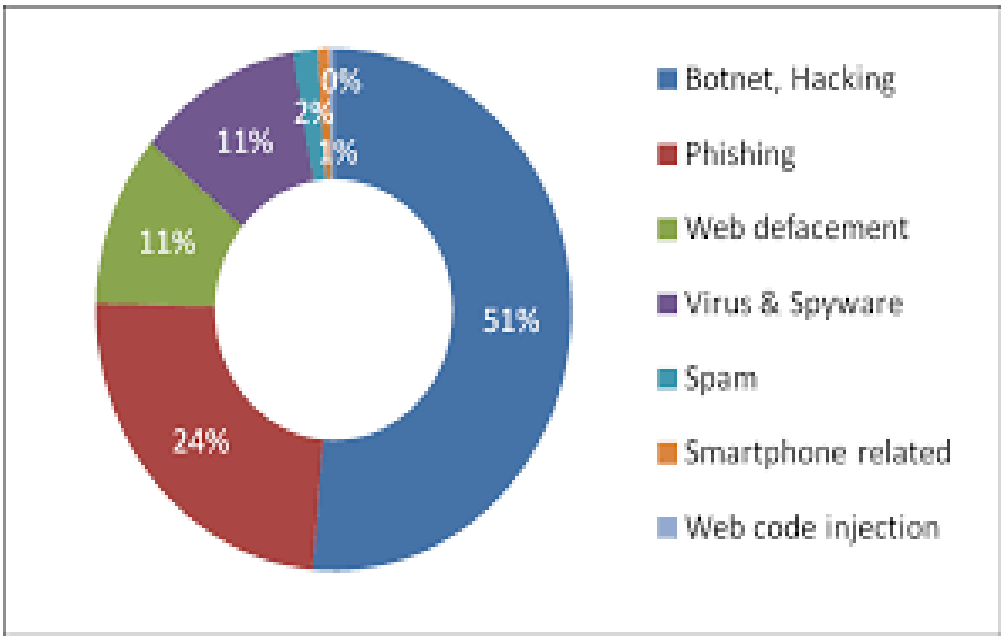

Figure 3. Security Vulnerabilities [3]

.

1.1 Aims and Objectives

The thesis aims to identify the steps, security guidance and the cloud security strategies needed by enterprises that work on cloud based environments. The research will narrow its focus on the challenges and security concerns that enterprises are exposed to prior to the use of cloud services and after the implementation of cloud computing.

The specific objectives of the study are to:

- Analyse the current as well as the future state of cloud computing adoption
- Understand the cloud security challenges and identify security strategies that can be applied in the world of cloud computing
- Identify the best practices for enterprises while using cloud based platforms
- Establish the perspective of cloud services providers with regard to security
- Analyse the emerging trends in cloud security
- Suggest counter measures for the cloud computing security challenges.

1.2 Research Questions

The study will be guided by the following research questions

1. What are the current and future states of cloud computing adoption in enterprises?
2. What are the main security challenges faced by enterprises that use cloud based platforms?
3. What are some of the security strategies that are applicable in cloud computing?
4. What are the best practices with regard to security that can be used by enterprises to protect themselves from cloud attacks?
5. What is the perspective of cloud service providers with respect to security?
6. What are the suggested counter measures for addressing security challenges in the cloud?

2 Background

2.1 Defining Cloud Computing

Cloud computing is a form of computer paradigm in which a collective pool of systems is connected with the aim of offering dynamically scalable equipment for storing applications, data and files [5] [6]. The advent of cloud computing made significant reductions in terms of computation costs, hosting applications and the storage of the aforementioned content. [8]Describes cloud computing as one of the most practical approaches that can be used by an enterprise to experience costs benefits. This view is supported by [9]who asserts that the computer paradigm has the potential of transforming a data center from a costly set up to a lower priced environment.

According to [8]cloud computing is founded on the primary principal of reusing the IT capabilities of an enterprise. The author goes on to say that the fundamental difference introduced by cloud computing is the broadening of horizons in respective boundaries of an enterprise. A similar view is held by [2] who defines cloud computing as a pool of scalable, abstracted and managed infrastructure that has the capability of hosting applications. Other definitions of cloud computing include defining it as a model that enables ubiquitous, on demand and consentient access to a pool of network [4]. This provides access to a large pool of configurable resources that can be provisioned as well as released with no management efforts from the use and similarly minimal interactions from the service provider.

This far, cloud computing as a computer paradigm is regarded as an evolution of technologies that have intertwined to change the approach used by enterprises to build and use their technological infrastructure. [3] Postulates that essentially, the technologies used in the paradigm are the traditional computing paradigms that have been used previously. The main difference is that the cloud makes the resources accessible on real time demand to a wide range of users.

As indicated by [4] the cloud is considered to be a software as well as an infrastructure. This means that the cloud can be an application that is accessible via the internet such as drop box or email services, or it can be considered an IT infrastructure that can be used upon request.

2.2 History of Cloud Computing

A review of existing literature indicates that cloud computing has undergone several stages among them are grid computing, utility computing, ASP and SaaS. As such, the cloud is a result of the evolution of the increased use of virtualization, autonomic, service oriented architecture and utility computing. [1] Indicates that in this paradigm aspects such as the location of the IT infrastructure, or the number of devices remain unknown to the end users.

The evolution of computer paradigms that culminated in the invention of cloud computing started in the early 1990s. Research indicates that historically, the telecommunication companies only provided dedicated, data circuits (point-to-point) to their customers [9] [3]. However, from 1990 the companies started broadening their services to include services such as virtual private networks. The introduction of virtualization allows the companies to offer the same quality at only fraction of the initial costs. This was attributable primarily to the fact that the companies could now optimize the utilization of resources such that there were improvements in the efficiency of the bandwidth.During the earliest phases of the evolution, the term “cloud” was used to refer to the computing space that existed between

the service providers and the end users. In 1997 for instance, Professor Ramnath Chellapa defined cloud computing as the new paradigm where the computing boundaries were determined using the economic rationale instead of the technical limits [8]. This became the basis of what is referred today as the paradigm of cloud computing.

In the second half of the 1990s, the telecommunications companies gained a clearer and deeper understanding of cloud computing, as well as its role in the provisions of superior solutions as well as services to the end users while simultaneously enhancing the internal efficiencies of the companies. Among the first companies to incorporate the idea of cloud computing was Salesforce which in 1999 became a mover in the cloud realm [2]. The company used the idea of cloud computing to pioneer the concept of delivering enterprise applications to customers across the internet. The applications developed by the company could be easily accessed by all end users that had internet access. Through the application, companies were able to buy the services on an on demand basis that was also cost effective.

The use of the cloud to share services soon attracted attention from other companies including Amazon who launched its web based retail services in 2002. According to [7] Amazon was the first enterprise to advances its company's data centres. [3] Reveals that prior to the use of the cloud, the data Centre was using only 10% of its capacity. With the realization that the new infrastructure model could allow the company to use the remaining capacity with more efficiency, the company launched cloud computing for the long haul. A similar strategy was used by other companies such as Google which became a leading player in internet commerce. With the launch of Google Docs in 1996, Google brought the power of the computer paradigm to end users [4].

2.3 Benefits of Cloud Computing

2.3.1 Elasticity

Cloud computing experts identify the scalability of an enterprises computing capacity, to either scale up or scale down is an important aspect of the computer paradigm [9] [7]. This feature of cloud computing that allows the enterprise to choose its services depending on their demand ensures that an organization reduces costs and have optimized resource allocation

For example, an enterprise that offer software as a service in the form of providing end users with online tax filling services can benefit from the elasticity of cloud computing. This is attributable to the fact that the tax fillers have peak and off peak seasons. As such, the computing resources of the company will have more demand during the tax season (2-3 months annually). From the financial perspective, it would be uneconomical to invest in the cloud resources in advance knowing that the infrastructure will only be used partially for 9 months. Cloud computing offers such an enterprise the option of scaling down during off peak seasons. In turn, this reduces the costs of resources.

2.3.2 Pay as You Grow

Service providers that offer public cloud services such as Google and Amazon allow enterprises to eradicate the upfront infrastructure investments which as indicated by [7] have large capital requirements. The cloud services offer enterprise the option of purchasing computing resources as they are needed dynamically. In other words, by using cloud services, the enterprise does not have to plan in advanced or make financial commitments up front. The model is especially feasible from small and medium sized companies as well as start-ups that are often unable to commit large sums of money during start up.

2.3.3 In House Liability

Enterprises that run IT services and use the IT resources within the organization are susceptible to various liabilities as well as costs. While some researchers hold the view that running the IT infrastructure from within the enterprise would be safer as well as more affordable, other researchers claim that most times, that is not the case. According to [8]depending on the IT budget of a company, as well as other factors such as the skills of the employees, it would be more effective, safer and cheaper to run the IT infrastructure from a public cloud. Research from [9]reveals that service providers that offer public cloud services can offer service level agreements commonly referred to as SLA's. Through these agreements, the cloud providers own the liabilities of the enterprise with regard to IT infrastructure.

2.4 Why Now?

What are the contributing factors for the rampant use of cloud services now rather than in the past? A review of existing literature identified the following factors that make the cloud services more common especially in enterprises.

2.4.1 Economies of scale

Among the factors that have advanced the use of cloud services include the great strides made in the realm of e-commerce, social media and web 2.0 services that have increased the demand of computing resources to a significant extent. As indicated by [1][4] companies such as Microsoft, Google and Amazon have realized the feasibility of designing and building large data centers for the needs of their customers rather than developing many small data centers. This is attributed to the fact that it is more cost effective for the companies to purchase resources like bandwidth, electricity, processing and storage at large volumes. In such large data centres, processes such as optimizing the amount of work done for each dollar spent becomes easier, faster and more accurate. In addition, the companies can share the components and resources more efficiently, and additionally improve the server density and reduce idle time. As shown in Figure: 4 below, the costs of bandwidth and system administration is 7 times more affordable when using large data centers. The Figure: 4 below from Microsoft shows that the storage costs are 5 times more affordable in the data centers that have 100,000 servers compared to the centres with 100 servers [4].

2.4.2 Expertise

According to [8]the process of designing and building a datacentre requires advanced expertise and technical skills. Once Google and Amazon realized that they had the expertise, technology and capacity to build datacentres that hosted their internal clouds, the companies decided to leverage the same expertise and skills to build public data centers and offer computing services to other companies through the cloud.

2.4.3 Commodity Hardware

The other factor that fostered the use of cloud computing is the reduction of the costs of production with regard to computer chips. Other than this, the standardization of computer architectures on the x86 platform, and the mechanical compatibility of the internal components of the PC also resulted in the decrease of hardware costs in the last ten years to a significant extent. According to the [3]the affordability of hardware components has resulted in its commoditization and also reduced the related computational costs.

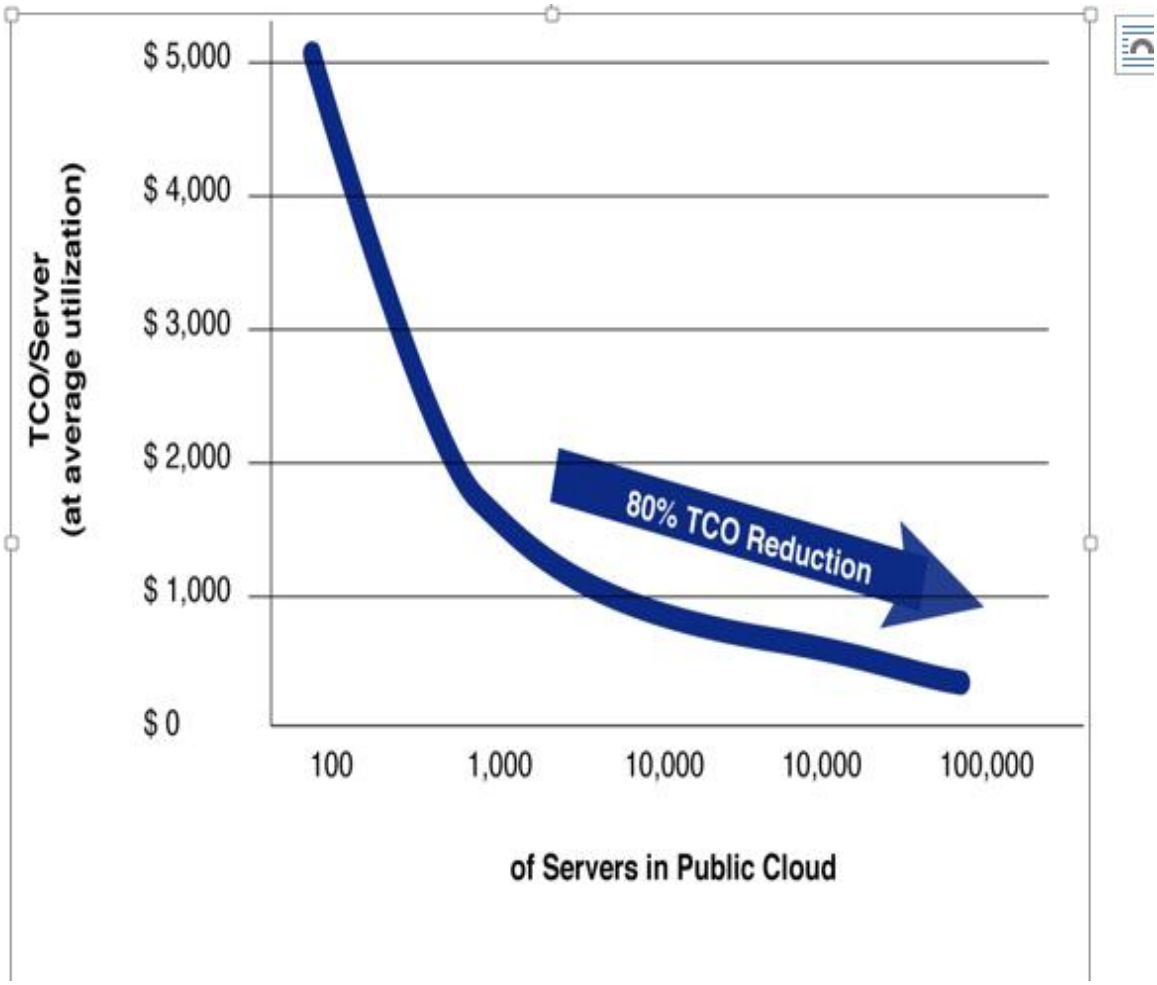

Figure 4. Cost of Utilisation [4]

2.4.4 Virtualization

The virtualization of hardware has enabled the increased the density of hardware utilization. In addition, virtualization ensures that the resources are used in a more efficient way. Research shows that virtualization is among the technologies that have made aspects such as elasticity and flexibility more functional in cloud computing [1]. This is because virtualization increases the deployment speed, auto provisioning in a dynamic way and more efficient cloud management.

2.4.5 Open Source Software

Computing experts postulate that commodity hardware and open source software are two leading enablers of cloud computing [3] [10]. [2] Particularly identifies the Linux OS as one of the leading building blocks at the center of the cloud environment. [4] Also identifies Xen which is the virtualization software that was used by Amazon to host an estimated 500,000 virtual machines. Hadoop is also a distributor of the computing platform that assists a wide range of companies to run parallel computations from the cloud. These examples show that the reduction of costs that would have been incurred in purchasing expensive software licenses is among the factors that enable Google and other cloud providers to offer affordable and reliable cloud services.

2.5 The Cloud Vs. The Grid

Although experts appreciate that cloud computing borrowed significantly from grid computing, they also reveal that essentially, the two computing systems are different to a large extent. The fundamental difference between the two computational systems is that grid computing was not created an on-demand public service. In addition, grid computers are used mainly in the same enterprise to run computational tasks. On the other hand, cloud computing is associated with a specific service that is in turn used as the access point that provides results to the end user. Historically, computing grids were used to carry out heavy computing tasks and were therefore constructed with many servers in advance [1]. This led to high costs even when some of the servers were idle during off peak season. The cloud has the advantage of scaling on demand. As such, it provides increased elasticity such that an enterprise environment can start with a few resources, and quickly grow to more resources and scale down when to a smaller size when necessary.

3 Theoretical Baselines

3.1 The Cloud Computing Architecture

Cloud architectures essentially describe the design of applications that use web enabled, on demand services. This means that the software applications used in cloud architectures are designed in such a way that the underlying infrastructure is used only when needed, use the required resources on demand, and to carry out computational tasks [10]. The architectures are also designed to relinquish the resources that are not needed. When in use the architecture demands that the application is elastic to scale up and down depending on the needs of the resources.

As observed in the introduction, the promise of offering computational services in a centralized way across the network, was in place even in the 1960s as evidenced by the mainframe time sharing technology.This architecture was replaced by the PCs and the client-server architectures. Until a decade ago, the typical IT infrastructure in an enterprise consisted of servers that were powerful but expensive. [11] postulates that the architecture of the infrastructure was monolithic, such that each of the powerful machines could host approximately 20 enterprise applications.The markets had dominant leaders among the HP, IBM and Sun whose servers proved to be very costly to buy and maintain. The servers also took a long time to be installed and upgraded and in certain scenarios were especially vulnerable to the outages. During this computer period, the internal resources of companies had to be pooled to ensure that the best was made out of the costly and monolithic resources. The Figure: 5 below gives a visual representation of the architecture of cloud computing.

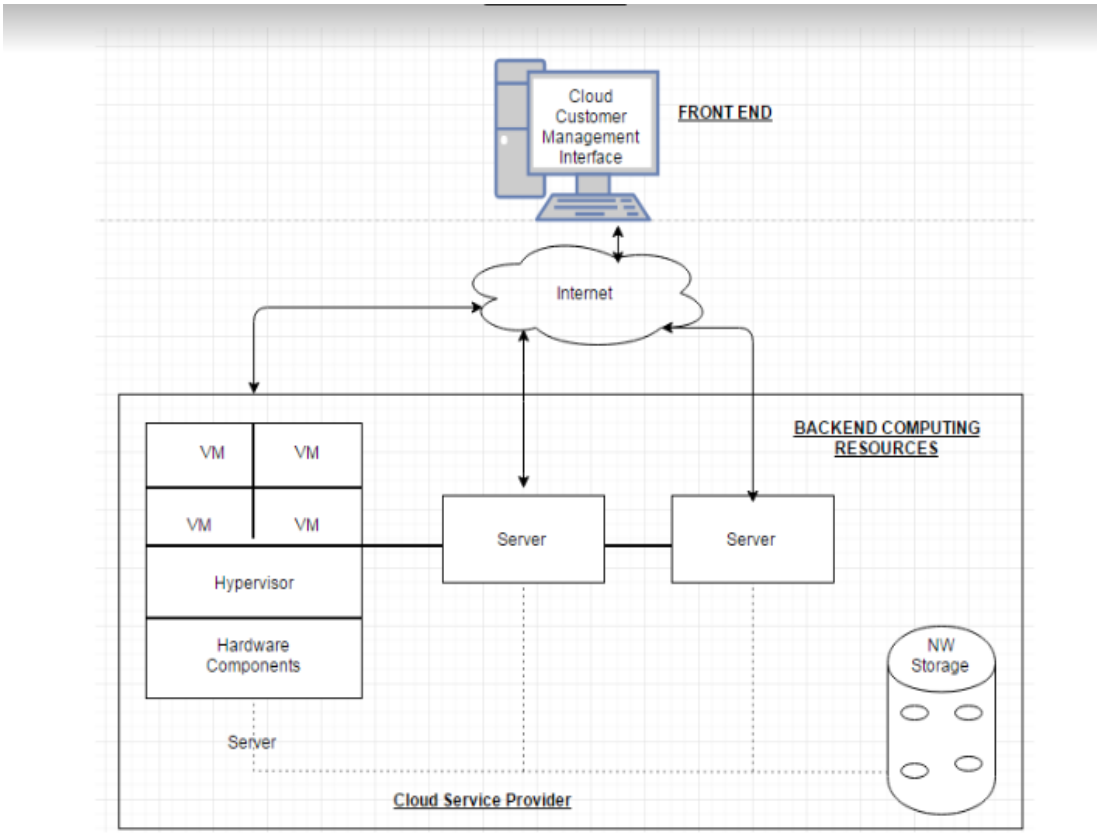

Figure 5. Cloud Computing Architecture

At the start of the 21st century, data centers began overfilling and power, cooling, and space became increasingly expensive [13]. This made concepts like virtualization and commodity computing popular and more established. the architecture of cloud computing borrowed from the two concepts through the use of self service by the end users, metered usage and automated and dynamic resource allocation and scalability. As service became more distributed, SOA became the fundamental method of integrating as well as orchestrating the distribution of business services. Currently, this approach forms the basis of cloud computing architecture more so because customers demand the integration of in-house, public and private computing services [14]. In more ways than one, the cloud has become the new version of the virtualized mainframe that was used in the past. Although certain aspects of the cloud architecture are different, they have simply evolved with the changing needs of the customers and end users. The cloud is based on the foundational computing concepts that addressed the need of leveraging the resources in the most effective way. However, security remains the main concern for customers that use the private and public services today. The cloud computing architecture can be changed to make the platform more secure for the enterprises and individuals that use it.

The architecture used in the cloud provides an effective solution for the myriad issues that surround the processing of large scale data. Research indicates that traditional data processing has the limitation of the difficulty of getting as many computers as needed by an application. The other limitation is the difficulty of getting the machines on demand. Traditional data processing is also limited by the challenges of distributing and coordinating a large scale computational task using different machines as well as the challenge of running processes on the machines and the provision of extra computers to recover the process in case of failure. Lastly the traditional data processing model lacks the ability of auto scaling the resource depending on the workload. The cloud architecture solves the aforementioned difficulties faced by enterprises that use traditional data processing techniques. The applications that are built on the architecture of cloud computing run in the cloud regardless of the physical location of the end user. The physical location of the cloud infrastructure is known and determined only by the service provider. The providers use simple APIs of web enabled services that are scalable on demand and have advanced industrial strength in which the reliability logic of the services is implemented and hidden in the cloud. In the cloud architecture, the use of resources is solely on an on-demand basis. In other words, the use of resources can either be seasonal or ephemeral which provides the optimum utilization of the resources and money.

3.1.1 Building Scalable Architecture

According to [11] among the most imperative aspects of the cloud computing architecture is scalability. In the traditional infrastructure, systems are designed fundamentally for the sustenance of future growth as well as the demand for the resource. This architecture demands that the organization should invests financial resources in advance to fulfil unseen demand in the future [15]. Since traditional infrastructure lacks in terms of elasticity, the resources of the system are non-scalable leading to the constant overprovisioning of resources which in turn creates an environment whereby the resources are underutilized.

Unlike the architecture used to develop the traditional system, the cloud architecture is described as multi-tenant; a feature that ensures that the resources are shareable among different applications [11] [10]. The shared environment is based on the premise that all the applications cannot be used at any given time. As such, the architecture's scalability function is based on the premise that when a resource is idle the other resource is in use. Using this concept, the cloud service providers can offer on demand resource availability and enhance

the effectiveness of the allocation and utilization of resources. The cloud computing infrastructure is made of shared resources which include storage, networks and servers. Cloud management software can be used to monitor how the resources are used and therefore make decisions regarding resource allocation. Cloud service providers have to ensure that the computing resources are available to serve the end users even during peak times. The Figure: 6 below shows a visual description of the main cloud characteristics, service models and deployment models.

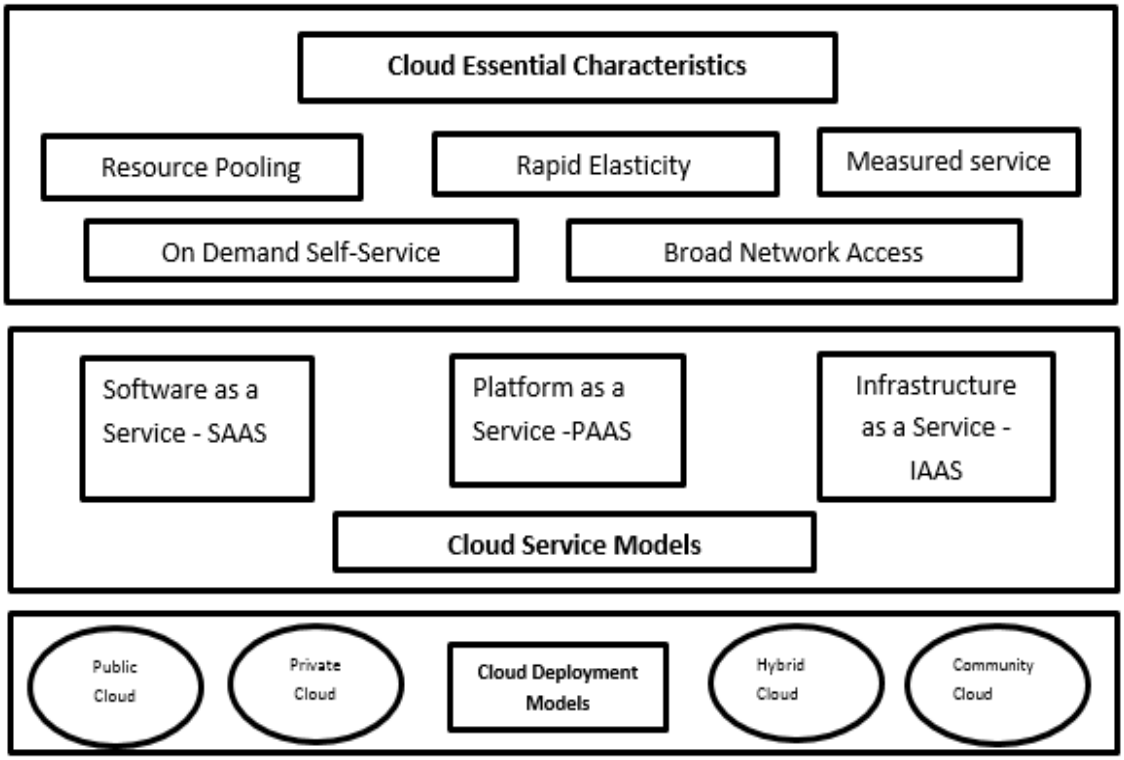

Figure 6. Essential Cloud Characteristics and Models

3.2 Essential Characteristics of Cloud Computing

The National Institute of Standards and Technologies (NIST) defines cloud computing as a computer environment that enables convenient network access on demand to a shared pool of configured resources such as servers, storage, services and application [10] [15]. These set of resources can in turn be provisioned and released without much management and interactions from the service providers. Providers of cloud computing services do not supplement IT resources, rather they offer strategic and core information technology services. From this definition, the NIST describes the essential characteristics of cloud computing as:

On demand self-service: in cloud computing, the consumers of services can make use of the capabilities of the service automatically [14].In other words, the end users can make use of capabilities like the network, server processing time and the storage without human interaction with the service providers.

Broad Network Access: NIST describes this as an essential characteristic in the sense that cloud capabilities like SW and HW are available across the network [12]. In addition, the said capabilities can be easily accessed using a variety of platforms among them laptops, tablets, and mobile phones.

Resource Pooling: The computing resources owned by the service providers are combined to serve many consumers. This is achieved using the multi-tenant model whereby different virtual and physical resources are assigned and reassigned in a dynamic way depending on the specific user's demand. This paradigm is among the most imperative features of applications that use the cloud. One of the outstanding characteristics of multi tenancy is the independence feature. This feature ensures that the end users have no knowledge and therefore no control of the exact location of the resources provided by the service providers. However, the end users have the ability of specifying the location at higher abstraction levels (e. g the country or state) [7]. Specific examples of the resources include processing, bandwidth, storage, virtual machines and memory.

Rapid Elasticity: This describes the characteristic that the computing capabilities can be provided in a rapid and elastic manner. In other words, the capabilities can be scaled out, and scaled in easily. According to [9] for the end users, the capabilities that can be provisioned are unlimited and can be bought in large amounts in real time.

Measured service: In cloud computing, the cloud systems are controlled and optimized automatically [3]. This is achieved through the leveraging of a metering capability whereby the use of resources can be monitored, controlled as well as reported. This feature is important because it ensures transparency between the consumer and the service provider. Through this feature, the consumers are assured that they are getting exact value for their money.

3.3 Service Models of Cloud Computing

Software as a Service (SaaS): in this cloud computing service model, the service provider provides the end users with the capability to use applications that run on their cloud infrastructure. The users can access the said applications using different client interfaces among them web browsers. When using this service model, users are not mandated to maintain or control the cloud infrastructure that includes aspects such as the network, operating systems, processing and storage [13]. Specific examples of SaaS model are NetSuite and Salesforce.

Platform as a Service (PaaS): In this model, the users are provided the resources needed for deployment on the service provider's infrastructure as well as the supported applications that they design or acquire [11]. PaaS users have control over the applications that have been deployed not the hosting environment for the application. However, the users have no control with regard to the infrastructure which as pointed out earlier in the discussion includes the operating systems, storage, servers and the network. Some practical examples of PaaS include Google App Engine, Azure and Heroku.

Infrastructure as a Service(IaaS): In this service model, the end users are given the authority to control processes, and manage resources such as network and storage among other imperative computing resources that are useful in the management of arbitrary software (can include the OS and system applications) [12]. In other words, when using this service model, the user can control the OS, storage and the deployed applications. In addition, IaaS users have limited control over certain networking components. Some examples of clouds that use the IaaS model include Amazon EC2, Nimbus, and Rackspace.

Privacy and Anonymization as a Service (PaaS): This service model is a proposed model to offer privacy and protection with regard to data management in specific organizations [1]. The proposed model also aims at using the work flow approach with regard to cloud data management. Hardware as a Service (HaaS): this service is based on the premise of purchasing hardware or even a data center with a PAYE [10].

In this model the users can scale up or down depending on their particular requirements. Some examples of services under this model include Blue Cloud Project from IBM, Nimbus and Amazon EC2.

Identity as a Service: This service model is used primarily by third party service providers that offer functions such as identity control and access control. Specific examples of the control functions include the user's life cycles as well as the process of signing in. Identity as a Service can be used alongside other services like software, infrastructure and platform services. The model can also be used in both private and public clouds [12].

Data storage as a Service (DaaS): The DaaS service models allows the users to specify the amount of data storage they need and pay for the exact amount of storage. In this service, the service providers form a different cloud that offers storage as a service. Some examples of main users of DaaS include Google Bigtable. Amazon S3 and the Apache Hbase.

Security as a Service (SaaS): In this model, the users have the authority to create and develop their unique security policies as well as risk frameworks. When using this service model, the users have to identify, examine, measure and finally prioritize on the risks associated with the system.

Anything as a Service (XaaS): This service model in general represents service deployment. The services provided under this model can be any type of service indicated by 'X". This means that the services could be software, hardware, data, IT, security, monitoring and infrastructure. Research indicates that the rate of developing new services has increased all of which can be categorized under the XaaS service model [9] [13] [11]. Examples of the XaaS applications include the management as a service, cloud as a service and the provision of IT as a service.

3.4 Deployment Models of Cloud Computing

The deployment models in c loud computing essentially represent the precise group of the cloud environment. The models can be distinguished through features such as size, accessibility and proprietorship. [4] Postulates that the models are used to describe the purpose as well as the overall nature of the cloud. Research indicates that since enterprises are becoming increasingly aware of the immense cost savings that accrue from using the cloud it is imperative that the organizations make the best decisions with regard to the most suitable deployment model for their unique needs [9] [16].

3.4.1 Public Cloud

Public cloud which is also referred to as external clouds are the services that are provided by third party service providers. Generally, the service providers manage as well as host the public clouds and assume responsibilities such as the implementation, management, maintenance and provisioning. Experts hold that this category of cloud services offers more efficiency with regard to the pooling of resources [7]. In this deployment model, the end users or consumers that consume the services and the resources are charged for the particular resources that they use based on the pay as you go technique.

The public cloud deployment model delivers the IT services and resources through a network that in most cases allows public access and use. The model represented cloud hosting whereby the providers offer the IT infrastructure and services to many end users. The end users cannot be distinguished and have no control with regard to the location of the IT infrastructure. From the technical perspective, [9] there are no major differences between this models with private clouds other than the advanced security levels that are offered on the

latter.This deployment model is suitable for enterprises whose business services include functions such as load management, and host application that is based on the SaaS model. It is additionally suitable for enterprises that management applications that are used by many consumers. The deployment model is popular in enterprises because it is deemed to be economical. This is attributable to the fact that the deployment model reduces, to a significant extent the operational costs and capital overheads. The enterprise can offer the services for free or by requiring the purchase of a license policy on a per user basis. The cost of public cloud is shared by the end users. As such, the deployment method benefits largely from the economies of scale. Good examples of public clouds include Google and Amazon.

3.4.2 The Private Cloud

Also referred to as the internal cloud, this deployment model of cloud computing is implemented in more secure cloud based environments whereby firewalls are used to safeguard the activities of the end users. The said firewalls are governed and managed by the respective IT department of the enterprise. Since this deployment method allows access only to the authorized users, enterprises are assured of control over the security of their data. In this deployment model, regardless of the physical location of the IT resources (internal or external) the model will provide them to form a precise pool of the private cloud services. Observations in [7] shows that since enterprises have unforeseen and dynamic needs, using this model for the assignments that are critical such as security alarms, uptime requirements and management demands would be done more efficiently using the private cloud deployment method. [12] Agrees by claiming that the obstacles pertaining to security can be avoided using this deployment method.

3.4.3 Community Cloud

This type of cloud hosting entails the sharing of resources by many enterprises that are in the same community. A good example is banks and trading organizations. The multi-tenant set up of the community cloud is shared among the companies that are in the same group and share the same computing apprehensions. In general, the members of the community have similarities with regard to aspects like security, privacy and concerns. The primary intention of the communities is the achievement of the related business objectives.

Observation in [2] shows that community clouds can be managed internally or managed by a third party service provider. In addition, the deployment model supports both internal and external hosting. The cost of the community cloud is shared by the member organizations of the community and therefore has advanced capacities with respect to cost savings. This deployment method is more suitable for the enterprises that work in joint ventures and tenders such that their operations need to be on a centralized cloud computing platform. The platform manages, builds and implements similar projects for the enterprises in the community cloud.

Research shows [7] that organizations are becoming increasingly aware of the potential of cloud hosting. In this regard the section of the best and most appropriate type of cloud hosting is a critical business decision. This calls for the management to identify its huskiness demands and align it with the most appropriate cloud deployment model. Upon the selection of the best model, the enterprise can achieve the business goals easily and additionally channel their efforts in a way that drives business success.

3.4.4 Hybrid Clouds

Hybrid clouds refers to the integrated deployment methods of cloud hosting. [14]Indicates that hybrid cloud can either be the avengement of more than two servers. In other words, it can be the integration of private, public or community clouds that are bound but are treated as separate entities. The individual benefits of the deployment methods are incorporated in hybrid clouds [15]. [4]Observes that hybrid clouds can go beyond isolation and therefore overcome the boundaries of the provided limits. They allow the users to significantly increase the capacity as well as capability through aggregation, customization and aggregation with other cloud services. In this deployment model, the IT resources and infrastructure are managed as well as provided internally or externally by third party service provider. [1] Describes it as the adaptation of two platforms whereby the work load is exchanged between the public and private clouds depending on the needs and demands of the enterprise.

According to [14]enterprises can host resources that are not critical such as the test and development workloads in the public cloud that is owned by external providers. On the other hand, the sensitive and critical resources can be hosted internally. A good example would be an E-Commerce enterprise that are hosted on private clouds. The websites benefit from advanced security as well as scalability. However, for the brochure site of the company they can use the public cloud since the security is not a prime factor of concern and would be more economical compared to the private cloud. On the contrary, enterprises that are more focused on security such as banks can use the hybrid clouds. During the peak season such enterprises can scale the public cloud to include the specific applications that would assist them to meet their IT needs. This phenomenon is referred to as cloud bursting and is among the most fundamental features of hybrid cloud.

Among the common applications of the hybrid cloud by enterprises is the processing of big data. On private clouds, the approach can be used to retain data while the process of initiating analytical queries can be done over the public cloud. Other than having disadvantages such as interface incompatibility issues, capital expenditures and network connectivity problem, the hybrid cloud is suitable for enterprise because of its scalability, security and flexibility.

3.5 Drivers of Cloud Computing

The main drivers of cloud computing in an enterprises can be seen in the Figure: 7. The subsequent discussion details why enterprises are choosing to move towards cloud implementation. The main benefits of cloud computing according to a clutch study [23] that involved data from 300 enterprises are shown in this Figure: 7 below.

3.5.1 Cost Flexibility

This is the primary driver of the adoption of cloud computing in enterprises. A research by the Gallup group revealed that at least 31% of the executives that were surveyed cited the ability to reduce the fixed costs of IT and the flexibility of shifting to the more variable of the pay as you go technique as a top benefit [3]. Researchers observe that using the cloud can assist enterprises to reduce the costs of IT infrastructure by enabling them to shift to the operational expenses rather than the capital expenses. According to [13]the capital expenses

of IT mostly comprised of licenses, servers and networking infrastructure are less fluid costly and unpredictable compared to the routing operating expenses. When the enterprise shifts to cloud applications, the need to build hardware and install the application is eradicated. In addition, the adoption of the cloud services can enable the enterprise to shift form fixed costs to variable costs. The enterprise simply pays for the resources needed when it

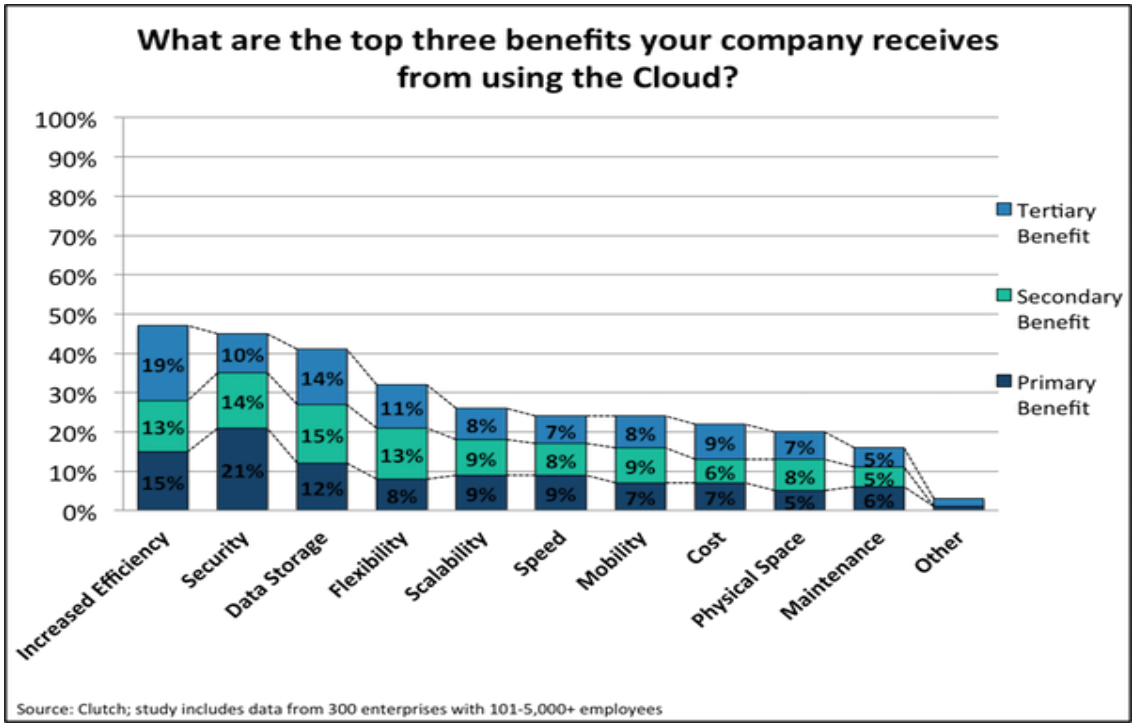

Figure 7. Drivers of Cloud Computing [23]

needs them. The model not only increased flexibility but also eradicates high capital expenditures.

3.5.2 Business Scalability

IT scalability is appreciated as among the top benefits of cloud adoption. Notably, the cloud offers more than scalability since it enables companies to scale the business operations. By enabling the provision of the needed resources with no limitations on the scale, the cloud allows companies to reap from the advantages of economies of scale. The recognition of the ability of the cloud to drive effective decisions with regard to growth and expansion was cited as third in an IBM survey [11].

3.5.3 Masked Complexity

Aside from enabling business scalability as well as market adaptability, cloud adoption also offers companies the capacity to benefit from masking complexity. As revealed by [14]the cloud enables organizations to hide some of the operational intricacies from the customers. This can help attract a wider customer base. Since complexity is veiled from the customer, the enterprise can easily enhance the sophistication of its products and services without letting the user acknowledge changes needed to maintain the product or the service. For instance, the company can carry out its upgrade and maintenance operations in the background without disclosing this to the end users.

3.5.4 Context Driven Variability

Due to the computing power and capacity of the cloud, the cloud can store information regarding the preferences of the users. In turn, enterprises can use this information to facilitate the process of customization [9]. The variability which is context driven allows companies to provide personal experiences to the customers. The variability also adapts to any subtle changes in the customer defined context which allows for a more customer-centric experience.

4 Strategies for Enterprise Cloud Security

An enterprise's cloud security posture can be measured by the maturity, efficiency and the completeness' of the security controls that have been implemented [13]. The security controls of cloud security in enterprises are implemented in the facilities, network infrastructure, IT systems, information as well as the applications. Furthermore, enterprise cloud security measures are also implemented at the processes and people levels as is the case in the separation of tasks and change management [1].

As noted in the earlier chapters, the responsibilities of cloud security in enterprises are shared by the provider and the consumer. However, their responsibilities differ to a considerable extent. For instance, the AWEC2 IaaS offering from amazon comprises of the responsibilities of the vendor and includes the implementation of cloud security to the hypervisor [3]. This means that the service provider only address the security issues in the physical, environmental and virtualization realms. In turn, the consumer in this case the enterprise takes on the responsibility for the security measures related to the IT system. This includes the OS, applications as well as the data. The inverse holds for the CRM offering from Salesforce. Com. This is because the service providers offer the entire stack [14]. In this model, the provider is responsible for the physical, virtualization and environmental security controls as well as the responsibilities of ensuring the security of the applications, data and the infrastructure. This model alleviates most of the direct responsibilities of the consumer (enterprise).

Since enterprises don't understand the technicalities of cloud security, a cloud security evaluation checklist is used to have a common way of verifying their Enterprise's security, as well as get assurance from the Service providers regarding their security [4]. One of the fundamental applications of the checklist is that the enterprise can use a predefined set of questions that can assess the level of security, as well as identify the security vulnerabilities that the enterprise is exposed to. The subsequent discussion highlights key considerations in the elements that make up the cloud security evaluation checklist.

4.1 Foundational Enterprise Security

Before the implementation of the cloud services enterprises should first create a security policy that details the requirements as well as the rules of the enterprise with regard to security [1]. The security policy can be used to delineate the constraints as well as the requirements that the processes and people operate in. In addition, the policy acts as the enterprise's security intent. The actions taken regarding security need to be traceable in the policy. Policies have different classes including the general security policy and the extra policies that address specific areas [11]. To ensure cloud security, the enterprise would need to implement both types of policies.

Augmenting the security policies are the statements that clarify the requirements for specific protocols. These are defined as the standards and involve realms such as technical security controls [13]. The standards of an enterprise state the actions that are mandatory with regard to the maintenance of security. Finally, an enterprise needs to have set guidelines that is oriented toward the best security practices in the company. The guidelines are made up of the description of safe practices that would support the aims of the security policy. Prior to the implementation of cloud services, an enterprise needs to have the security policy, define its security standards and provide a document that issues guidelines that promote security.

Before the implementation of the cloud services, the enterprise should ask the following questions:

• Has the enterprise clearly documented a security policy? Has the policy been represented and approved to the parties concerned? Does it represent the management intent?

• Has the security policy been reviewed by the legal representatives?

• Is the policy augmented with the relevant guidelines and standards?

• Does the enterprise have a privacy policy that augments the security policy?

• Are the policies, standards and guidelines in a line with the industry standards?

• Does the enterprise hold third parties to similar policies and standards?

4.2 Transparency

An enterprise needs to have control regarding the customer data stored in the cloud. To do this, the enterprise would need to be transparent about data handling. The service providers have to issue the company with clearly stated policies as well as procedures the location of the customer data and additionally assist the enterprise to secure it [13]. The enterprises also need to be aware of the people that have access to the customer data, and in what circumstances.

Some of the security considerations at this stage of cloud implementation include:

• Does the enterprise know the processes and procedures used by the service provider towards securing their data?

• Does the enterprise know the location of storage and how the service providers manage it?

• Does the enterprise know the people authorized to access its data? Does it know the terms of authorizing access?

• Are the service providers transparent with regard to how they would respond to access to the enterprise's data from the government?

• Can the enterprise review the security standards of the service providers?

4.3 Personnel Security

The operational security issues reside in the personal security culture in an enterprise. The main aim of personnel security is to delineate the security risk classes as well as to help in the development of an environment that foster the security objectives of the enterprise. [14] Notes that in cases where the personnel of the service providers have access to an enterprise's systems and data, then the enterprise would have to have confidence in the trustworthiness of the personnel. To this end, the customer should carry out screening and training to reduce the compromise of an attack by a personnel of the service providers. In addition, the enterprise should ensure that the service providers ensure security screening as well as provide regular training to its personnel. The enterprise should ask the providers how they screen the personnel and also how they managed the personnel that have access to privileged roles [9].

4.4 Third Party Providers

When an enterprise contracts a service provider for cloud computing services, one of the main difficulties is that more than one party will have access to an enterprise data. The service vendors can for example outsource some services in the cloud services contract. In other cases, the vendors could change ownerships after an acquisition. Other than third party access that accrues from the vendors, the enterprise can use a cloud broker [1]. The introduction of the third parties such as the ones mentioned increase the security risk. As such,

it is critical for the client to identify these parties before they implement the cloud service. The enterprise should also ensure that it clearly understands the role of the third parties and additionally make sure that the contract addresses the responsibilities of the third parties.

To ensure cloud security, the enterprise should obligate the service providers to identify the outsourced functions and the names of the third parties [2]. The enterprise should make a requirement that the vendors abode by similar procedures and policies that apply to the vendor personal. The enterprise should also ensure that it has continuity plans in case the third party providers fail.

4.5 Business Considerations

Business considerations is the set of the legal considerations, business continuity considerations and resource provisioning. The evaluation criteria for the security of the aforementioned areas is as described below.

Legal Considerations

These cloud security considerations concern issues such as the jurisdiction in which the data is stored as well as the laws that govern data security in the said jurisdiction. Enterprises should ask the service providers to provide information regarding where the data will be stored, the jurisdiction in which the vendors are incorporated. The enterprise should also require the vendors to give information of any third parties that leave outside the jurisdiction. In addition, the enterprise should be aware of any services and personal subcontracts and establish if they have access to the data and in what terms [14]. Other legal considerations include finding out if the vendors use the data outside the service protocol and whether these vendors have a procedure of responding to legal issues such as subpoenas [9]. Finally, it is important to know whether the vendors are insured against losses which includes the remuneration of the losses experienced by customers as a result of the outages of data leakages.

4.6 Resource Provisioning

This security consideration deals with taking the steps to ensure that the cloud service will be resourced in sufficient measures as the demands of the enterprise increase [13]. To achieve this the vendors would have to take several steps to deliver the cloud services to the enterprise. In turn, the enterprise would need to be aware of the procedures as well as the controls that are used by the vendors to mitigate resource exhaustion. Resource exhaustion can result from oversubscription for processors, network congestion, memory exhaustion and the exhaustion of storage. The enterprise would need to know if the vendors limit their service subscriptions to protect against such incidents. Lastly, it would be important to know if the vendors provide information regarding utilization and capacity.

4.7 Software Assurance

Among the most efficient techniques of ensuring software security is developer empowerment during the process of developing software applications [10]. This can be done by giving the developers access to the tools that test security. The tools can range from code analysis to the testing of web security. [2]Observes that a best practice would be having a development environment that closely mirrors the eventual staging, and production environments. Although this is a challenging process for developers the reduction of deltas between the two environments is a more efficient way of transitioning. In addition, it has less security risks for the client's developers. The enterprise needs to consider issues such as the

controls that have been put in place by the vendors to ensure the integrity of the OS, applications, updates and file configuration. The enterprise also needs to know if the vendors followed the standards, practices and the guidelines of the industry. Importantly [13]observed that having knowledge about the controls that have been implemented to obtain software as well as the configuration file. Finally, the client needs to be aware of the penetration testing that was used by the vendors for each release as well as the step of identifying the vulnerabilities that have been remediated by the vendors.

4.8 Network Security

Network implementation is considered to be the most imperative aspect of network security during cloud adoption. According to [1] the choices regarding the architecture of the systems and isolation that are made during this phases can have far reaching benefits or severe consequences. [9]Observes that network choices in an enterprise begins at the physical level, and the functionality of the equipment. It also includes network virtualization as well as monitoring. The isolation extent is different depending on the traffic cases. Traffic cases include customer access, operations between customers and the management of external access. The aforementioned aspects drive additional security requirements at the system and virtual levels.

The checklist for an enterprise with regard to network security includes asking the vendors about the controls that have been implemented to manage internal and external attacks [12]. The enterprise also needs to have effective isolation management between the hypervisor and the vendors. The enterprise should also ask the vendors to give information regarding the standards as well as the best practices that the vendors have implemented. Another important consideration would be how the VM network manages isolation network hardware routing. The enterprise should also familiarize with the standards as well best practices that are used to implement the equipment and network infrastructure. The responsibilities of enterprises with regard to security management are shown in the Figure:8 below. If the vendors allow penetration testing, the enterprise need to establish whether the testing is carried out from external sources to the cloud, and vice versa. Carrying out vulnerability testing of the infrastructure, cloud management as well as the components that can be used by the user also needs to be performed by the vendor to limit the network security attacks on the enterprise. To this end, the enterprise needs to ask the vendors to provide the vulnerability information and also require that the vendors allow them to carry out vulnerability testing on their own VMs.

4.9 Identity and Access Management

Identity management is an important aspect of network security for enterprises that have adopted the cloud. According to [14]identity and access management entails authenticating the information of personnel that wish to access the data of the enterprise. To ensure security access privileges are assigned based on the role of the personnel. To ensure that the vendors provide the enterprise with stringent security controls with regard to who has access to their data, some of the factors that need to be taken into account include finding out if any of the vendor's controlled accounts have privileges and if so it is critical to identify the precise operations. It is also important to find out the processes used by the vendors to manage the administrative accounts and those with more privileges. Among the techniques used by vendors to ensure network security include the 2-man access controls [8]. The enterprise needs to establish if the vendors use this technique and if they do then they should require the vendors to reveal the specific operations.

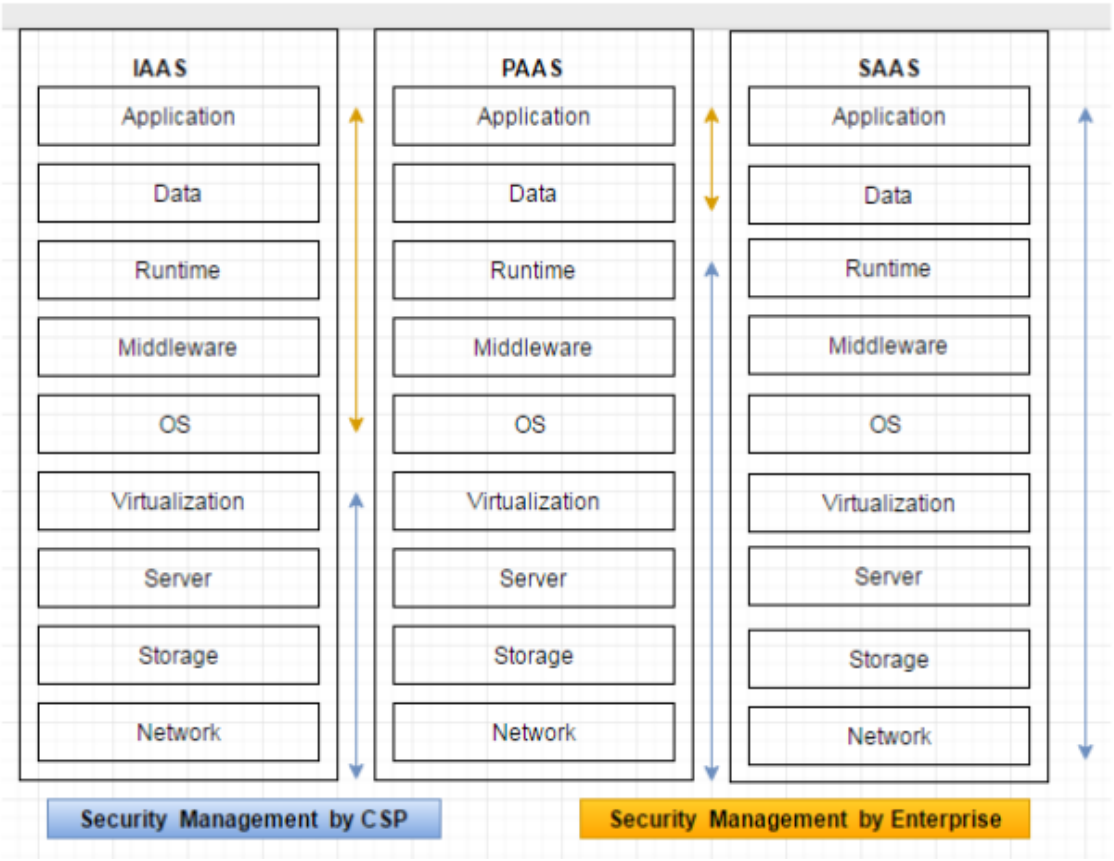

Figure 8. Security Management responsibility in Cloud Service Models

The best service providers reinforce the separation of privileges to limit the access to certain data sets. The enterprise needs to establish the roles that limits privileges such as security, and identity [13]. In the same line, it is advisable for enterprises to implement break glass access, and the circumstances in which such access is offered. It is also imperative to establish the post clean-up process of using the break glass access to mitigate future vulnerabilities [11]. It is also imperative for the enterprise to know if the vendors offer administrative privileges and the limits to this provision. Other important considerations include identity during registration, and the check levels based on the granting of the resources. It is also important to take into account the de-provisioning of the credentials as well as the accounts that would be useful for example when an employee stops working in the enterprise [7].

In some cases, the vendors include the provision the identity and management systems used by the enterprise. In such a case, it is critical to establish whether the service complies with the federated systems of identity management [14]. It is also important for the enterprise to determine whether they can incorporate sign on, role separation, and the verification of the identity the enterprise when the enterprise uses the API to interact with the vendor.

Although the enterprise will implement its own access control mechanism to ensure security, it is also important to ensure that the vendor's covers security concerns such as authentication in the high assurance business operations. The company also needs to know whether the high assurance tasks are limited to the cloud network only. Finally, the enterprise needs to be aware of the procedures used by the vendors in case their credentials and accounts are compromised.

Research on cloud adoption strategies reveals that there are still significant threats in the cloud applications adopted by enterprises. This has been attributed to the fact that the user

endpoints continue to move further from the control of the IT department. In addition, the existing IT equipment and staff in enterprises are not able to handle the existing vulnerabilities and threats. According to [5] most of the IT departments are overstretched and have considerable insufficiencies with regard to the skills and the manpower needed to address the unique and increasing security threats that are borne of cloud adoption.

Recently, there has been a long string of security breaches in enterprises that provide proof of the increasing security pressures of cloud adoption. For instance, Verizon in 2013 reported at least 63,000 security breach cases [5]. Furthermore, there were 1,367 data breaches reported in the company's security investigations report that is published annually. In 2015, at least 395 data centers were breached in the US leaving even top conglomerates like JP Morgan vulnerable to the security threats [5]. In addition, both enterprises and individual users are forcing companies to use cloud applications regardless of their security approval. 73% of the enterprises for instance discovered cloud adoption that were against their security policies. More recently a leak of at least 7 million passwords in the cloud storage Dropbox were leaked leaving legitimate concerns with regard to the security of cloud applications as well as their adoption.

The scenarios above make it evident that the adoption of the cloud services by an enterprise increases the security risks that are developed during deployments if the enterprise does not have revamped, and updated security techniques, training as well as practices. This phenomenon is not because the security threats are part of the cloud. Instead it is attributable to the factor that the discovery, tracking, as well as the protection of technology, systems, devices and the operational boundaries is challenging. Enterprises with high numbers of users, variety of users and more responsibilities are more exposed to the security threats and vulnerabilities. Business driven IT projects also aggregate the security problem since the number of untrained users cause more problems in IT security [6].

With the above security concerns in mind, enterprises that have adopted the use of the cloud needs to implement a security first strategy that is specifically created with security in mind focusing on the fundamental areas highlighted below.

4.10 Maintaining a State of Discovery

During cloud adoption, an enterprise will need to ensure the development and the maintenance of a state of discovery that is consistent with the current security threats and vulnerabilities. This means that the enterprise needs to mitigate the risks that are created by the SaaS and IaaS offerings made by the service providers [4]. In addition, the enterprise needs to be aware of the applications that are being used and their individual security risks.

Enterprises also need to have control access to the cloud applications including the applications that are sanctioned as well as the unsanctioned applications. For instance, the enterprise IT department should ensure that they have federated sign on to the applications of the end users. This places the enterprise in control with regard to the users of the cloud services, and also enables the enterprise to control the data used in the cloud applications [16].

4.11 Data Protection

The next strategy to secure its cloud applications is the implementation of data protection. This is where most of the security techniques reside. Some of the techniques that can be used include encryption, data masking, loss prevention solutions and tokenization, that will play a leading role in protecting cloud based data. The enterprise can also implement endpoint protection against threats as a customized feature of its cloud applications. Since the cloud applications are a collection of physical as well as virtual endpoints, they need a

protection system that would be applied in the servers in the enterprises' data center [19]. Importantly it is fundamental to install antivirus applications as well as other solutions that can detect system vulnerabilities and threats. The company can also install white listing controls that determine the applications that can be installed and executed by the end point users. For instance, the company can have authorized programs that are matched to a database called the "approved" applications [5]. This technique has been proven to be successful in the detecting and blocking of malware cloud applications.

An enterprise also has to have a protection against network threats for its cloud based applications. The network protection techniques can assist to defend the data stores from network attacks. For instance, the enterprise can implement network protection systems that use digital signatures to detect as well as block the network stream from the cloud.

4.12 Security Management

The enterprise also needs to appreciate the role of security management. This is because it is not possible to secure an aspect that is poorly managed. As such, the enterprise will need to put systems in place that will have quick responses in case of a security outbreak. This can only be possible in an environment where there is effective and efficient management of the company's security technologies [8]. Along similar lines, it is important for the company management to acknowledge the importance of compliance in the implementation of security management.

4.13 Fostering Visibility

Ensuring constant and consistent states of visibility is also paramount in fostering security in the cloud based applications used by the enterprise. The management needs to be aware of the personnel, when and where of the cloud based applications to ensure security. [8] observed that security information coupled with event management, as well as the related technologies are among the baseline needs of the security practices adopted by the company. The company can also invest in threats intelligence expertise because the IT staff, including the end users have to stay up to date with the recent threats and vulnerabilities. This can assist the IT department to combat threats before they happen. In this regard, the enterprise should train the end users about the software assets and update them on the threats that exploit the vulnerabilities of the assets.

4.14 End User Training

Cloud based security threats can also be averted through the provision of security training for the end users. According to [5]the end users have been identified as the weakest link in enterprise cloud security. As the proliferation of the technological devices, social communication and the internet the users are only a click from compromising the entire security of an enterprises network. This is increasingly the case for the users that use laptops who are more exposed as a result of the limited protection they get from the security mechanisms of the company's network. [3] Notes that the existing defences are not only difficult to use, but hard to manage as well. As such it is not uncommon for the enterprises to give the employees administrative rights to facilitate the free use of all the software and applications. This practice gives malicious attackers access to information including intellectual property and credit card numbers. An enterprise can train its end users with regard to how to protect the data and information they access through their mobile devices and the best practices that will prevent cloud attacks.

4.15 Differentiate Compliance and Security

It is also important to differentiate between compliance and security. According to [13]the auditing techniques cannot match with the recent security threats. As such, it is important to assess if the strategy is more prioritized on passing security audit reports than the implementation of actual techniques that will mitigate threats and foster data protection. It is also critical to ensure that the company is not being to risk aversive. Some companies have been known to use the lock it all down technique that slows growth, agility, as well as the opportunities [7]. It is paramount to view risks as a spectrum rather than a binary aspect. This will enable the company to make strides in the understanding of risk as a component of all cloud implementations.

4.16 Handling Sensitive Data

The company should also establish its most important data and where it resides. It is also important to know the size of this sensitive and important data and the applications as well as users that can access this information [10]. Lastly, the IT department needs to be aware of the business processes that rely on the sensitive data, and this will enable the department to pay more attention on its resources and where it would be most useful.

4.17 Assessing Similar Cloud Deployments

It is also critical for the enterprise to assess the success of cloud deployments used by other companies that were provided by the same service provider. While most of the cloud solutions provided by most vendors are attractive on paper, they have proven to have high security vulnerabilities upon deployment [9]. In this regard, in its efforts to mitigate deployment risk, the enterprise can carry out research on other organizations that have executed the configuration they are planning to implement. Part of this process would be identifying relevant examples of the functional points, ROI and the proof of additional business value. The enterprise can also seek third party confirmation through past anecdotes as well as awards. In addition, they should seek information from the vendor regarding the successful use of the application to solve the challenges that the company seeks to solve [18]. Among the additional information asked for include customer references.

4.18 Service Level Agreements (SLAs)

SLAs enable the company to develop the much needed alignment between the company and the service providers. Although the company may avoid developing exclusive dependence on the agreement prior to the alignment, or cloud implementation, it has been identified as a necessary backdrop [5]. This means that the company should invest sufficient thought and effort in the SLA. [5] suggests a mature as well as professional cloud vendor that provides the necessary security information. Some of the considerations that will assist the company to evaluate the SLA provided by the vendor include establishing if the agreement is relevant to the security areas that need to be aligned [19]. This include storage and performance security. The enterprise should also establish if the agreements are aligned with their objectives. According to [14] cloud applications rely on the enterprises subscription model. This means that much of the enterprise does not have to purchase a perpetual license, it can use the application for a predefined duration. Since the vendor's business model is dependent on the enterprise renewal, most of the vendors have developed incentives that prioritize on customer satisfaction [20]. An enterprise should take advantage of this objective to demand cloud application services that prioritize on data security and the mitigation of security threats.

4.19 Controlled Use of Administrative Privileges

Cloud adoption adds a new aspect with respect to the administrative accesses. This aspect is referred to as the cloud management console [8]. In cloud adoption, the security set up entails the development of a root account that allows access to the applications as well as the functions in the console such as billing and management. Implementing the controlled use of the administrative privileges of the enterprise cloud applications will ensure that the employees can only access the applications needed to carry out their jobs, but restricted access to the other applications. The enterprise can use the cloud application to create administrative accounts that have granular permissions across the whole cloud infrastructure. Amazon makes the recommendation for the storage of the credentials associated with the root account as well as the creation of general user accounts that are used by the administrator or the application that the employee needs access to [5]. The administrator can subsequently delegate the permissions for the accounts according to the need.

An enterprise can also use security policies to reinforce the authentication process for the applications that need administrative privileges. To this end, the enterprise should ensure that the vendor issues federated accounts that allow the active directories to login to the main console [9, 4]. The use of the federated accounts will ensure removal of access as part of the employee's termination process since the account held by the employee be removed or disabled.

5 Conclusion

The first research question aimed at investigating the current and future states of enterprise cloud adoption. The findings indicate that the adoption of cloud computing has gained a high level of traction that have been fostered with significant technological developments that present, better, faster and more efficient ways of harnessing the immense potential and capabilities of the paradigm. Using different techniques of evaluating the current state of cloud adoption, the thesis concludes that cloud adoption is high in the leadership pipeline as the global market of cloud services reached $131 billion in 2014. This resulted in the establishment of more cloud players that in turn created offerings that can be used effectively by enterprises. The thesis showed that the cloud market is led by leaders such as Amazon and Salesforce which are followed closely by other companies like Google, IBM and Microsoft that continue to increase the gains of cloud adoption. The thesis concludes that since cloud adoption is perceived as a technology enabler, it is currently being extolled for increasing the speed as well as the flexibility of business operations. In addition, enterprises are moving towards the use of cloud based applications, field force connections and the improvement of their processes through cloud adoption. As such, most enterprises are making more investments in cloud adoption. An increasing number of enterprises are also considering the cloud as an integral component of their continuity strategies, as they continue to use the cloud offerings such as web services, communication, and management applications to foster their business outcomes. With regard to the future state of cloud adoption, the thesis concludes that cloud technologies including Open Stack and Cloud Stack from Apache will increase their customer base especially with the possibility of providing equal technology across different segments to create a fair playing ground for enterprises in the various industry segments [21]. For instance, the PaaS framework has a renewed strategy that will create a cloud ecosystem that will impact public cloud adoption by enterprises. It is also postulated that cloud computing will become a must have for enterprises as they continue to innovate. As such, cloud adoption will propel in the future, and is likely to enhance trends such as delivery of insights through big data analysis, and auto collaboration systems between machines that will in turn deliver safer and better business experiences.

The second research question guided the analysis of the current security challenges that is faced by enterprises which use cloud computing services. The thesis conducted a systemic review of existing literature to establish the challenges. It was observed that while cloud computing as well as virtualization assist enterprises to break the physical barriers between the infrastructure and the users, they are forced to overcome heightened security threats and vulnerabilities. Some of the security challenges that firms are exposed to include the loss of control over some IT aspects such as privacy which have to be reassessed by costly security models. It was also observed that the security of an enterprise's data is heavily dependent on having a reliable cloud service provider, and vendor. Since the enterprises share the IT resources with other companies, they have no knowledge of the physical location of the resources [22]. This vulnerability exposes the firm to government seizes as a result of legal violation by another company. In addition, the storage services provided by the vendor are sometimes incompatible with the services offered by a different vendor making it difficult for an enterprise to change from one provider to the other. A significant amount of risk also accrues from third party access to the data of an enterprise. This is especially the case for firms that outsource some of their needs. This vulnerability translates into the creation of legal contacts to protect corporate data as well as the use of SLAs.

Other than the challenges above, cloud adoption also results in the mobile access of an enterprise's data without having to traverse the corporate network. Besides this, the placement of big data in accessible cloud leaves the enterprise open to distributed attacks from virtual

locations. The thesis also observed that the virtual machines, servers, and enterprise applications use the same operating system in cloud computing. This increases the security attacks on the aforementioned aspects remotely. The thesis concludes that the virtual machines are more susceptible to such attacks since they crisscross the public and private clouds. It was also concluded that a shared cloud environments have more attack surface and therefore pose a greater security risk compared to the dedicated environments. The thesis concluded that in a bid to benefit from the gains of cloud computing including the cloud savings, enterprises are adopting the use of cloud services without taking the security implications into consideration. In order to successfully use the cloud based applications, enterprises need to create virtual machines that are self-defending, and develop perimeter security that integrates, firewalls, intrusion detection, prevention systems, and network segmentation. In addition, in light of the increasing security threats and vulnerabilities, enterprises also have to implement monitoring tools, and security policies that control the security of the data outside its perimeters.

The third research question investigated the security strategies that can be used to counter the cloud security threats and vulnerabilities. The thesis concluded that the security posture of an enterprise can be measured by the maturity, efficiency and the completeness' of the security controls that have been implemented. It was observed that the security controls of cloud security in enterprises are implemented in the facilities, network infrastructure, IT systems, information as well as the applications. These strategies can also be implemented at the processes and people levels as is the case in the separation of tasks and change management.

Prior to cloud adoption enterprises should create a security policy that details the requirements as well as the rules of the enterprise with regard to security. The security policy can be used to delineate the constraints as well as the requirements that the processes and people operate in. In addition, the policy acts as the enterprise's security intent. The service providers have to issue the company with clearly stated policies as well as procedures, the location of the customer data and additionally assist the enterprise to secure it. The enterprise also needs to be aware of the people that have access to the customer data, and in what circumstances.

After the implementation of the security policies and transparency between the enterprise and the vendors, the next security strategy would be ensuring network security. Network implementation is conserved to be the most imperative aspect of network security during cloud adoption. Some of the strategies that can be used to enhance network security include asking the vendors about the controls that have been implemented to manage internal and external attacks. The enterprise should also implement isolation management between the hypervisor and the vendors. In addition, it should ask the vendors to give information regarding the standards as well as the best practices that the vendors have implemented. The other important strategy would be learning the VM network manages isolation network hardware routing. Lastly, the enterprise can align with the standards as well best practices that are used to implement the equipment and network infrastructure.

The implementation of data protection techniques is concluded as a stringent security strategy for cloud adoption. Some of the techniques that can be used include encryption, data masking, loss prevention solutions and tokenization, that will play a leading role in protecting cloud based data. The enterprise can also implement endpoint protection against threats as a customized feature of its cloud applications.

The thesis also concludes that it is critical for the enterprise to assess the success of cloud deployments used by other companies that were provided by the same service provider.

Although most of the cloud solutions provided by most vendors are attractive on paper, they have proven to have high security vulnerabilities upon deployment. An enterprise also needs to differentiate between compliance and security. It was concluded that the auditing techniques cannot match with the recent security threats. As such, it is important to assess if the strategy is more prioritized on passing security audit reports than the implementation of actual techniques that will mitigate threats and foster data protection.

The thesis concludes that cloud security for enterprise is a standard procedure rather than an optional luxury. Among the set of best practices to ensure cloud security include learning the difference between the three cloud computing models IaaS, PaaS and SaaS to enable the selection of the most appropriate and secure deployment model. After selecting the best deployment model an enterprise also needs to have a Service Agreement License with the vendors. This practice will ensure that the enterprise has full control from its IT department as well as its security team. The SLAs will ensure that issues such as unavailability of the infrastructure, DDoS attack and other security incidents are discussed in the contract. The other best practice of having a specialized protection system for the enterprise perimeter. The thesis observed that since the cloud security goes beyond firewalls, the firm's vendor needs to provide strong perimeter protection that includes anti-spam, anti-virus, intrusion detection tools, monitoring, log correlation, content delivery network, and other tools for attack mitigation. The enterprise should also ensure that it holds the firewall that segregates the servers, users and the network this will ensure the segregation of sensitive data such as credit card information. The thesis also concludes that carrying out frequent vulnerability analysis is an effective security best practice.

Research question five aimed at analysing the perspective of the service providers with regard to cloud security. The research observed that most service providers recognize the importance of the secure implementation of cloud services. To ensure security, the service providers provide additional security services that can enhance the security of their basis cloud offers. For instance, Amazon Web Service Offers a VP cloud service that increases the security through the mitigation of threats that result from multi tenancy. The vendors provide security segregation through cryptography. Other service providers provide host based firewalls, as well as the use of IP addresses to control the people that can access cloud applications and services. The thesis concludes that service providers take cloud security seriously and have mechanisms to mitigate threats and vulnerabilities.

5.1 Future Work

Vulnerabilities in a cloud computing environment can be exploited by cyber criminals as well as other individuals with malicious intent. However, as seen in the thesis the issue of cyber security is not owned by a single entity. As such, there is the need to develop a broader view to promote transparency, as well as confidence building among the service provides, enterprises and government agencies that use cloud services. Future work should investigate how the aforementioned entities can work cohesively to ensure more security when using cloud based services. Future work should investigate on how the private and public sectors can work together to develop as well as validate effective measures and controls. This would involve researching on the standards that prescribe certain minimum requirements needed for cloud security.

6 References

[1] G. Booth, A. Soknacki and A. Somayaji, "Cloud Security: Attacks and Current Defenses," 8 Annual Symposium Information Assurance, vol. 3, no. 1, pp. 4-5, 2013.

[2] T. Steiner, "An Introduction to Securing a Cloud Environment," GIAC (GSEC) Gold Certification, vol. 1, no. 1, pp. 1-18, 2012.

[3] I. I. Centre, "Cloud Computing Research for IT Strategic Planning," Intel IT Centre, vol. 1, no. 2, pp. 1-8, 2012.

[4] J. Archer, D. Cullinane, N. Puhlmann, A. Boehme, P. Kurtz and J. Reavis, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0," Cloud Security Alliance, vol. 1, no. 1, pp. 1-31, 2011.

[5] J. M. Allen, "Implementing the Critical Security Controls in the Cloud," SANS Institute, vol. 1, no. 1, pp. 1-38, 2016.

[6] I. M. Abbadi and C. Namiluko, "Dynamics of trust in Clouds—Challenges and research agenda.," a. In Internet Technology and Secured Transactions, vol. 4, no. 1, pp. 100-115, 2011.

[7] J. G. M. Al Morsy and I. M¨uller., "An analysis of the Cloud Computing Security Problem," Asia Pacific Cloud Workshop, vol. 2, no. 1, pp. 42-69, 2010.

[8] I. K. C. Cachin and A. Shraer, " Trusting the cloud," ACM SIGACT, vol. 40, no. 2, pp. 81-86, 2009.

[9] D. Catteddu., "Cloud computing: benefits, risks and recommendations for information security," Web Application Security, vol. 1, no. 3, p. 17, 2010.

[10] ORACLE, "Architectural Strategies for Cloud Computing," An Oracle White Paper in Enterprise Architecture, vol. 1, no. 1, pp. 1-21, 2009.

[11] G. Kaefer, "Cloud Computing Architecture," Siemens, vol. 4, no. 2, pp. 1-10, 2010.

[12] S. Microsystems, "Introduction to Cloud Computing Architecures," Sun Microsystems, vol. 1, no. 1, pp. 1-18, 2009.

[13] E. Gorelik, "Cloud Computing Models," CISL, vol. 1, no. 1, pp. 1-45, 2013.

[14] G. Breiter, "Cloud Computing Architecture and Strategy," IBM, vol. 1, no. 1, pp. 1-12, 2010.

[15] T. Dillon, E. Chang and C. Wu, "Cloud Computing: Issues and Challenges," 24th IEEE International Conference on Advanced Information Networking and Applications, vol. 1, no. 1, pp. 27-33, 2010.

[16] K. Jeffery and B. Neidecker-Lutz, "The Future of Cloud Computing," European Union, Belgium, 2010.

[17] L. Schubert and K. Jeffery, "Advances in Cloud Future of Cloud Computing," European Union, Belgium, 2012.

[18] G. Menegaz, "The future of cloud computing: 5 predictions," IBM, New York, 2014.

[19] K.-K. R. Choo, "Trends & issues in crime and criminal justice," Australian Insitute of Criminology, vol. 1, no. 1, pp. 1-6, 2010.

[20] E. Johnson, "The Future of Cloud Computing Security," Business 2 Community, New York, 2013.

[21] H. Takabi, J. Joshi and Gail-Joon, "Security and Privacy Challenges in Cloud Computing," IEEE Computer and Reliability Societies, vol. 1, no. 1, pp. 24-30, 2010.

[22] N. M. Turab, A. A. Taleb and S. R. Masadeh, "Cloud Computing Challenges and Solutions," International Journal of Computer Networks & Communications, vol. 5, no. 5, pp. 209-216, 2013.
[23] "Best Cloud Service Providers - 2016 Reviews | Clutch.co", Clutch.co, 2016.[Online]. Available:https://clutch.co/cloud#survey. [Accessed: 06- Dec- 2016].

Appendix

I. Glossary

AWS	AWS is cloud computing services offered by Amazon
SP	Refers to the term _ service providers
IT	IT refers to the term Information Technology
SLA	Service Level Agreements
SaaS	Software as a service
NIST	Refers to National Institute of Standards and Technologies of the United States Department of Commerce.
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
PaaS	Privacy and Anonymization as a Service
HaaS	Hardware as a Service
DaaS	Data storage as a Service
SaaS	Security as a Service
XaaS	Anything as a Service

II. license

Non-exclusive licence to reproduce thesis and make thesis public

I, **Mohit Kinger**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Enterprise Cloud Security Guidance and Strategies for Enterprises,

(title of thesis)

supervised by Andro Kull, Raimundas Matulevicius

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.12.2016**