# Chapter 2: Literature Review

## 2.1 Definition of Cloud Computing

Data which is stored or accessed from the cloud is referred to as a robust and portable tool. When using the Internet, clients can access such provided tools and services to store their data. An example of such a service is *Dropbox*. Instead of saving essential items on their physical hard drives or depending on offline services, a cloud makes data, resources and services accessible and available anywhere. Additionally, photos, music, and any information imaginable can be placed in the cloud - which is a network of servers; where one can store anything from simple websites to more complex web software that is accessible from an online source. [2,10,16,20]

CC (Cloud Computing) refers to the access and usage of information and software on the cloud by devices such as smartphones, tablets and computers, and is also used to describe the business model (Narula et al, 2015). *CC* encompasses the idea that the need for using your physical device is not necessary and can be considered as an *SOA* (Service-Oriented Architecture) that joins nearly every capability of computation involved (Saeed et al, 2019). CC means portability for either the client or the enterprise. This means that clients do not need to go to the store to buy software on a disk and then configure into the device in use. In today’s world, many companies are hosting some of their products online. Also, CC increases the limit and information storage while keeping the scalability and flexibility while the cost is much less (Saeed et al, 2019). [2,10,16,20]

## 2.2 Reasons for using Cloud Computing

CC is very modern technology and provides the individual with various benefits, such as the portability to access data at the most convenient time for the client. The cost of having such technology costs less, and the technology provides scalability of calculation and could be used to support the management of the data (Emeakaroha et al, 2015). CC computing can also be used because of its simplified interface, therefore, CC assists administrators because of this visualization, and because of the portability and scalability, the movement of the data is much more comfortable (Emeakaroha et al, 2015) [4]

In a physical topology, mechanisms such as storage, need to be configured to allow the right permission to every individual. In a cloud environment however, the management to give permissions is much easier to the user to give and have access to their data only, and comfortable monitoring of the data is much easier than on a physical topology environment. Another vital service that the CC offers is when using an application, the knowledge of the location of the application is not needed (Zhang et al, 2015), but when clients make use of a physical topology, the individual needs to know where the application is to launch otherwise, the application would not launch. [1,3,4,19]

## 2.3 Types of Service Providers

Because of the evolvement of the cloud, there are multiple *CSP*s (Cloud Service Providers) that are offering multiple services to attempt to accommodate the client when the Cloud service is in use. Every CSP is trying to compete which other CSPs by offering and implementing tools for the client, in order to be the first choice as a service. Two very famous competitors of CC are the *Microsoft Azure* (MA) and the *Amazon Web Services* (AWS). Competition between the two CSPs stems from the fact that both try to implement and gather many multiple features and tools of the same sort, and always trying to have the best feature from the CSP (Saeed et al, 2019) [10]

Another CSP is the *Google Cloud Platform*, which is popular with clients because the service has an excellent infrastructure that its mother company *Google* designed and also because when the client makes use of the service, the service resembles *Google Search*. Therefore, the client feels a lot more comfortable using the service since there is a similarity to the Google Search tool (Wuyou, 2016). Another different CSP is OpenStack. This CSP is an open source and is generally useful for the scalability the service provider offers and its ability to build infrastructures that can be either as public or private, depending on what the client needs to deploy as an IaaS (Marathu et al, 2016). [8,18]

## 2.4 Categories of Cloud Computing

In CC, there are three types of clouds, which are the Public, Private, and Hybrid. The Public is there to be accessed by everyone, and the client is not sure about the control delivered by the framework of the computing. This type of cloud allows data to be shared between clients and even enterprises. The Private cloud is much safer, and this cloud is ideal for enterprises and even users who do not like to share their data with other clients. The Hybrid cloud is implemented by forming both the public and the private. This cloud is much more popular than others because of the scalability, cost-effectiveness provided, and also due to the fact that the cloud does not make regular changes (Narula et al, 2019) [20]

## 2.5 Kind of Services Provided

In CC, many things can be done to accommodate the client and make the client feel comfortable, just like when using a standard physical topology. Instead of using physical mechanisms and tools though, CSPs provide services such as *IaaS* (Infrastructure as a Service), *PaaS* (Platform as a Service) and *SaaS* (Software as a Service). The IaaS accommodates and equips users with essential features of CC, allowing users to build the wanted network topology with virtualized mechanisms, such as storage servers and virtual servers. SaaS presented to the client, is useful to implement platforms that the CSPs offer. The final service is the SaaS, which ultimately offers access to the software application, and this type of service is introduced to the client by the CSP based on pay-per-use (Narula et al, 2019) [20]

## 2.6 Issues/Risks discovered when using Cloud Computing Services

Anything which involves computing, encompasses some sort of risk. The same understanding applies to CC. CSPs provide excellent service every day in order to be the best CSP. Some clients are very concerned about the migration to the cloud and opt to remain using physical topology. Some of the rationale behind such fear include the question of security, fear of the possibility of data loss or inaccessibility and even the fear that a hacker would enter the system to manipulate, tamper or even delete their valuable data, because of a vulnerability or glitch in the cloud. These reasons though can even appear on the physical topology, however it is possible that perhaps, individuals are not fully aware that such risks can also happen on a physical topology as well. [1,20]

In a survey called “*Risk factors and their associated range values*” - which was published in one of the papers by Ahmed et al, 2015, from all of the risks mentioned below, the most concerning risks that individuals were worried about were *Insufficient Due Diligence* (IDD), *Business Continuity* and *Service Availability* (BC & SA), Recovery of data, Shared environment, and virtual vulnerabilities. Due to these risks, individuals may have less faith in cloud computing, and that is the reason why CSPs are implementing such tools, which to try and convince such individuals that such risks do not have such a negative impact (Ahmed et al, 2015). [1,20]

Figure 1: Risk Factors and their associated range values

## 2.7 Importance of Security

Security is important in every aspect, making everyone feel safe when there is security involved. Security provides assurance to the user that their data is safe and that it is safely locked away, only allowing sole access to the client. Security always mitigates the risk, since attackers constantly try to find any loophole which would give them the access wanted and to use the risk in their advantage. The CC industry is constantly developing and growing, and therefore a lot of energy in security is being invested throughout the applications that the cloud provides, keeping potential attempts by attackers in mind (Wuyou, 2016). [8,18]

## 2.7.1 CIA Triad

Every now and then, the *CIA triad* is mentioned when security comes into the conversation. The CIA triad is useful to protect the client both in a physical topology and in a cloud topology environment. The meaning of the CIA triad is:

* Confidentiality; meaning no authorised access is allowed, [10]
* Integrity; meaning that no other individual beside the owner can temper with the data and, [10]
* Availability; meaning that the data must be available for the wanted users and no one else. [10]

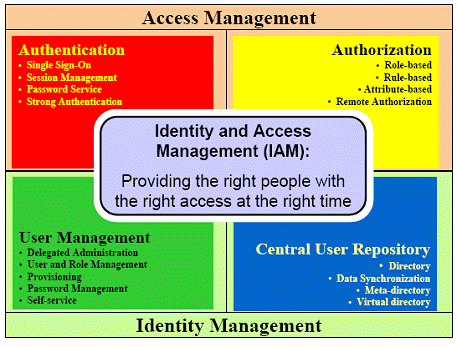
Just as in the example of a physical topology network, the CIA triad works the same way on a cloud environment topology, This is the reason why CSPs are preserving the CIA triad to offer more security. (Saeed et al, 2019) [10]

## 2.8 Solutions for such Risks

For every risk there is a mitigation to decrease the possibility for a risk to happen. For instance, when an individual is working on something important, a backup of that data needs to take place for the user to be assured that the risk of losing data is impossible and that the data is always available. Another situation can be that a physical UPS is installed, so when there is a power cut, the individual would have enough time to save the data before that data is lost. According to (Narula et al, 2015) the CSPs created some mechanisms to try and mitigate the risk for the loss of data to happen. The solutions are an interrupted UPS which can be utilized 24/7 and climate control in the room where the hardware is being kept, in order to maintain a normal temperature. Another solution to make the client feel safe, is to encrypt the data while making use of digital certificates to use the process of authentication (Wuyou, 2016).[18,20]

## 2.8.1 Types of Security Mechanisms

In today's modern world, for a client to feel safe, a mechanism for safety needs to be used. For instance, in an enterprise, every device such as a laptop or computer needs to have a password, so only the owner of that device can have access to the device, because the only person that knows the password is the owner. In the discussion of Encryption mechanisms,  *OTP* (One Time Password) is a mechanism which provides a password and is available for the exact device in that exact moment of the utilization (Swedha et al, 2018). Swedha et al, maintain that this type of authentication is secure because it assures the user that the identity is compliant.  *IAM* (Identity and Access Management) is used to make an identification, authentication, and authorization of either the client or groups or processes, in order to access the resources of AWS (Saeed et al, 2019). [10,13]



IAM Framework

Figure 2: An explanation of the IAM model featuring the levels available when this model is in use.

Another type of security mechanism is the *HTTP* (HyperText Transfer Protocol) authentication, which is considered as the primary type of authentication (Swedha et al, 2018). Information of the client goes through an authentication process to the gateway of the enterprise - a process known as "challenge-response", since the user provides information such as a username and password that must match. *SSL* (Secure Socket Layer) and *TLS* (Transport Layer Security) are used with the certificate of the server's common name, to be sure that the authentication is in use by the right owner (Saeed et al, 2019). Wuyou (2016) argues that the use of the certificate is a general solution, where clients authenticate themselves with such a certificate. This then uses a symmetric key that only the owner only knows, in order to encrypt the data. It once again uses a public key to encrypt the symmetric key, and it is then that the user has access to data and decrypts the data with the symmetric key.[10,13,18]

## 2.8.2 Cloud Computing Services: (Types of Security)

The aforementioned Service Providers try to provide safe services for their clients by taking extra safety measures to safeguard their clients’ most precious data, while trying to be the number one choice for other potential clients. For instance, MA and AWS both offer the service of *SSO* (Single Sign-On). This service can be used to access other needed services. Although this service is excellent, there are some precautions that need to be taken, because if other users see leaked credentials, the service can be in serious jeopardy and in risk of being attacked. Another service is the *Azure AD* (Active Directory), as a typical AD lets the administrator set the policies and permissions of who can access what. Two other services which are provided by the AWS are the *client-side encryption* and the *server-side encryption*, which are in used to protect the data against any unwanted access (Saeed et al, 2019). [10]

Another CSP that can be used for the precise service of the IaaS is OpenStack. This CSP allows clients to build their network topology and provides services like the MA and AWS which can be used by the clients, so that when the client implements the topology, they install the service that is needed. There are multiple services which can be used by the clients; therefore, the client needs to be careful of what service the client needs to install. A service that relates to some of the services mentioned by Saranya et al (2016), is *Keystone*, which is utilized to check if the identity matches the authentication provided. Another service presented by OpenStack is the *Bandit*, which checks if, in the topology, there are any security concerns in the code of OpenStack. (Marathu et al, 2016) Two more services are the *Barbica*n, which secures the storage by certificates and password, and the other is *Karbor*, which protects the data, ensuring that if something happens to the data, this service provides the restore feature. [8]

## 2.9 Scenarios of the mentioned Types of Security

For every tool, the user needs to decide how the service is going to be used. Every service therefore has a purpose and the individual needs to decide which service is going to be used. SSO, for instance, can be used by a user to access his/her data/services. Therefore, the SSO needs to be in use to make sure that the right person is accessing the needed items with a single username and password. The Azure AD can be beneficial for administrators in order to manage the users of the enterprise where for example, administrations permit A to access items A but not permitting B to access such items A. The administrator has absolute control of polices and rules to set to keep everyone and everything under control (Saeed et al, 2019). [10]

Saeed et al (2019) also describes some services offered by the AWS, including the client-side encryption and server-side encryption. These features are needed, therefore when the data is either going to be sent or received, this data is always protected, and therefore no unwanted access reaches the data. For instance, if Group A is going to send data to Group B, the data is encrypted, so members of Group C do not have access to the data, as it goes Group B or is received by Group A. OpenStack, offers a different service because OpenStack is an open-source platform, however it still provides the same features as other CSPs. Keystone can be comparable with SSO because this one needs the credentials of the owner to authenticate the identity. For example, a user needs to enter his username and password to access his data (Saranya et al, 2016). Another different feature mentioned by Marathu et al (2016) which is used to troubleshoot the code, is Bandit. For instance, when there is malicious code, Bandit informs the user about the code. [8,10]

## 2.10 Specifications of the Machines

For every tool, the user needs to consider the purpose of the service which is going to be in use. The same discussion should also include the specification. For instance, what does a gamer need to consider when building a computer? The same scenario stands when implementing one’s cloud environment using IaaS. For instance, Darmanin (2019), utilized a CPU (Central Processor Unit) with the model of Intel Core i7 with 4 GHz quad-core, 16 GB of RAM (Random-Access Memory) and 500 GB SSD for storage to implement and test cloud topologies. [3]

In another paper by Emeakaroha et al (2015), an Intel Xeon 2.4 GHz was used, with 12 GB of RAM and 1 TB of storage to experiment with IoT, while making use of the cloud infrastructures. In another paper, where Real-time QoS is used in the experiment on cloud infrastructure, Zhang et al (2015) used 20 GB of storage, 2.8 GHz of CPU, and a maximum of 60 GB RAM. In this section, it is clear that in every scenario, the specifications differ from each other. [4,19]

### 

Figure 3: Explaining the importance of security in the infrastructure

## 2.11 Plan of Topology to be Utilized

In every topology, whether it is a physical topology or a cloud topology, before choosing the right environment, a plan which illustrates the type of security that is going to be used, should be in place and studied. In Figure 3, the instances are storing the data, followed by the utilization of authentication through Keystone - which identifies the user and locks their data, so that no unwanted access takes place (Saranya et al, 2016). In every situation, the user needs to know all the risks which can take place when making use of the cloud infrastructures. The user also needs to know what kind of measures need to take place, as well as the type of service that is going to be used to protect their precious data, as per Figure 4. Therefore, security should always take place in order to gain the trust of the client, to reassure the client when utilizing cloud services. [12] The only way to see whether security functions well is to first implement the planned topology, and then test it to establish whether the security feature that has been chosen is compatible and functions well within the topology chosen and whether it functions in the same way that the user thought it would.



[Diagram of cloud security](https://data-flair.training/blogs/cloud-security/)

### Figure 4: Levels of how to consider encrypting the data before assigning the encryption