CHAPTER TWO: REVIEW OF LITERATURE
CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.0 Chapter Introduction

An Empirical and Conceptual literature had been reviewed with regard to the Research Topic in order to get in-depth knowledge and idea of subject matter “Cloud Computing, SPI Models and Technologies” which resulted to a comprehensive summary and assessment of the series of present and previous resources dealing with knowledge and understanding in a given area of research. The main purpose of the review is to find out more about the research topic/project, in order to form its background, and also provide comprehensions into previous work. This comprises a review of a scholarly paper, that includes current knowledge be it a functional findings, theoretical and or methodological contributions to a specific area of cloud computing and security threats or research that comprehend the secondary sources of research, it also serves as the important preliminary responsibility of a researcher in order to discover and review current literature that relates to a research area. The purpose of this literature review is to incorporate the researcher’s study into a wider framework of significant theory and research in relation to the effectiveness and concept of cloud computing, security issues in services models, deployment models and various technologies of cloud computing. This chapter will explore and evaluate the effectiveness and concept of cloud computing and also look at its adoption in Nigeria. These will be further enumerated under the following headings so as to define some of the objectives and answer some of the research questions:

2.1 The History and Theory of Cloud Computing

It’s quite wonderful how recurrent the IT world stands. A lot of evaluations to how the mainframes computers developed decades ago facilitates the emergence of cloud computing. In recent times, in accordance with the history Cloud Computing is the major technology that is striving in the market. It all started as the initial stage of data processing when single computer is created in 1941, \[24\]. After which the need for sharing data among computers was introduced and referred as Interconnection of Computers “Networking” was reported in 1950. The data before shared among computers needs a “Server” A server is used in assisting multiple clients to share data and information across. Therefore, server and client model was introduced for efficient data
sharing in 1976. As a result access to server by clients and many connected computer to the server is formed in 1977 (Computer Group Network), the server started processing lots of information resulting to the formation of (Big Computer Group Network). Moreover, because of the large numbers of computers existing in 1982 the network started collapsing, then era of local client and remote server where server spaces are rented in 1983, instead of continue renting data space, an idea was initiated to rent the server, operating System (OS) and the software. That’s the beginning of full pledge Cloud Computing Era in 2000 when clients are connected to the cloud via the internet. The figure below will best describe the about explanation with regards to the History of Cloud Computing.

Figure 10: A Graphical Presentation of Cloud History
The origin of Cloud Computing started as early as 1960-1970s theoretically, which shows a collective idea with that of mainframe era. Unlike the present day clouds that possess the essential architecture of computer clusters. The Mainframe era, Abstraction Layers, High-performance Computers (HPCs) as well as connections to data need to be seamlessly accepted in the early days of cloud. Therefore, access to clouds need to be dependable as well as universally sufficient to drop off the detector of users. As early as 1960, although, John McCarthy a computer scientists predicted that computing services would remain preserved as a public service. After very long time, networks and Internet sustained to make processing an additional abstract part of the computing. However, [26] emphasized that the Cloud Computing Concept initiated from telecommunication companies shifting to Virtual Private Network (VPN) the table below describes the changes from 1999 to 2009, that is about ten (10) years gap of evolution.

Table 1: Cloud Computing Evolution

<table>
<thead>
<tr>
<th>YEAR</th>
<th>CLOUD EVOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>SALESFORCE.COM-DELIVERY OF APPLICATIONS VIA WEB.</td>
</tr>
<tr>
<td>2002</td>
<td>AMAZON LAUNCHES AMAZON WEB SERVICES (AWS).</td>
</tr>
<tr>
<td>2006</td>
<td>GOOGLE DOCs, AMAZON ELASTIC COMPUTE CLOUD (EC2).</td>
</tr>
<tr>
<td>2008</td>
<td>EUCALYPTUS.</td>
</tr>
<tr>
<td>2009</td>
<td>MICROSOFT AZURE.</td>
</tr>
</tbody>
</table>

Abstraction and the change to computing as a public service, seized a countless stages advancing while the theory of Software as a Service (SaaS) was established. As relation between applications and hardware persistent to decline, information technology experts explored for innovative techniques to define systems that ensued of different mechanisms organized with certainly not concern to locality of every single piece. The Internet had already remained discussed by many scholars and researchers as “cloud” for sign used to signify Internet in
network illustrations and currently to incorporate development towards SaaS and Web 2.0 as general computing technologies.

Cloud computing is in several instances, reappearance to be the centrally synchronized combination of mainframe period: The personal computer (PCs) provided users chance to strike back against and exclusiveness common to the previous era as an alternative of letting additional cooperative incorporation of the innovative resource. Cloud computing can be a counterreformation that gets with it the opportunity of certain factual presentation successes for users and various organizations. Furthermore, According to [24] the humble beginning of Cloud Computing dated back to 1950s while large scale mainframes where obtainable to schools and corporations. Mainframe Comprises hardware, infrastructure, which are all installed in the server room, whereby the server room only holds a single mainframe. Several users are able to access the mainframe through the Dump Terminals Stations with the self-function facility and access to mainframes. Due to the high price of purchasing and maintaining mainframes, corporations where able to report to its users, it became practice to permit many users to share access to the same data storage layer and CPU power from several stations through allowing collective mainframe access and organizations will get a very Return of Investment (ROI) in an elegant piece of technology. Virtualization changes the whole thing, after about twenty (20) years in 1970s. IBM Company released an operating System (OS) that allow many mainframes system to have multiple Virtual system over Virtual Machines (VMs) in a single physical load. New IBM OS takes over in 1950s with application for shared access of the mainframe to the next level by permitting numerous distinct compute environments to stay in the same physical environment. The greatest elementary function of several virtualization software at the present time can be traced back to the slowly IBMOS and virtualization became a technology driver and one of the biggest revolution in telecommunication and computing.

2.2 Grid Computing, Virtualization and Automation

According to [62] Grid computing is the arrangement of distributed computing whereby a “super and virtual computer” is composed with collection of networked, loosely-coupled computers, acting in performance towards accomplishing very large responsibilities. The grid computing technology has been practically used in computationally-intensive scientific, mathematical, and academic problems over volunteer computing, besides it’s sometimes used in profit-making
enterprises for many different applications like seismic analysis, economic forecasting, and back-office data processing in support of e-commerce as well as web services.

The only different of grid computing and that of a typical cluster computing systems as at then is grids have a tendency to be more lightly coupled in diverse, and geographically distributed. Similarly, however a grid computing could be dedicated to a particular application, it’s sometimes built with help of general purpose grid software libraries and middleware. Grid computing grades an intermediate stage among clusters and clouds. Grid computers remain distant more broadly distributed compare to clusters, and the hardware have a tendency to remain slightly more abstract.

2.2.1 Virtualization Technology

As discussed briefly in previous part the significant aspect in development toward cloud computing evolution has come through better adoption of virtualized PC operating systems \(^{17}\), considering the mainframe world, PC operating system engineers practicalized past knowledge in order to permit full server systems to exist in a virtual container on a host, therefore letting for additional comprehensive application of host system resources while keeping control. Virtualization is the key concept and mechanism behind a cloud computing \(^{47}\) this lead to discovery of major types of this building block of cloud computing as network, storage, server, desktop and application virtualization respectively \(^{48}\).

2.2.1.1 Network Virtualization

Nowadays, there is a prevalent use of Infrastructure as a Service (IaaS) in the area of networking, most especially the Wide Area Networks (WANs) this comprised of a massive and expensive network of fixed, leased and dial-up lines that connected the different units in organizations. Distributing the use of a previously existing infrastructure with additional organizations was establish to be much more effective \(^{17}\). The “virtual” migration in this regard is by making use of a “virtualization layer” that connects single machine or device to the network.

2.2.1.2 Storage Virtualization

Data was normal stored in various storage devices, that is all data are saved on the memory of computers locally and accessed by any user that has an access to a particular system. But then, Storage virtualization is used by cloud computing technology in storing the user data virtually in
mass using same “virtualization layer” which presents a portion of a larger whole, as a precise dedicated facility to users.

More innovative use of storage virtualization is what Amazon has been providing since 2002 as a form of the Amazon Simple Storage Service (S3). Objects (files, images) can be stored and recovered using a simple Web Service Interface. Example of such are the Flicker, Slideshare and Twitter that uses S3 storage services. Remote virtual storage does suggest some changes on exactly how data is stored and managed.

2.2.1.3 Server Virtualization

Before the invention of cloud computing organizations uses normal in-built servers that are access within the premises of such organizations, which consist of high capacity servers that contain information like staff data, payroll and many others. Server virtualization is presently the greatest significant, and definitely the greatest debated type of virtualization. This type of virtualization shared physical infrastructure like the VMware, the Elastic Compute Cloud (EC2) service launched by Amazon in 2006 is alternative service that allow organizations to charge such virtual servers over the Internet (IaaS) Physical servers are almost never used after configuring the virtual server using virtualization layer optimization also known as (Hypervisors).

2.2.1.4 Application Virtualization

Apart from the network, storage and server virtualization there is similarly an application virtualization; Application virtualization is all about traditional PC applications that are operational within a “virtual box” which permits them to be installed faster.

The virtual box comprising the application is basically loaded as an image and make sure other applications are not in conflict with others because all are in various virtual boxes, sad also does not change the underlying operating systems.

2.2.1.5 Desktop Virtualization

Desktop virtualizations are when the desktops no longer workings using the software been installed on local desktop machine, but rather make use of a virtual machine that is installed on a server (either at the office or in the cloud) which in turns supports the resource sharing. Like the Sun’s virtual travelling thin client based desktop.
2.2.2 Automation

Automation is one of the substantial advantages of cloud computing. So, Virtualization needs to be in the same path through automation. A cloud environment indicates dynamic scaling capacity based on demand. Organizations create as well as configures virtual machines manually, this development results in a very slow in processing data and information. Therefore, when automated it supports the processes very fast \[^{17}\]. Automation without virtualization would not work, as the application complication is expensive. Automation is significant to virtualization due to its dynamic scalability. Implementing virtualization itself eases the complication to a level that makes automation possible.

2.3 Cloud Computing Models and Issues

There are three (3) Models or types of Cloud Computing; these are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In all the three types a user can rent the server, rent the Operating System (OS) or even rent the Software \[^{13}\]. Once the Server is rented a user can use any OS and software because the server is owned by the user, this is mentioned to as Infrastructure as a Service. But in a situation whereby the OS is rented, the user can use any software and make use of it as a Platform as a Service. While if the software is rented user can use any software, this is referred to as Software as a Service. Picture below will describe the explanation made above.

Figure 11: Cloud Computing Models/Types

![Cloud Computing Models/Types Diagram]

IAAS  
**Put Any Software**  
**Put Any OS**

PAAS  
**Put Any Software**  
**Rented OS**

SAAS  
**Use Software**  
**Rented Software**  
**OS by the Vendor**
2.3.1 Infrastructure as a Service (IaaS)

This service model offers to company or users computing resources on the basis of pay-per-use, some of the resources are server, networking, data centers space and storage. In this type of service model user has direct contact to Central Processing Unit processing, servers, network, and storage devices. User can install and use operating system, software of their choice on their virtual machines which are accessed through Internet Protocol (IP) address. Cloud provider sustains the basic infrastructure and offers virtualized IP address to the users for direct contact to hardware resources. Examples of IaaS are Amazon EC2, IBM Computing on Demand, GoGrid and Rackspace Cloud. Some of the issues with regards to this model are Compatibility with Legacy Security Weaknesses, Strength of VM Level Solutions, Virtual Machine Sprawl and Data Erase Practice as shown in the Figure below

Figure 12: Issues related to IaaS Model Technology


IaaS physical services and infrastructure hardware form the basis of IaaS, with cloud computing; user can abstract and pool these resources, but at the most elementary level continuously require physical hardware, networks and storage build on. These resources are pooled by means of abstraction and orchestration. Abstraction, frequently through virtualization, delivers the resources after their physical constrain to permit pooling. At that moment a set of essential connectivity and delivery tools (orchestration) links these abstracted resources collectively, generates the pools, and deliver the automation for onward delivery to users. All this is enabled using Application Programming Interfaces (APIs).
APIs are typically original communication technique for components within a cloud, some of which are visible to the cloud user to accomplish their resources and configurations. Most of the cloud APIs these days makes use of REST (Representational State Transfer), which runs above Hyper Text Transfer Protocols (HTTP) building really well appropriate for Internet services \(^{[21]}\).

In most cases, those APIs are equally remotely accessible and wrapped in to a web-based user interface. This arrangement is the cloud management plane, and then users use it to manage and configure cloud resources, like launching Virtual Machines or configuring Virtual networks. From a security viewpoint, it is both the main difference from defending physical infrastructure as well as the highest importance when planning a cloud security program, if an attacker gets into management plane, the attacker may possibly have complete remote access to the entire cloud deployment.

Therefore IaaS comprise of facility, hardware, an abstraction layer, an orchestration or core connectivity and delivery layer to connect together the abstracted resources and APIs to remotely manage resources and provide them to users.

**2.3.2 Platform as a Service (PaaS)**

This type of model offers an environment that is based on cloud having all the requirements of preserving the whole development of building and delivering cloud application. Without considering the budget and difficulty of obtaining, managing the required software as well as the hardware. PaaS service model offers operating system and other tools for software development and let user to use its application on the cloud. User does not need to sustain the cloud infrastructure like storage, servers, operating system, programming tool kit, and network and software license \(^{[48]}\). User only sustains its software or application and its environment configuration deployed on cloud. Examples of PaaS are Microsoft Windows Azure, Google App Engine, Amazon Web Services, and Elastic Beanstalk. Some of the issues with regard to this particular model are Lack of Portability between PaaS Cloud, Event based Processor scheduling and Security engineering for PaaS application asn shown in the Figure Below.

Figure 13: Issues related to PaaS Model Technology
PaaS of all the service models, this is the toughest to absolutely characterize due to both the wide range of PaaS offerings and the several ways of building PaaS services. PaaS complements an extra layer of integration with application development frameworks, middleware capabilities, and purposes like databases, messaging, and queuing. These services permit developers to build applications on the platform with programming languages and tools that are maintained by the stacking. A layer of integration and middleware is made on IaaS, before pooled together, orchestrated, and render to users using APIs as PaaS. For Instance, a Database as a Service might be made by deploying adapted database management system software on applications running in IaaS. The user manages the database through API and accesses it either through the normal database network protocols, or over API.

In PaaS the cloud user understands the platform, not the underlying infrastructure. In recent example given the database increases as required based on utilization, without the user managing individual servers, networking, patches and many others. Second example, is an application development platform. That’s a place where developers can load and use application code without management of the original resources. Services occur for running almost every kind of application in any language on PaaS, allowing the developers from configuring and structuring servers, keeping them updated, or disturbing about complications such as clustering and load balancing. PaaS does not essentially require to be made on top of IaaS; there is no reason it cannot be custom-designed separate architecture. The significant feature is that user’s access and manages the platform, not the original architecture.

2.3.3 Software as a Service (SaaS)

The Software as a Service model of cloud computing is based on SaaS application that functions in the remote computers in the cloud environment which are maintained and functioned by others who joins the network of the users workstation via the Internet Technology generally the web browsers.

Users access the cloud application over internet by making use of interface like web Brower as per requirement and pay for use. It’s the duty of cloud provider to sustain the hardware, operating system and application maintenance [48]. Cloud provider offers the security to user as per service level agreement.

Many Users can access the application at the same time with their respective subscription. Examples of SaaS are SalesForce, Customer Relationship Services, Google Apps, Gmail, and Google Docs. The issue of Saas is the SaaS Application Security.

Figure 14: Issues related to SaaS Model Technology


SaaS services are complete multitenant applications, with all the architectural complications of any large software platform. Various SaaS providers build on top of IaaS and PaaS due to enlarged agility, resilience, and economic advantages. Most modern cloud applications like SaaS uses a combination of IaaS and PaaS, sometimes through diverse providers. Many also have a tendency to provide public APIs for some or general functionalities. They frequently need these to support a diversity of users, particularly web browsers and mobile applications. Therefore all SaaS have a tendency to have application layer and data storage with an API on top. Then, present are one or more presentation layers, frequently including web browser, Public API access and mobile applications.
Figure 15: Issues of Cloud Computing Models

Source: Adopted from google.com

Figure 16: Cloud Computing Technology

Source: Adopted from google.com
Cloud Resources can also be termed as the up-to-date in technology advances that have advance users from running a data center. Where “network” are used to communicate, play games, and do many things, all without regard to what the operating system and CPU. Stored information can be accessed Irrespective of whether using a private or a public terminal.

Abstraction is a critical basis and theory for cloud computing, since it allows for a specific service, an application, a particular communication protocol, processing cycles within a Central Processing Unit (CPU), and storage capability on a hard disk without discerning about a particular hardware that will provide that service.

2.4 Evaluation of Different Models of Cloud Computing and Security Controls

Different models of cloud computing have numerous ways of revealing their fundamental infrastructure to user [49]. This impacts the degree of direct control over the management of computing infrastructure and the dissemination of responsibilities for managing its security. The SaaS Model, most of the duty for security management is responsibility of the Cloud Services Provider (CSPs) by providing a number of ways to control admittance to the Web portal, such as the management of user identities, application level configuration, and the capability to limit access to specific IP address ranges. The PaaS Cloud Models allow user to undertake more responsibilities for handling the configuration and security for the middleware, application runtime environments and database software [19]. The IaaS Cloud Model transfers even supplementary control, and concern for security, from the CSPs to the users. In this model, access is obtainable to the operating system that supports virtual images, networking, as well as storage. Organizations are interested with this Cloud Computing Models (SPI) because of their elasticity and cost-effectiveness, but also much concerned about security. Current Cloud Computing Adoption researches by experts and many articles confirmed these concerns (IBM, 2009) mentioning the lack of reflectiveness and control, disquiets about the protection of delicate information, and storage of regulated information in a shared, externally managed environment.

2.4.1 Cloud Computing Security Controls

Cloud Computing Security Architecture is operational only when right protective mechanism operations are put in place. An effective cloud security ought to identify the issues that will arise with the security Management [1]. The security management controls problems with security
controls. The security controls are put in place to defend any faults in the cloud architecture and decrease or lower the effect of an attack [25]. While there are many types of controls behind a cloud security architecture, which can be structured in the classifications as follows:

- **Deterrent Control:** Cloud computing security issues can be control by the deterrent controls, the controls are anticipated to lower attacks on a Cloud System. Deterrent Control usually lowers the threat levels by notifying possible attacker that there will be adverse consequences for user if continued and is sometimes considered subcategory of preventive control.

- **Preventive Control:** Preventive control in cloud security supports the cloud system against threats occurrences, usually by decreasing prevailing risk and sometimes eradicating vulnerabilities. Robust authentication of cloud users, makes it less likely that unauthorized user can have access to the cloud architecture and possibly the users may certainly be identified.

- **Detective Control:** Detective Control in cloud security control are usually planned to identify and possibly counter applicably to any occurrences that may occur. In the event of an attack in the security of a cloud, a detective control normally indicated to the preventive or corrective mechanism in order to address the security problem. Cloud system and network security monitoring that includes intrusion detection and prevention planning is usually employed to identify any attack on cloud system as well as subsidizing communication infrastructure.

- **Corrective Controls:** Corrective Controls in cloud security decrease the security concerns of an occurrence, most of the times by preventing the damage. Corrective security controls are quite effective during or even after the occurrence. It automatically repairs system backups in order to restore a compromised system.

### 2.5 Cloud Computing Security Mechanism

Cloud Security Mechanism: are some set of fundamental cloud security mechanism that can be used in order to counter the security threats while accessing Data and or Information in the cloud/internet [50] each and every user will have to provide his identity before the CSP will allow or grant access to that particular data stored in cloud. There are lots of security mechanism for
cloud computing users but discussions will be restricted to Four (4) most commonly used, which consist of Encryption, Public Key Infrastructure, Single Sign On and Identity and Access Management [57].

2.5.1 Encryption

Encryption as a cloud security mechanism is a digital coding system that is dedicated in preserving the confidentiality and integrity of data [51]. However, if plain text data is applied, the data is then been paired with string of character called encryption. The following graphical representation clearly shows the concept of Encryption.

![Encryption Diagram](Image)

Source: Adapted from google.com

Therefore, the difference between Encryption and Decryption is that: Encryption is the procedure of changing the Plaintext into Cipher text. While: Decryption is the procedure of changing Cipher text into plaintext. So that, receiver will receive the confidential message [51]. There are two (2) types of Encryption; Symmetric Encryption uses the same key for both encryption and decryption which is sometimes known as Public Key Cryptography. And Asymmetric Encryption uses dissimilar keys that is Private Key and Public Key is also known as Public Key Cryptography.

2.5.2 Public Key Infrastructure (PKI)

Public Key Infrastructure it is also sometimes known as Asymmetric encryption because it uses two keys both Public key and Private keys [57]. However, there are different ways in which messages can be used in PKI or Public Key Cryptography that is sending Data to receiver in a confidential manner. These are Encrypted Messages, Signed Messages and Signed and
Encrypted Messages by making use of the following PKI entities Certificate Authorization (CA), Registration Authorization (RA), Subscriber, Relying Party and Repository.

### 2.5.3 Single Sign-On (SSO)

The SSO cloud security mechanism allows one cloud service user to be authenticated by a Security broker which creates a security context that is persevered while the cloud service user accesses other cloud services of cloud-based Information Technology resources. Then, the cloud service user would need to re-authenticate itself with every subsequent request. The SSO mechanism essentially enables mutually independent cloud services and Information Technology resource to generate and circulate runtime authentication and authorization credential to each cloud user for efficient security [57].

### 2.5.4 Identity and Access Management (IAM)

Identity and Access Management cloud security mechanism comprises element and strategies necessary to regulate and track user identities and access privileges for Information Technology resources, environment and systems [53]. Therefore, IAM cloud security mechanism occurs as a system that includes four (4) main components as follows:

- **Authentication**: User name and password combination are the most collective forms of user authentication managed by IAM systems, which can similarly supports digital signatures, digital certifications, biometric hardware (finger prints), specialized software (voice analysis). The below figure shows how authentication takes place using the client/user exchanging the security keys with the Cloud Provider Interface, where the client is authenticate through the cloud server [53].

Figure 18: Cloud Security Mechanism - Client/User Authentication
- Authorization: The authorized components defined the character granularity for access controls and oversee relationship among Identities, access control rights and IT resource availability [57].

- User Management: In this case it is associated to the administrative capability of the system; the user management program is accountable for creating new user identities and access groups, resetting passwords, managing privileges and defining password policies.

- Credential Management: This system established identity and access control rules for defined user accounts, which mitigate the threat and insufficient authorization. AIM mechanism is mainly used to secure insufficient authorization, overlapping trust boundaries threats and denial of services.

2.6 The ISO- OSI Model: Seven Layers of Abstraction

The most universally used abstraction layers in the computing environment are originated in the Open Systems Interconnection (OSI) seven-layer networking Basic Reference Model [61]. This presentation of abstraction layers means that network equipment manufacturers (NEMs) will no longer have to write an application program for particular equipment. In practice, this means that network card adapter can connect through a standard cable to an Ethernet switch. It also means that corporate communication applications like electronic mail (email) and World Wide Web (WWW) can function without vendor network they are interconnecting. The International Standards Organization (ISO) established the seven-layer model, with each succeeding layer suitable into the next in a well-defined, standardized manner.

Figure 19: The OSI Model
The OSI model offers different functions for devices, services, and protocols which stands in-between each layer, and for precise ways in which the mechanisms in one layer interrelate with mechanisms in other layers. These cautiously planned roles and connections not only make today’s open networking promising, but offer a model for an open and highly planned architecture necessary for cloud computing to be promising. While the networking model is critical, nevertheless, it is not the only category of abstraction model necessary while understand cloud computing.

2.7 Cloud Computing Components

Cloud computing like any other technology is coupled with some components that help in running the functionality of that technology. In order to effectively implement cloud computing, there are selected components that are primarily required in order to achieve certain objective. Without those components Cloud computing would not be implemented and well-coordinated to function. The components are as follows:

Application: The application own its own, is the component that end users spend most of their time making use of, its hosted on severs that are isolated from the user and can be used in actual time from a thin client that hosts the application over a web browser. Most common applications hosted on clouds are run by browsers. This takes main benefits in that because no installation of the application, there is no need for maintenance that are needed and help problems that are rationalized since the software is hosted on a computer that is dedicated to the software thus there is less concern of external effects of the thin client on the software. Cloud applications are similarly termed as software as a service (SaaS).

Client: The client, or thin client, is usually a web browser like Microsoft Internet Explorer or Mozilla Firefox. The new web browser among them is Google’s Chrome, which may rapidly be able to spread dynamic application interfaces thus becoming more of a portal or possibly an operating system on its own, many type of thin clients do exist For instance, in the mobile telephone setting Apple’s iPhone or Google’s Android platforms run a suite of applications that can be reflected to that of a cloud. Furthermore some web sites can be called clients, for instance Facebook, where there are many applications accessible by users in order to explore.
**Infrastructure:** The infrastructure is another component of cloud computing that comprises of computer hardware and the buildings that housed the hardware [26]. Previously, the hardware comprises of cheap, mass produced server technology which has become dominant in the computer industry nowadays. The server environment is running virtualization technology. Relatively, it is of significant to run software that can connect the computers’ with inbuilt multiple processing power which the cloud provider can acquire additional benefits from customers processing ability.

**Platform:** The cloud platform is defined as the way that applications can be positioned, most probable the platform component of cloud computing is originated from Platform as a Service (PaaS) [26]. This consists of the web application frameworks like language Ruby on Rails, which is an open source web application design. Some additional instances of the cloud platform is proprietary PaaS service, Salesforce.com’s, Force.com, the Google App Engine that runs off of Python and the web hosting service called “Mosso”.

**Service:** Service is also defined as what users can obtain from their cloud experience. Nowadays, many services do exist on the Internet for users to take benefit from [26]. Many of which are relatively exceptional, whereas others develop services that are already in existence. One of the most common services in modern days that make use of cloud computing is “mapping services”. Examples comprises of Google Maps, Mapquest and Yahoo Maps. All of these services need large database storage and processing power to execute tasks like as giving users accurate directions.

**Storage:** Storage is a major component of Cloud computing, because physical storage a times is costly for companies who intend to expand their storage requirements [26]. It is inexpensive expanding to cloud. That is why storage is considered as the major features of cloud computing. The main purpose is the hardware in terms of storage devices that are likely to fail on a computer. Therefore, making use of cloud technology make the computer storage redundant in the respect that user can be assured that their data is safer with the cloud technology. Cloud providers generally provide service level agreements in order to make assurance to the customers by making sure the data is safe. This is because there are lots of computers in the cloud environment, the likelihoods of whole disaster of all systems is very minimal. In this way, cloud providers are able to attract customers with motivations of defending their data from destruction.
Example of companies that offers database storage services in the cloud comprises Amazon’s SimpleDB, Google App Engine’s Bigtable data storage service and regular storage services of Amazon’s Simple Storage Service.

**Processing Power:** The processing power that cloud computing is accomplished of is enormous [26]. In fact, 99.9% of users who use cloud computing, the resources accessible will appear to have no limitations. All of this is commonly accessible at very low and affordable cost. Cloud Providers are able to use this kind of capability for some reasons: specifically testing new markets, and trying new applications over the web. The certainty, though, is that many corporate servers are left unexploited during off peak hours. So, they are wasting valued processing resources that are accessible.

### 2.8 Features of Cloud Computing

The features of cloud computing According to [1] as described in the cloud computing definition are on-demand computing, pay as you go, software as a service, utility computing, cost effective that emphasizes on virtualization technology. However, scalability (expand on current hardware), Elasticity (dynamically add hardware as needed by application/user) distributed and highly parallel approach. Therefore, below are the features as discussed by [27].

- **On-demand Self-service:** cloud computing resources can be provisioned on-demand by the users [27], without demanding communications with the cloud service providers. The procedure of provisioning resources is quite automated.
- **Broad Network Access:** cloud computing resources can be accessed over the network using standard access mechanisms that offer platform-independent access over the use of diverse client platforms such as workstations, tablets, smartphones and laptops [27].
- **Resource Pooling:** the Computing and storage resources delivered by cloud service providers are pooled to function by multiple users by making use of multi-tenancy [27]. Multi-tenant aspects of the cloud permit multiple users to be served by the same physical hardware.
- **Rapid Elasticity:** cloud computing resources can be provisioned rapidly and elastically. Cloud resources can be rapidly scaled up or down based on demand.
- Reliability: Applications that are deployed in cloud computing settings commonly have an advanced reliability since the underlying IT infrastructure is skillfully managed by the cloud service.

- Multi-tenancy: the multi-tenanted method of the cloud permits multiple users to make use of the same shared resources \(^{[27]}\).
  
  - In virtual multi-tenancy, computing and storage resources are shared among multiple users.
  
  - In organic multi-tenancy environment every component in the system architecture is shared among multiple tenants.

In order to fully understand the features discuss above, one have to consider the most essential of all the features of cloud computing. Resource pooling is greatest essential feature as discussed previously. CSPs conceptualize resources and assemble them into a pool, portions of which can be distributed to different users (typically based on policies). Users facilitate the resources from the pool by means of on-demand self-service. Users manage their resources themselves, without having to communicate to a human administrator. Broad Network Access means that all resources are accessible over a network, without any requirement for straight physical access, the network is not essentially part of the service. Rapid Elasticity allows users to expand or contract the resources they use from pool (provisioning and de-provisioning) regularly entirely automatically. This allows user to more closely counterpart resource consumption with demand (for instance, adding virtual servers as demand increases, then shutting them down when demand decreases) measured service matters what is provided, to confirm that users only use what they are allocated, and, if required, to charge users for it. This is where the term Utility Computing comes from, since computing resources can now be disbursed like water and electricity, with the user only paying for what is been used.
2.9 Architecture of Cloud Computing

The architecture of cloud computing is imbedded in the hardware and software infrastructures that allow for scaling and virtualization \(^1\). Various data centers set up these capabilities today. Cloud computing architecture as discussed briefly in Chapter One above, discusses the components and subcomponents that are necessary for cloud computing. These components usually comprise of a front end platform which includes fat client, thin client and mobile device as well as back end platforms which include servers and storage, a cloud delivery model, and a network which also includes Internet, Intranet and Intercloud. The cloud architecture layers are shown in the figure below:

Figure 20: Cloud Computing Architecture Layers

![Cloud Computing Architecture Layers](source)

**Source:** Adapted from NIST, 2011.

- **Virtualized Infrastructure:** Virtualization certifies that applications services are not directly reliant on the original hardware infrastructure like storage, servers, or networks. This permits other services passage dynamically in a very effective method, which have basis upon predefined policies.

- **Virtualized Applications:** This component supports the application to decouple itself from the original operating system, storage, hardware, and network to allow elasticity in deployment. Virtualized Application servers can take benefit of grid computing and SOA and certifies scalability to meet the operational requirements.

- **Development tools:** Development tools enable cloud's distributed computing capabilities. These tools not only enable service orchestration but also enable operational
processes to be developed that can control the parallel processing capabilities. The development tools necessitate the maintenance dynamic provisioning.

✓ **Enterprise Management:** Enterprise management delivers the top-down, end-to-end management of the virtualized infrastructure. The enterprise management layer controls the full lifecycle of virtualized resources.

✓ **Security and Identity Management:** Clouds need to make use of a security infrastructure and integrated identity to allow elastic provisioning. As clouds provision resources external to the organization's legal limits, it becomes completely essential to implement an Information Asset Management system to offer the required controls in order to adhere compliance requirements.

### 2.9.1 The Cloud Architectural Components

Cloud Architectural Components establish cloud computing services. Cloud computing necessitates presence and functioning of numerous technologies and service providers who in turns create the innovative technology [1]. Each of the technologies played a vital role in the cloud computing environment. The visible component that user sees are the front-end, this includes the desktop or any other end-user device like mobile phone, I-pad, browser and network. The remaining part of the cloud computing component that are not seen that includes numerous applications, software, computers and data storage devices. Cloud architecture comprises a diversity of systems and technologies, service and deployment models, as well as business models. It is a combination of three sub-architectures that include business architecture, technical and operational architectures. These combinations organized comprehend the cloud architecture.

**The Business Architecture:** this particular architecture strategized the business parts of the cloud services that cover service contract, pricing, and cost prototypes. It similarly involves the business model and its communication to several stake holders.

**The Technical Architecture:** this specifies the strategy of several cloud components. It covers among others which cloud platform to implement, generating a structure of several cloud components displaying relationships, choice of middleware as well as security considerations.
**The Operational Architecture:** this strategies operational possibility, network obtainability, legal issues associated with place of hosting of data, observing of operational performance. The figure below shows several clouds architecture components and their relationship.

Figure 21: Cloud Computing Architecture Component

![Cloud Computing Architecture Component](adapted_from_NIST_2011.png)

**Source:** *Adapted from NIST, 2011.*

Management of cloud comprises events like event management, configuration and compliance, provisioning of resources, workload balancing and service integration [1]. Security of cloud contains types like identity and access management, data encryption, segregation among the users and protection, VM isolation, secure VM migration, virtual network isolation, security intelligence and software, platform, and infrastructure security and security event and access monitoring.

Security guarantees:

- Access authentication and authorization
- Ensuring uninterrupted availability
- Maintaining client confidentiality
- Subscriber identity management
In a cloud computing architecture, the entire applications are controlled, managed, and served by a cloud server. Its data is virtual and well-preserved remotely as part of the cloud configuration. A well-integrated cloud system can produce almost immeasurable efficiencies and possibilities.

### 2.10 Advantages of Cloud Architecture and Technology

Cloud architecture makes use of a simple APIs to offer simply accessible services to the user through the internet technology\(^{[27]}\). It provides scale on demand feature to increase the industrial strength. It offers the transparency between machines so that users don’t have to worry about their data. Users can just perform the functionality without even knowing the complex logics implemented in cloud architecture. It delivers highest optimization and operation in the cloud platform. Cloud computing technology is presently changing the method of doing business in the world; this enables services to be consumed easily on demand and has some unique features such as on-demand self-service, universal network access, location independent resource pooling, rapid resource resistance, usage-based pricing, and transference of risk, \(^{[27]}\). Many researches had been conducted with regards to impact, benefit and advantages of Cloud computing services. These advantages of cloud computing have attracted substantial interests from both the industrial world and the academic research world. The reliable environment is the basic requirement to gain confidence of users to adopt cloud technology. Cloud computing is very favorable for the IT applications. The benefits of the cloud technology may be technical and economical, some of which are discussed in the table below given comparison tabulation before further enumerating into the general benefits.

Table 2: Benefit of Cloud Computing Comparison

<table>
<thead>
<tr>
<th>OWN SERVER</th>
<th>CLOUD SERVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>- INVESTMENT COST</td>
<td>- NO INVESTMENT COST</td>
</tr>
<tr>
<td>- MAINTENACE COST</td>
<td>- NO/LOW MAINTENACE</td>
</tr>
<tr>
<td>- HARDWARE PERFORMANCE</td>
<td>- INCREASE/DECREASE HARDWARE BASED ON USAGE</td>
</tr>
</tbody>
</table>
Source: Adapted from [27] Salim et al, 2017.

There are enormous benefits from exploiting cloud computing, although with any innovative technology there will be integral threats, but companies that plan to run cloud computing resources will have many structures that can benefit and add value to organizations expending cloud technology in order to become an effective organizations. Generally, Cloud computing have lot of benefits, some of which are as follows:

- **Worldwide Access:** Cloud computing increases mobility, as you can access your documents from any device in any part of the world [27]. For businesses, this means that employees can work from home or on business trips, without having to carry around documents. This increases productivity and allows faster exchange of information. Employees can also work on the same document without having to be in the same place.

- **More Storage:** In the past, memory was limited by the particular device in question [27]. If you ran out of memory, you would need a USB drive to back up your current device. Cloud computing provides increased storage, so you won’t have to worry about running out of space on your hard drive.

- **Easy Set-Up:** You can set up a cloud computing service in a matter of minutes. Adjusting your individual settings, such as choosing a password or selecting which devices you want to connect to the network, is similarly simple. After that, you can immediately start using the resources, software, or information in question.

- **Automatic Updates:** The cloud computing provider is responsible for making sure that updates are available – you just have to download them. This saves you time, and furthermore, you don’t need to be an expert to update your device; the cloud computing provider will automatically notify you and provide you with instructions.

- **Reduced Cost:** Cloud computing is often inexpensive; the software is already installed online, so you won’t need to install it yourself. There are numerous cloud computing applications available for free, such as Dropbox, and increasing storage size and memory
is affordable ⁴⁷. If you need to pay for a cloud computing service, it is paid for incrementally on a monthly or yearly basis. By choosing a plan that has no contract, you can terminate your use of the services at any time; therefore, you only pay for the services when you need them.

2.11 Challenges and Security Issues of Cloud Computing

There are numerous challenges and or limitations with cloud computing technology, because it comprises many technologies like networks, databases, operating system, virtualization, resource scheduling, transaction management, concurrent control and memory management ⁵⁴.

Therefore, it’s important for the cloud service provider to ensure that the cloud clients are not facing any serious challenge like data loss and control ⁴⁰, security and privacy which may lead to a great loss of information depending on the sensitivity of the data that is been stored in the cloud. Although, there are still some complications to be solved for personal users and enterprises to store data and deploy applications in the cloud computing. One of the most major obstructions to cloud adoption is its challenges/limitation. Some of the challenges are not limited to:

✓ **Security**: when using a cloud computing service, you are essentially handing over your data to a third party. The fact that, the entity as well as users from all over the world is accessing the same server can result to a security issue. Companies handling confidential information might be particularly concerned about using cloud computing, as data could possibly be harmed by viruses and other malware. Although, some servers like Google Cloud Connect come with customizable spam filtering, email encryption, and SSL enforcement for secure HTTPS access, among other security measures.

✓ **Privacy**: cloud computing comes with the risk that unauthorized users might access your information. To protect data against this happening, cloud computing services offer password protection and operate on secure servers with data encryption technology.

✓ **Loss of Control**: cloud computing entities control the users. This includes not only how much you have to pay to use the service, but also what information you can store, where you can access it from, and many other factors. You depend on the provider for updates.
and backups. If for some reason, their server ceases to operate, you run the risk of losing all your information.

✓ **Internet Reliance:** while Internet access is increasingly widespread, it is not available everywhere yet. If the area that you are located as a user doesn’t have Internet access, you won’t be able to open any of the documents you have stored in the cloud computing environment.

However, [27],[28] highlighted that apart from the general challenges mention above there are tendencies of having more challenges with regards to Cloud Computing Implementation and adoption.

✓ **Policy Integration:** Several cloud providers like Google and Amazon are more accessible to the end users. There should be at least an issue of disagreements concerning their policies as they use their private methods or techniques and policies.

✓ **Trust Management:** The trust management methods must be established and utilized in the cloud environment which should have trust cooperation aspect among the users and the service providers of the cloud.

✓ **Authentication:** The data of the clients that is stored on the cloud is accessible through the internet to the unlicensed clients. Thus, the genuine and licensed users and assistance on cloud must have substitutable administration.

✓ **Service Management:** Many kinds of cloud providers like Amazon and Google are involve in building new innovative services to meet the requirement of their customers. So, that collaboration may result to serious conflict which may affect the data of users stored.

✓ **Access Control:** Cloud need to have the factual policies of access control in order to authenticate and encourage only authenticated customers. These services need to be well adjustable, planned and their distribution required being control conveniently. Service Level Agreement (SLA) method needs to be used among the parties that are involved in the cloud services.
2.12 Issues of Security in the Cloud Computing

Figure 22: The Security Issues in Cloud Computing

Source: Adapted from [28] Akanksha Dubey, 2016.

The security issues in cloud computing, which are further describe and detail explanation given below:

- **Data Locations:** Once users migrate and adopt the cloud services, they possibly will not identify where their data will be hosted and in which physical setting the data stored will be. Users require enquiring from the service providers whether the providers will store the whole data or modify the data for the storage purpose. Similarly on the basis of their users will the cloud service providers make unbiased undertakings to monitor the local privacy requirement?

- **Trust Issue:** Trust is also a topmost issue in cloud computing setting. Trust can be among human to machine or machine to human or human to human. Trust interchanges about confidence and assurance. In cloud computing, users store the data on cloud as there is trust among the parties that are involved in cloud. For instance, users use Yahoo or Gmail servers as users trust on these particular providers.

- **Data Recovery:** The procedure of restoring the data that has been misplaced or corrupted due to a misfortune is called is “data recovery”.

- **Data Security:** It is also known as Confidentiality, Integrity and Availability (CIA). These are the significant issues for the cloud providers. Confidentiality can be well-defined by way of the privacy of the data. Confidentiality is considered to avoid the complex information from attaining accessed by unlicensed users. Integrity is defined as
the accuracy of the data. Availability can be described as the data that is available whenever necessary.

- **Network Security**: Networks are of different types, which comprises of public or private network, shared and non-shared network, small area or large area network and both of these have a number of security issues to deal with. The problems that are related with network level security comprise of the Sniffer attacks, issue of reused IP address, DNS attacks and many others.

### 2.13 Cloud Security Threats and Preventive Measures

There are numerous security threats that prevent users from being attractive to the significance of the cloud computing, [29]. Therefore, an analysis have been made for the purpose of this research work in order to analyzed the security threats that are currently in the cloud and various preventive measures in the implementation process of the cloud, as shown in Table below:

Table 3: Analysis of Issues, Threats and Preventing Measures of Cloud

<table>
<thead>
<tr>
<th>S/No</th>
<th>Security Threats of Cloud</th>
<th>Preventive Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Monitoring and Coordination of Credit Card Fraud.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Self-examining of User’s Network Traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Network blocks through observing public block lists.</td>
</tr>
<tr>
<td>2.</td>
<td>VM-Level Attacks</td>
<td>- Instruction Detection System (IDS).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Intrusion Prevention System (IPS).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Applying Firewalls.</td>
</tr>
<tr>
<td>3.</td>
<td>XML Signature Element Wrapping</td>
<td>- Digital Certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- List of Elements for discarding messages with malicious files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Discarding of Unpredicted messages.</td>
</tr>
<tr>
<td>4.</td>
<td>Loss of Government</td>
<td>- Determined and Cautious effort for implementation of Service Level Agreement (SLA).</td>
</tr>
<tr>
<td>6.</td>
<td>Flooding Attacks</td>
<td>- Screening of malicious request by Intrusion Detection System (IDS), Connecting Firewalls.</td>
</tr>
<tr>
<td>8.</td>
<td>Insecure Interfaces and API’s</td>
<td>- Security Model of Cloud Provider Interface should be Examine.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Robust Authentication and Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Use of Encryption.</td>
</tr>
<tr>
<td>9.</td>
<td>Lock-In</td>
<td>- Use of Standardized Cloud Application Programming Interface (API).</td>
</tr>
<tr>
<td>10.</td>
<td>Data Loss or Leakage</td>
<td>- Prevented by Encryption and Protecting Integrity of Data in Transit.</td>
</tr>
<tr>
<td>11.</td>
<td>Isolation Failure</td>
<td>- Robust Isolation Properties should be engaged.</td>
</tr>
</tbody>
</table>

*Source: Adapted from [29] Mohsin Nazir, M. S. Rashid, 2013.*
As presented in the table above, the threats and preventing measures of cloud as discussed by [29], which is further analyzed and detailed by the researcher in the below:

Table 4: Cloud Computing Threats and Risks in Details

<table>
<thead>
<tr>
<th>S/No</th>
<th>CLOUD SECURITY/PRIVACY ISSUES &amp; THREATS</th>
<th>PREVENTIVE MEASURES</th>
</tr>
</thead>
</table>
| 1.   | Abuse And Nefarious Use of Cloud Computing: This threat comes up because of relatively fragile registration systems that exist in the cloud computing environment. Now, cloud computing registration process, everyone having a usable credit card may register and even make use of the cloud service. This enables anonymity, due to which malicious code authors, criminals and spammers can simply attack the system. | This type of threat can be prevented by following these simple methods:  
- Implementing strict registration and validation processes.  
- Monitoring and Coordination Credit card fraud.  
- Self-examining of user’s network traffic.  
- Network blocks through observing public black lists. |
| 2.   | VM-Level Attacks: The cloud computing is established on Virtual Machine (VM) technology. While implementing of cloud, there is a need for hypervisors like vSphere, VMWare, Xen and Microsoft Virtual PC exist in the implementation process. The VM-Level Attacks threat in cloud come up as a result of the liabilities appearing in the hypervisors because of overlooking some realities by developers throughout the coding process of the hypervisors. | The threats associated with VM-Level Attacks ascending to VM-Level liabilities can be prevented by intensive observing over Instruction Detection System (IDS) also known as Intrusion Prevention System (IPS) and by applying firewall. |
| 3. | **XML Signature Element Wrapping:** XML signature Element Wrapping is the well-known attack for the web service. It is use for defending an element name, attribute and value from criminal party but then incapable to protect the documents. Attacker aims the element by operating the SOAP messages and setting whatever that attacker need. | The security measure for this kind of attack is by making use of the digital certificate. For Instance, X.509 authorized by third party like certificate authorities and also uses the mixture of WS-security with XML signature to a specific element. XML ought to have the list of elements so that it can discard the messages which have malicious file and also discard the unpredicted messages from the user. |
| 4. | **Loss of Governance:** The user provides control to the cloud provider on many issues despite the fact of using the cloud infrastructure. The service Level Agreements (SLA) may not require commitment from the cloud provider, towards providing such services, as a result having a gap in security defenses affecting the security. This loss of control could lead to a deficiency in integrity, availability and confidentiality of data. | There are no openly obtainable standards explicitly define for cloud computing security. As a result companies bearing in mind to migrate cloud services require exercising determined and cautious efforts for the implementation of Service Level Agreements (SLA). |
| 5. | **Browser Security:** As a user sent the request to the server through web browser the web browser need to use of Secure Socket Layer (SSL) to encrypt the authorizations and authenticate the user. SSL provisions point to point communication, meaning “if a third party, intermediary host can decrypt the data”. “If hacker connects sniffing packages on intermediary host”, the attacker might get the Security measure for this attack is cloud provider should use WS-security technology on web browsers since WS-security mechanisms are used in message level that uses XML encryption for endless encryption of Simple |
authorizations of the user and use in these authorizations in the cloud system as a legal user.

Object Access Protocol (SOAP) messages which do not have to be decrypted at mediator hosts.

### 6. Flooding Attacks:

Flooding Attacks: The Flooding Attack. In this kind of attack the Attacker outbreaks the cloud system responsively. The most important characteristics of cloud system is making available of dynamically scalable recourses. Cloud system continually increase its size when there is additional demands from users, cloud system adjust innovative service demand in order to sustain user requirements. Flooding attack is essentially allocating a great volume of non-sense demands to a particular service. As soon as the attacker send a requests, by making additional recourses cloud system will challenge to work against the requests, eventually the system ingest all recourses that are not accomplished to resourcefully service to ordinary requests from user. Then attacker outbreaks into service server.

Security measure for this kind of attack is although is not easy to stop Dos Attacks. From attacking the server, Intrusion detection system will screen the malicious requests, installation of firewall. Sometimes intrusion detection system offers false alerts and could deceive administrator.

### 7. Cloud Malware Injection Attack:

Cloud Malware Injection Attack: The main threat of cloud is the Cloud Malware Injection Attack, which goes by trying to harm a spiteful service, application or virtual machine. An interloper is necessary to create his particular spiteful application, service or virtual machine request and put it into the cloud configuration. Once the spiteful software is move in into the cloud configuration, the attacker attention is focus for the spiteful software as legitimate request. If successful user request for the spiteful service at that moment malicious is executed.

A security measure for this type of attack is authenticity check for received messages. By so doing the system will check the authenticity of all the incoming messages and will prevent further attack.
Attacker then upload virus program in to the cloud configuration. Once cloud configuration care for as an authentic service the virus is executed which damaged the cloud configuration. Therefore, the hardware damages and attacker goal is to course destruction to the user. When user requests for the spiteful program request the cloud send the virus to the user through the internet. The user computer is now infected by virus created.

<table>
<thead>
<tr>
<th>8. Insecure Interfaces and API’s: Cloud users use a set of software Interfaces or APIs to relate with cloud services. The provisioning, management, adaptation and monitoring of the cloud service are commonly done using these interfaces. Whenever the fragile set of interfaces and APIs are used, this may render users to various security threats, like reusable tokens or password, clear-text authentication or transmission of content, anonymous access, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities. To prevent Insecure Interface and API threats, the security model of cloud provider interfaces should be examined. Robust authentication and access controls should be applied. Encryption should be used for transmission of content and, dependency chain related to the API should be evidently understood.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Lock-In: Lock-IN means inability of the user to migrate from one cloud service provider to another cloud service provider. This is because of loss in portability of the user data and programs. Currently, there are limited tools, procedures, methods or standard data formats that offer data, application or service portability. This stops users or companies from adopting cloud computing. Making use of standardized cloud Application Programming Interface (API), this standardization will guarantee cloud computing to be further completely acknowledged.</td>
</tr>
<tr>
<td>10. Data Loss or Leakage: Data loss or leakages have an opposing effect on the business. The status is entirely lost. The threats arising as a result of data loss or leakage can be</td>
</tr>
</tbody>
</table>
and the users’ assurance and trust are battered. This data loss or leakage may be as a result of inadequate authentication, authorization and audit controls, unpredictable use of encryption and software keys, disposal challenges, a data Centre reliability, and disaster recovery.

### 11. Isolation Failure:

The services are delivered in cloud computing through distribution of infrastructure. The element that are used in building Disk partitions, graphics processing units and CPU cache, are not intended to suggest robust isolation properties. The hypervisors, that are elementary building blocks for cloud computing, have shown faults that allow guest operating system to gain illegal control. Because of this isolation failure, the attackers’ emphasis to influence the operations of other cloud users to gain illegal access to data.

Robust Isolation Properties should be engaged so that the individual user does not influence the operations of other users. This can be required by applying paramount practices for installation, configuration, monitoring setting for illegal changes/activities, encouraging robust authentication and access control, fixing the vulnerabilities and directing vulnerability scanning and configuration audits.

---

**Source:** Adapted from [29] Mohsin Nazir, M. S. Rashid, 2013.

### 2.14 Cloud Computing Adoption, Future Prospect and Existing Adoption Model

Cloud Computing permits the usage of information technology on the basis of effective functionalities on-demand by users. This technology (CC) offers lots of advantages to businesses and organization having an inadequate capital, lack of human resources, and also lack access to marketing network. The rapid development of cloud technology indicates certainly non reduction in terms of adoption and frequent utilization from different sectors.
According to 2016 BSA Global Cloud Computing Scorecard, estimates that by 2019 global market will exceed US$130 billion, The Scorecard positions the “IT infrastructure and policy environment — or cloud computing readiness — of 24 countries that account for 80 percent of the world’s IT markets”, that Cloud computing as a current IT invention, has further supplement innovative measurement to that significance by increasing access to technology that pushes for economic growth generally at all levels. Cloud computing democratizes the use of innovative technologies. Cloud computing permits everybody a brighter future, be it an individual user, a government or a small and medium enterprises to access technology that is obtainable only to big organizations in the fast years. These innovative technology services in return have released the entry to unique connectivity, productivity and competitiveness.

Countries proposing a policy in which cloud computing services shows an increase in productivity and economic development. The countries with the most encouraging policies are those with free movement of data, privacy, intellectual property protections, robust deterrence and enforcement of cybercrime is all main concern. Several countries also identify that coordination of national cloud-computing policies with those of other countries will ease benefits for all countries contributing in the global economy. The Scorecard can be examined in several ways, but the strongest measurement depends in the scores. The main improvers were South Africa “moving up six places”, Canada “moving up five places” and Brazil “moving up more than 4 points” but not changing in previous place.

Another forecast is made by Intels which also shows a global expenditure on cloud services will approach US$150 billion in 2020. While today various cloud providers are situated in North America, this evolving technology of computing is achieving reflectiveness all over the world. For example, as part of its Digital Agenda to improve Europeans access to fast internet services and interoperable applications, the European Commission has launched a 170 million Euro public-private partnership to aid in building the internet of the future, with cloud computing as a main element. China is also concentrating on the cloud, its 12th Five-Year Plan, some years back, discourses cloud computing as a part of a creativity to advance intentional industries. Because cloud computing signifies a main transformation in the approach computing services will be retrieved and delivered in the future.
2.14.1 Cloud Computing Future Prospect

Currently we are in the initial generations of cloud computing, with several organizations taking their leading stages. But in many years to come cloud computing is working to be a main and everlasting part of the organizations innovativeness computing infrastructure \[^{30}\]. And definitely, by coming years, a generational change will have followed in organizations in the sense that different generation of Chief Information Officers (CIOs) will be in control, most especial those who developed using cloud-based tools, and adopt cloud on an enterprise. With all these advances in innovative technology cloud computing will appear completely changed in the future. Some of the future expectations of cloud computing includes the following:

- **Software floats away from Hardware**: John Manley discusses that software will become unconnected from hardware, with additional technologies are expended as a service: "Cloud computing is the final means by which computing becomes invisible."

- **Modular Software**: cloud computing in the future will take benefit of the enormous fleets of hardware existing through clouds, specific software applications are set to get bigger and composite as they are developed to take advantage of scale. By the growth in the size and complexity of specific programs, the software development procedure will place an importance on modular software, that is to say, big applications with mechanisms that can be changed without shutting down the program.

- **Social Software**: in the future, software could take on qualities presently found in social-media applications such as Facebook, According to Merrill. Programs could form automatically, if transitory, associations with bits of hardware and software in accordance to their needs.

- **Commodity Hardware Rules**: In future the transition to low-cost hardware will be in complete swipe as schemes like the Open Compute Project (OCP) discover their way out of the data centers of Facebook and Amazon Web Services and into services operated by other, smaller companies as well. "Servers and storage devices will be replaceable" By means of breaking infrastructure down into its elementary components, replacements and upgrades can be done quickly.
✓ **Low-power processors and Cheaper Clouds:** low-power had been in the fast, once ARM chips are available in the market with 64-bit capacity then developer will fast-track, as enterprise software will be developed for the RISC chips, permitting companies to use the power-thrifty processors in their data centers, and thereby cut their electricity bills by an order of magnitude.

✓ **Faster Interconnects:** The associated requirements of enormously distributed applications and an increase in the core count of high-end processors will meet to bring super-fast interconnects into the data center. [37] forecast that communications are expected in the data center to be "running at a speed in the low hundreds of gigabits per second". He anticipates that there will be a "very rapid commodification" of high-end interconnect technologies, leading to a very cheap, very high-performance interconnect. This will let organizations generate more applications that circulate additional data through their hardware possibly permitting developers to build more intelligent, automated and complex programs.

✓ **Data Centers become Ecosystems:** Cloud data centers will “become much like a breathing and living organism with different states” [37]. The associated technologies of distracted software and commodified hardware should associate to make data centers function similar to ecosystems, with over-arching system dominating equipment through software, with hardware controlled from a single point, but increasing and decreasing based on workloads.

✓ **Clouds Consolidate:** The internet recompenses scale, and with the huge capital costs associated with running clouds, it appears possible that there will be a point of consolidation in the cloud provider market. Severe rivalry between big providers could be a good object, as it would quiet motivate both of them to investigate with major technologies.

✓ **The Generational Shift:** According Jack Clack, cloud computing in the future generation of CIOs will have come into companies, and rose in a cloudy as-a-service world. There will be an expectation that things are available "as-a-service" "Our consumption model is changing as a generational issue."
Clouds will stratify: Presently clouds are separated by whether they offer infrastructure-as-a-service, platform-as-a-service or software-as-a-service capabilities, however in the near future more specific clouds will have appeared. Things like 'middle virtualization tools' and 'dynamic BPO services' to appear alongside various big providers offering basic technologies such as storage and compute, there will also be an expansive ecosystem of additional particular cloud providers, permitting companies to shift workloads to the cloud that would then be distributed with particular on-premise applications.

According KPMG survey, organizations are most probable to consider using cloud when experiencing key technology upgrades, or otherwise, when organization are experiencing some procedure of business transformation. The survey shows that the main desirability is to reduce the cost of IT. The agility of cloud allows businesses to grow faster by connecting the diverse parts of the development sequence. Without requirement to advance infrastructures like servers and data centers, organizations can develop faster and take more threats. Setting up a new sector externally, or entering into a new product area is faster and cheaper when the IT backbone already exists on the cloud.

Outburst of information across organization as well as user is no longer a miracle that amazes, but the scale of it preserves success more. For instance, about 120 hours of videos are uploaded to YouTube in each minute every day; more than 200 million emails are exchanged every minute; and a server has to be activated every 10 seconds to support new smartphones. This is important to exceptional challenges for businesses, which requires in managing IT infrastructure to provide to such needs; and at the same time is offering enormous opportunities to organizations that can deploy their infrastructure efficiently to tap into the requirements of users and organizations.

CIOs, which are responsible of motivating organizations to adjust to the changing world, are no longer just directing support roles for the business focused on cost, optimization and reliability. On the other hand the IT department is becoming a significant business driver in itself focused on speed, flexibility and innovation to provide to user requirement.
This developing role has required a transformation in the way IT objectives are well-defined in organizations. While Chief Executive Officers (CEOs) supervise growth, this is prompting CIOs to look at new consumption models for IT and to use new developing technologies. The higher adoption of cloud computing is one of the significant concentration areas for CIOs to facilitate their businesses to be more responsive to market demands. Developments in hardware technologies in relations to higher performing Central Processing Units (CPUs), additional Random Access Memory (RAM) expandability and improved networking possibilities have added to the effective operation of cloud computing for additional workloads. A prediction was made by [23] about the future of cloud computing in many several ways which includes the following:

1. Specialized clouds.
2. Media clouds.
3. Clouds as the fertile ground for the growth of federation.
4. Clouds as a security proxy.
5. Office productivity clouds.
6. Compute clouds in a mixed environment.
7. Mobile clouds and
8. Cloud-aware applications.

Android phones are just the commencement of systems intended particularly to control the back-end cloud. This based on programming tools and how the cloud Providers supports developers.

2.14.2 The Existing Cloud Computing Adoption Model

The existing cloud computing adoption by most visionary organizations and businesses is modeled on Capability Maturity Model (CMM) [43], [44]. The Cloud Computing Adoption Model recommends the following stages:

- **First Stage:** Virtualization as the Cloud adoption engages application virtualization technology for public server infrastructure and continuous portability.

- **Second Stage:** Cloud Experimentation because Virtualization take place internally or externally, as established on Amazon Elastic Compute Cloud (EC2) to compute capacity and as a result of the reference architecture.
✓ **Third Stage:** Cloud Foundations arising because of procedures, policies, Governance, controls, and best practices originate to form everywhere in the deployment and development of cloud applications. These efforts continuously make emphasis on non-mission critical and internal applications.

✓ **Forth Stage:** Cloud Advancement. Government bases permit organizations to measure the capacity of cloud applications over broad-based deployments in the cloud.

✓ **Fifth Stage:** Cloud Actualization as the Applications is disseminated on the basis of proximity to customer, cost and cloud capability.

### 2.15 Cloud Service Providers

Cloud Service Provider(s): The fundamental aspect surrounded in the cloud environment is the CSPs [61], the cloud provider are companies or entities that offers or deliver cloud services to users. Example of cloud services providers are: Amazon, Microsoft, IBM or Google etc. CSPs may deliver several solutions based on the business model, for instance: Software as a service (SaaS) delivers simple to composite software over the Internet, Infrastructure as a service (IaaS) delivers virtual servers, virtual storage and virtual computers, while Platform as a service (PaaS) deliver a combination of both IaaS and SaaS which are all provided as a combined services. A cloud service provider besides the services models, it might also deliver the classification of various deployment models as a public, private, hybrid and community cloud providers. These providers offer and control the computing infrastructure which comprises of the hardware and software to provide the cloud services to users over the Internet.

Figure 23: Cloud Service Providers based on Services offered.
As for **SaaS** function, the cloud service provider takes whole ownership of application as well as the infrastructure then making it accessible to the end-user. In this type of service the cloud provider would install, maintain and upgrade applications and will guarantee uptime, response time and security aspects of the application software. The cloud user has basically certainly not have an administrative control on the controlling of the application.

Whereas, in a situation whereby **PaaS**, the cloud service provider restricts its function in observing the infrastructure platform deployment [34]. It also creates and allows an environment in such a way that the cloud user can develop and install its application. The cloud service provider makes Integrated Development Environments (IDEs), Software Development Kits (SDKs), deployment and controlling tools. Even though the end-user accomplishes the application parameters and controls the equilibrium responsibility of original infrastructure like the Operating System (OS), storage and network are all controlled by the cloud provider.

**IaaS** is considered as the elementary of cloud services, In IaaS the cloud service provider controls the hardware, host Operating System (OS), storage, network and hosting infrastructure. The single service runs by the service providers are a regular of services such as Cloud Computing and beyond, virtual machines and virtual network interfaces. The remaining of the covering layers are runs, accomplished and controlled by the cloud user. The IaaS user takes bigger control on software, application and likewise the OS. The cloud provider’s obligation comprises deployment, grouping, management, security, and privacy of the cloud services.

Apart from these functions that some are controlled by the cloud service providers while others are controlled by the users, there are a lot of functionalities in the cloud service providers as [42]:

- **Service Request Examiner and Controller**: This can be a particular person or even a programmed and computerized system in observing of an professional assigns and reassigns resources based on predefined significance, example resource accessibility and criticality.
- **Pricer**: cloud computing services can be based on pay per use on demand principle; therefore pricer controls price on the demand type and payment strategy this pricer
otherwise a programmed and computerized system in observing of an professional ensures the pricing and accounts for usage.

✓ VM Monitor: Virtual machine (VM) monitor observe the virtual machines and its obtainability. The other key components in the cloud environment are as follows:

- The cloud carrier offers connectivity among the cloud services users and devices like the desktop computers, laptops, mobile phones, Iphone, I-pad and any other device.
- Load dispatcher is a system that receives service demands and assigns virtual machines as required.
- Monitor of Services (MOS) this particular MOS relates the performance levels of services with the approved service levels.
- Cloud auditors are autonomous entities that check cloud service control, confirm adherence to standards and inspect parts like privacy and performance levels. The functions of a cloud auditor are not limited to conducting security check comprising privacy impact and performance assessment. Usage of cloud auditors is required in order to reduce Cloud Computing Architecture differences between the users and the cloud providers and similarly to identify fragile areas.

Generally these are unbiased activities set up by the standards organizations assisted by the relevant authority. Similar to credit evaluation organizations who identify the dependability of the investment proposals and those who identify fire safety standards of buildings, the requirement of cloud auditors is compulsory. The third party organizations can make a timely checks if the data backups are taken, data records are maintained, data privacy or encryption are done or extra controls are applied.

Some of the companies that provide cloud services as discussed previously include Amazon Elastic Compute Cloud (EC2), Microsoft Windows Azure and Google App Engine. These will be further explanation as:
2.15.1 Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) offerings of cloud comprise of a web service which can be extended on demand and computing capability can be made to host diverse software systems \[62\]. As a result it supports the software developer to simply make web-scale computing which will be created, launch, and dismiss server requests as required. As user can pay hourly rate to active servers it is therefore referred to as Elastic Compute.

Scalable non-relational data store that discharges the function of database administration, SimpleDB aids in generating physically distributed data automatically to enable high obtainability and data robustness. The charges of the service are merely for the amount of data that is stored or computing power expended for query, read or write. Access of several user cases are enabled through allocating two (2) addresses (private and public) IP address. For instance, an emergency instance will have a changed public IP address. Amazon EC2 similarly offers Elastic IP addresses in other terms are called static IP addresses for active cloud computing. Amazon EC2 offers other functions like load distribution, load balancing and cloud monitoring tools. Besides it offers API for beginning computing instances with any of the operating systems sustained.

2.15.2 Microsoft Windows Azure

Microsoft windows similarly offer a cloud service in the name of Window Azure \[59\]. This is a development, hosting, management environment and facilitates enterprise-level on-demand computing capability like computing power and storage on-request for a particular amount. For consuming Azure Cloud function user is requested to use Azure API. Windows Azure is hosted in Microsoft data center and offers OS, development tools to develop web based applications which can similarly require interface with local devices. These applications can be established by Visual Studio development environment and the .NET Framework. It also provisions various Internet protocols comprising HTTP, SOAP, REST and plain XML. Its several assisted mechanisms are as follows:

- SQL Azure gives the Microsoft SQL Server abilities for cloud based application to store, accessed Cloud Computing Architecture, structured, semi-structured, and unstructured data.
✓ Windows Azure Marketplace is an operational marketplace for application developers to purchase and trade code, components, training, service templates, and many other functions that are required for emerging Windows Azure applications.

✓ Windows Azure Services aids in association through organizational limitations by preserving security through the domains with ease. It provides verification and access control functions by making use of powerful, secure, standards-based infrastructure.

✓ Windows Azure HPC Scheduler provides components and functions to present and accomplish high performance computing (HPC) applications inside Windows Azure service.

2.15.3 Google App Engine

Google App Engine facilitates development environment for developers to propose, develop and organize Java and Python-based applications in Java, Go and Python environment\(^ {162}\). This ensures dependability, accessibility and scalability at balance with its particular applications. Interface is software programming based. It similarly offers comprehensive programming platform regardless of the size small or large for its users. Some of the useful functions comprise range of templates and appspot, tremendous monitoring and management support for cloud based applications.

2.16 Roles of CSP in Ensuring Security

Cloud Service Providers apart from offering and controlling the computing infrastructure, providing lots of services they also ensure that the physical security, personnel security and privacy of users are well protected\(^ {11}\).

The Physical Security: Cloud Services Providers secure physical Information Technology hardware that consist of the servers, routers, cables and many others against illegal access, interference, theft, fires, flood and many other disasters and also guarantee that important supplies like electricity are appropriately robust to reduce the probability of any disruption\(^ {45}\). This is usually accomplished by serving cloud applications in a standard manner that is professionally recognized, planned, achieved, supervised and sustained data centers.
Personnel Security: many Information Security concerns connected to the Information Technology and other experts related with cloud services are normally controlled through Pre-employment, para-employment and post-employment events like security screening, probable recruits, security responsiveness and training platform proactive.

Privacy: Cloud Service Providers guarantee that most critical data are screened and even encrypted whereby only authorize user have contact to data in its totality. Furthermore, digital identities and identifications need to be secured because any data and information that the CSP saves or produce about user action in the cloud.

2.16.1 Responsibilities of User and Cloud Providers

Both Users and Cloud Service Providers have a very important roles and responsibilities to play while ensuring their data is protected in cloud computing environment [46]. The level of control by cloud service providers is very little when compare to that of user, the providers in most cases are only responsible for availability of their services. However, users’ of cloud computing have the highest responsibility in ensuring the confidentiality, data privacy as well as data integrity. The below picture provides details of the responsibilities by both user and providers.

Figure 24: Security Responsibility in Cloud Service Models by User and Providers
Furthermore, when talking about cloud computing security in general there are two (2) major distinctions in the security components and responsibilities. The security responsibility measures put in place by cloud service providers and that responsibility measures of the client/customer/user. For example the Amazon Web Service (AWS) shared responsibilities with their customers as indicated in the AWS Shared responsibility Model below

Figure 25: AWS shared Responsibility Model,

Source: Adapted from AWS

There are some exceptions in some instances where the CSPs like AWS is responsible for the security configurations which includes antivirus, patching and many others. While from user or customers point of view is responsible for account management and user access. Moreover, EC2, S3 and VPC are completely controlled by customers/users and also responsible for performing all the security configuration and management tasks. This is because the Cloud Service Providers does not have access to user’s personal information and Data. The providers on many occasions provide multiple options in order to secure the user credentials like the password, Multi-Factor Authentication (MFA), Access keys, key pairs and X.509.
2.17 Cloud Security in SPI

According to [31] Security and privacy issues in cloud computing has established widespread considerations in recent times. Most of the researches presently focused on the security with regard to storage and computation. Data management, data privacy as well as security are worries for both cloud user and the cloud service provider. Forgetting the security in the building block of the cloud computing, thus the cloud SPI models ought to have their security challenges.

Figure 26: Cloud Security Architecture

Source: Adapted from [31] Usman Ahmad Usmani et al, 2015.

Cloud Security in addition to the usual challenges of developing secure IT systems, cloud computing presents an added level of risk because essential services are often outsourced to a third party. The externalized aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance [45]. Cloud Computing shifts much of the control over data and operations from the client organization to their cloud providers, much in the same way organizations entrust part of their IT operations to outsourcing companies. Even basic tasks, such as applying patches and configuring firewalls, can become the responsibility of the cloud service provider, not the user.
Inside the cloud, it is difficult to physically locate where data is stored. Security processes that were once visible are now hidden behind layers of abstraction. This lack of visibility can create a number of security and compliance issues. Furthermore, the massive sharing of infrastructure with cloud computing creates a significant difference between cloud security and security in more traditional IT environments. Users spanning different organizations and trust levels often interact with the same set of computing resources. At the same time, workload balancing, changing Service Level Agreements (SLA), and other aspects of today's dynamic IT environments create even more opportunities for mis-configuration, data compromise, and malicious conduct.

2.18 SPI Service Delivery Model

The SPI Model Stands for software, platform, and infrastructure as a service model that incorporates and joins the three general types of cloud computing services; the model is regarded as a building block of cloud computing \[^{[19]}\]. SPI model allows user of cloud computing to run applications and store data online, but they all offers different level of user flexibility and control. The SPI model incorporates three services in a combined manner, either to separate them or combined cloud computing that delivers two or other combined services. The SPI model is becoming suitable as organizations gradually use the Network to find items for operational purposes; it provides significant benefits compare to outsourcing IT infrastructures

SPI service delivery model is a quite an innovative technology in cloud computing and IT world, because it encompasses the services offered which gives a lot of opportunities to its users; though, it also raises certain security problems which might slow down its usage. The popularity of this model is obstructed by its security to some extent. Cloud computing generally has its distinct security threats due to different service delivery model (SPI) \[^{[37]}\].

Security issues in SPI models are classified into two different categories: (a) Security issues related to Cloud Service provider and (b) security issues related to customers \[^{[19]}\]. Securities remain a serious challenge; clients stores the data on the cloud and that information can be shared. Therefore, the responsibility of the provider is to make sure that their infrastructure is well secured and the client’s data is protected as well with different authentication techniques.
Figure 27: SPI Service Delivery Model

Source: Adapted from [31] Usman Ahmad Usmani et al, 2015.

2.18.1 SPI Technology Models

There exist numerous SPI security models of cloud computing which includes the following:-

1. **The Cloud Multiple-Tenancy Model**: Multiple-tenancy is an essential role specifically in cloud computing that allows several applications of cloud service providers that runs in the physical server to provide cloud service for customers \(^9\). The physical server then divides and processes several clients’ demands with virtualization.

2. **The Cloud Risk Accumulation Model**: Cloud Risk Accumulation examines the security threats of cloud computing \(^9\). IaaS is the base level of the cloud services, PaaS is constructed upon IaaS and SaaS is constructed upon PaaS, so there is a relation between the service capability of different layers in cloud computing. However, the security risks of cloud computing is also inherited between different service delivery models.
3. **Jerico Formu’s Cloud Cube Model:** Jerico formu’s cloud cube model is a security model that points out information understood in the service and deployment models of cloud computing and the location. Cloud cube model is considered in describing the physical location of data storage.

4. **The Mapping Model of Cloud, Security and Compliance:** The mapping model of cloud ontology, security control, and compliance provides a good technique to evaluate the gaps between cloud architecture and compliance structure and the consistent security control approaches that should be delivered by cloud service providers, clients or third parties [9].

Security is generally the combination of confidentiality, the avoidance of the unauthorized revelation of information, integrity, the avoidance of the unauthorized alteration or erasure of information, and accessibility, the avoidance of unauthorized concealment of information [32].

The major issues in the SPI in cloud computing comprise resource security, resource management, and resource monitoring. Presently, no guidelines and procedures for deploying applications in the cloud environment, and there is a shortage of regularization control in the cloud. Several innovative methods had been developed and executed in cloud; yet, these methods cannot guarantee full security due to the underlying forces of the cloud environment.

**2.19 Cloud Computing Deployment Models:**

A Cloud can have one of four types of access [19], Public Cloud - allows systems and services to be easily accessible to the general public; Private Cloud - allows systems and services to be accessible within an organization; Community Cloud - allows systems and services to be accessible by a group of organizations; Hybrid Cloud - is a combination of public, private, and community cloud [33].

Figure 28: Cloud Computing Deployment Models
2.19.1 Public Cloud

A public cloud is usually established where several organizations have similar requirements and wishes to share infrastructure [34]. This is the kind of cloud computing deployment model where the service providers make accessible online for public computing resources. It allows users to access numerous types of significant resources on the cloud, be it; Software, Stored data or Applications. One of the most advantages of public cloud deployment is that users have an autonomous power from executing specific tasks on their computers like installation of resources, configurations and data storage. Typical examples of public cloud deployment model are: Microsoft, Google and Amazon. These resulted in having several benefits of public cloud model as presented in the figure below:

Figure 29: Benefit of Public Cloud Deployment Model

Source: Adapted from [34] Sankar Somepalle 2015.

2.19.2 Private Cloud

This type of deployment is an infrastructure that functioned exclusively for only a particular organization, which can be controlled internally or externally by a third party and hosted both internally and externally [34]. The Private cloud deployment model can take the benefit of the cloud’s efficiencies, as well as providing extra control of essential resources and also directing and stoppage of multi-tenancy approach of cloud deployment. Followings are the benefits of the private cloud deployment model that is presented in the figure below.
2.19.3 Community Cloud

The community cloud deployment model infrastructure is established for limited use by an explicit community of users from organizations that have common concerns and agreed to share the network within their respective communities, an example of such are mission, security requirements, policy, and compliance considerations. Community Cloud deployment model could be maintained, controlled, and operated by one or many organizations within the community, a third party, or specific combination, and it could be deployed on or off locations. Community cloud allows for sharing of Capital Expenditure and Operational Expenditure in order to reduce cost \[35\].

Figure 31: Benefits of Community Cloud and other Deployment Models
2.19.4 Hybrid Cloud

A hybrid cloud deployment is a combination of public, private and community cloud, a private cloud basis when combined with the considered combination and use of the public cloud services is identified as hybrid cloud. In essence a private cloud cannot endure in separation from the rest of the organization’s resources and also the public cloud. Many of the organizations devising private clouds develop to manage the capabilities through several data centers, private and public clouds, therefore generating the hybrid clouds. Several benefits have been associated with the hybrid cloud deployment \cite{33} as presented in the figure below:

Figure 32: Benefit of Hybrid Cloud Deployment Model

2.20 The Relationship between the Services and Deployment Models of Cloud

Looking at the Figure below which clearly shows the relationship between the Cloud computing services model and the deployment models, one cannot fully function without the support of other. Because all the models are link together in order to provide a specific function to the user and or organization \cite{33}. 

Source: Adapted from [35] Stephanie Walden, 2015.

Source: Adapted from [33] Sankar Somepalle, 2015.
2.21 Cloud Migration

Cloud migration is the procedure of partly or fully deploying an organization's digital assets, services, IT resources or applications to the cloud. The migrated assets are easily reached at the cloud's firewall. Cloud migration is sometimes referred to as Business Process Outsourcing (BPO), which may possibly involve transferring a total organizational infrastructure, where computing, storage, software and platform services are moved to the cloud for ease of access. Cloud computing is accepted by several organizations because of its scalability, ease of management and little costs expenditure. Cloud migration enables the implementation of flexible cloud computing. An organization's cloud migration procedure sometimes comprises merging an on-site IT infrastructure through a hybrid cloud solution, which may be retrieved through the Internet for a specific charge. Hybrid cloud solutions move among one or many cloud service providers and commonly offer on-demand and provisioned server space, applications and services. Cloud migration is significant for attaining real-time, up-to-date performance and efficiency. As a result, cloud migration needs thoughtful exploration, planning and execution to guarantee the cloud solution's compatibility through organizational requirements.
2.21.1 Cloud Operating System (COS)

A cloud operating system mainly accomplishes the operation of one or more virtual machines in a virtualized environment \[^{[36]}\]. Depending on the virtual environment and cloud services function, the functionality of cloud operating systems differs. For instance, a COS developed to be used in a computing-specific environment will control the procedures and threads of a particular or cluster of virtual machines and servers. On the contrary, a light-end COS may offer end users with pre-installed applications and services, retrieved via Internet browser. Microsoft Windows Azure and Google Chrome OS are among existing instances of COSs.

2.21.2 Cloud Migration Consideration

According to \[^{[36]}\] Cloud migration is not infrastructure revitalization in which old hardware splitting and changing it with new hardware takes place. It's an application setting restructure that will transform not only the technique of how IT administrators relate with systems, but also the way applications relate with one another and are provided to the users.

There are several considerations which are essential while migrating organization’s applications to a cloud environment. The following considerations need to be considered when migrating application to the cloud: Resource usage and availability, Licensing, Existing Access Mechanisms, Security, IT Service Management (ITSM), Integration, Replication and Application architecture.

2.21.3 Cloud Hosting

Cloud hosting is the process of obtaining computing resources from a cloud computing provider or capacity to host data, services and/or solutions \[^{[58]}\]. Cloud hosting is an IaaS cloud service model that offers a collection of remote and virtual services. These are provided by the cloud providers based on-demand and hosted on a cloud computing infrastructure.

Cloud hosting can be defined as mainly the use of virtual hardware, network, storage and composite solutions from a cloud provider. It is facilitated via virtualization, whereby the whole computing ability of an infrastructure or data center is spread and delivered to many users concurrently. The user uses original infrastructure to host applications, services and data. For
instance, a physical server can be virtualized and combined to host a number of cloud servers, entirely sharing the processor, memory, storage, network and other resources.

Cloud hosting offers available elasticity in scaling hosted resources. Also, cloud hosting might also combine the ability of numerous servers in order to offer a particular cloud hosted server. Specific cloud hosted solutions are cloud servers, cloud desktops, cloud storage and the likes.

2.21.4 Cloud Networking

Cloud networking is the locating or operation of one or many network resources and services from the cloud [58]. It involves shifting specific or all network operations on top of a cloud-based network. The network resources are hosted on a public, private, community or hybrid cloud environment. Network resources can be virtual routers, bandwidth, virtual firewall, any network management software and the likes.

There are basically two types of cloud networking:

- Cloud-enabled networking: this type uses cloud resources to control a local network, like by making use of a SaaS network management software or anti-virus solution to control and protect local network.
- Cloud-based networking: this type also uses networking resources completely from the cloud. In order for the processes to be completed completely over the cloud, the network nodes and equipment need to be cloud based.

Cloud networking may possibly comprise the solutions like interconnecting several virtual private servers or connecting a virtual machine with cloud storage.

2.22 Technologies of Cloud Computing

[37] In there paper titled “Security Issues in SPI Models and the Role of Virtualization Technology in Cloud Computing” discusses various technologies of cloud computing as web/server application, database clusters, terminal servers, and virtualization. The basic concept of Cloud Computing is separating the application from the operating system as well as the hardware its self. This processes of separation brought about the underlying technology of cloud computing called Virtualization [17]. However the paper identifies many technologies of cloud
computing some of which are programming model, data management, data storage, virtualization but more emphasis was focused on the Virtualization technology as the major technology involved in the cloud computing.

Virtualization plays a vital role in cloud computing processes. It is a method of installing and organizing computing resources. It separates the different levels of the application system comprising the hardware, software, data, networking, storage etc. It also breakdowns the division between the data center, servers, storage, networking, data and the physical devices, by recognizing dynamic architecture, then attains the goals of organizing centralized and making use of dynamically the physical resources and virtual resources, improving the flexibility of the system, reducing the cost, improving the service and decreasing the risk of management.

As briefly discussed in the previous chapter apart from Virtualization, there are more technologies use in the cloud computing like the Mass Distributed Storage (MDS), Parallel Programming Model (PPM) and Data Management (DM) [9] will also be discussed.

Mass Distributed Storage: is a cloud computing technology used for ensuring high credibility and economy, cloud computing embraces distributed storage to save data, by making use of redundancy storage to guarantee the consistency of stored data and by high dependable software to make up the incredibility of the hardware, therefore providing the cheap and credible mass distributed storage and computing system. The data storage systems of cloud computing are as follows: Google File System (GFS) and Hadoop Distributed File System (HDFS) which is developed by Hadoop team.

Parallel Programming Model: this particular type of technology allow users to resourcefully use cloud computing resources and services that cloud computing brings about; cloud computing programming model need to make task scheduling and parallel execution transparent to users and programmers. Cloud computing adopts MapReduce programming model, which decomposes the task into multiple subtasks, and through two steps (Map and Reduce) to realize scheduling and allocation in the large-scale node.

Data Management: this technology is used in Cloud computing because cloud computing needs to process and analyze mass and distributed data, therefore, data management technology must be able to efficiently manage large data sets. There are two kinds of data management
technology in cloud computing system: BigTable of Google and HBase developed by Hadoop team.

The security of data is the main issue for any cloud services model. The SPI service providers need to guarantee that the data is effectively protected by making use of different real encryption techniques so that the data can be saved confidentially, [27], [37]. Virtualization also helps in separating the data by storing it in different virtual machines so as to retrieve data in case of system failures, also implementing operational data control mechanism supports to keep data safe and secure from unknowns users.

2.23 Don’ts for Security in Cloud Computing Environment

The Don’ts for security in the Cloud Computing Environment which will also help the users in tackling and or maintaining Privacy and Security some of these don’ts are:

- A User/Client is expected not to circulate information about his/her master cloud service accounts.
- Delegating a system administrative functions by user to least-privileges Identity and Access Management groups is not advice.
- User/Client should always make Multi-factor Authentication mandatory for root level access.
- A User/Client should physically secure the Multi Factor Authentication devices in a secure place such as Vaults.
- Users/Clients should not share master accounts information with anyone other than the account holder.
- User/Client should always use Identity and Management roles to provide cross-account access.

2.24 Security and Privacy Issues in General

1. Data related Security Issues:
   - Data Breach: Confidentiality and Integrity
   - Data Lock-in: User may lose data if migrate from one vendor to another
• Data Removal: it is the residual representation of data that have been nominally erased or removed in some ways.

2. Application related Security Issues

• Cloud Malware Injection Attack
• Cookie Prisoning
• Backdoor and Debug option
• Hidden Field Manipulation

3. CSP Level Attacks

• Guest Hopping Attack
• SQL Injection
• Malicious Insider
• Side channel attack

4. Network Level Attacks

• DNS Attacks: Domain Hijacking, Cross-site Scripting
• IP Spoofing: Dos Attack
• Man in the Middle Attack
• Network Sniffing