Literature Review.

1.1 Definition of Cloud Computing.

When someone mentions that, the data was stored in the cloud, or the data was accessed from the cloud, that someone is referring to a robust and portable tool. While using the Internet, clients can access some of the provided services, Dropbox, for instance, and store their data there. Instead of saving essential items on their physical hard drives or depending on offline services, the cloud controls, to make resources and services available. Additionally, photos, music, and any information imaginable can be placed in the cloud which is a network of servers; one can also stores everything from simple websites to more complex web software that is accessible from an online source. [2,10,16,20]

CC (Cloud Computing) was referring to the access and usage of information and software on the cloud by devices such as smartphones, tablets, and computers and 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 in means of that clients do not need to go to the store to buy software on a disk that you have to configure into the device in use. In today’s world, 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]

1.2 Reasons of using Cloud Computing.

CC is very modern technology and provides the individual with benefits such as the portability to access the data at the most convenient time of 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 the 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 where mechanisms such as storage need to be configured and give the right permission to every individual. Where in a cloud environment, the management is much easier to give the permissions to the user to access 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]

1.3 Types of Service Providers

Because of the evolvement of the cloud, there are multiple CSPs (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 to be the first choice as a service. To mention two very famous competitors of CC are the Microsoft Azure (MA) and the Amazon Web Services (AWS). Competition between the two CSPs originated when both are trying to implement and gather many multiple features and tools of the same sort and try to always have the best feature from the CSP. (Saeed et al, 2019) [10]

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

1.4 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 won’t be sure about the control delivered by the framework of the computing. This type of cloud makes the data to be shared between clients and even enterprises. The Private is much safer, and the aim of this cloud is for enterprises and even users that do not like to share the data between other clients. The Hybrid cloud is implemented by forming both the public and the private. This cloud is much more famous than others because of the scalability, cost-effectiveness provided, and the cloud does not make changes regularly. (Narula et al, 2019) [20]

1.5 Kind of Services Provided

In CC, many things can be done to accommodate the client and make the client feel comfortable, like when using a standard physical topology. Instead of using physical mechanisms and tools, CSPs provide services such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The IaaS accommodate the users with essential features of CC, which allows the user to build the wanted network topology with virtualized mechanisms such as storage servers and virtual servers. SaaS presented to the client, which is useful to implement platforms that the CSPs offer. The final service is the SaaS, which ultimately offers to access 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]

1.6 Issues/risks found or met when using Cloud Computing Services

Everything that has to do with computing, risk is always a step behind, and the same situation applies to CC. CSPs provides excellent service every day to be on top of the race to be the best CSP. Although some clients are very concerned about the migration to the cloud and decide to stay using the physical topology and the reasons are because of the security queries, the possibility of the loss of data or maybe the data would not be available at all times, maybe someone hack into the system and tries to steal some precious and valuable data because of a vulnerability in the cloud. These reasons can even appear on the physical topology, but maybe individuals are not aware that these kinds of risks can happen even on a physical topology. [1,20]

A survey “Risk factors and their associated range values” that was mentioned in one of the papers by Ahmed et al, 2015, from all the risks mentioned below the most concerning risks that the individuals are worried about are Insufficient due diligence (IDD), Business continuity and service availability (BC & SA), Recovery of data, Shared environment, and virtual vulnerabilities. By these risks, individuals may decrease the amount of trust in cloud computing, that is the reason why CSPs are implementing such tools to try and convince the individuals that such risks do not affect a lot. (Ahmed et al, 2015) [1,20]

Figure 1: Risk Factors and their associated range values (Ahmed et al, 2015)

1.7 Importance of Security

Security is important in everything and makes everyone feels safe when security is involved. Security provides assurance to the user that the data is safe and that is locked away only for the client to access. Security always mitigates the risk but since everyday the attackers try to find a loophole which gives them the loophole wanted and to use the risk in their advantage. The CC industry is getting bigger in size, and energy therefore security throughout the applications that the cloud provides has been in the mind of the attackers. (Wuyou, 2016) [8,18]

1.7.1 CIA Triad

Every now and then the CIA triad has been 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 if the CIA triad is:

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

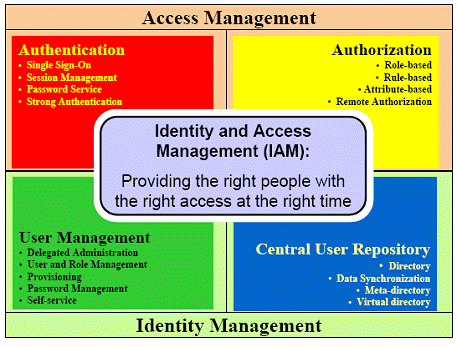
This was an example on a physical topology network, the CIA triad means the same for a cloud environment topology and this the reason why CSPs are preserving the CIA triad to offer more security. (Saeed et al, 2019) [10]

1.8 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 the 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 will be installed so when there is an electricity cut the individual will have time to save the data before the data is lost. According to (Narula et al, 2015) the CSPs made some mechanisms to try and mitigate the risk for the loss of data to happen. The solutions are an interrupted UPS which will be utilized 24/7, climate control to the room where the hardware is to keep the temperature normal. Another solution mentioned by (Wuyou, 2016) to make the client feel safe is to encrypt the data while making use of digital certificates to use the process of authentication. [18,20]

1.8.1 Types of Security mechanisms

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



IAM Framework

Figure 2: 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 by (Swedha et al, 2018) as the primary type of authentication. Information of the client goes through an authentication process to the gateway of the enterprise, this process "challenge-response" since the user provides information such as a username and password that must be a match. SSL (Secure Socket Layer) and TLS (Transport Layer Security) mentioned by (Saeed et al, 2019) used with the certificate of the server's common name to be sure that the authentication is in use by the right owner. Since mentioning the certificate before (Wuyou, 2016) mentioned that using the certificate is general solution which clients authenticate themselves with such certificate than uses a symmetric key that only the owner only knows to encrypt the data then again uses a public key to encrypt the symmetric key then user has access to data and decrypts the data with the symmetric key.[10,13,18]

1.8.2 Cloud Computing Services: (Types of Security)

Service Providers mentioned before tries to provide services to be in use by their clients to take extra safety measures for the most precious data and to be the number one choice for other alternate individuals. For instance, MA and AWS both offer the service of SSO (Single Sign-On). This service can be in use to access other needed services. Although this service is excellent, there are some precautions to be taken because if other users see leaked credentials, the service can be in serious jeopardy to be 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. Another two services which are provided by the AWS are the client-side encryption and the server-side encryption, which are in utilization to protect the data against any unwanted access. (Saeed et al, 2019) [10]

Another CSP that can be in use for the precise service of the IaaS is OpenStack. This CSP allows the clients to build their network topology and provides services like the MA and AWS to be in use by the clients, so when the client is implementing the topology, install the service that is in need. There are multiple services to be in use by the clients; therefore, the client needs to be careful of what service needs to install. A service that relates to some of the services mentioned by (Saranya et al, 2016) is Keystone, 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 Barbican, which secures the storage by certificates and password, and the other is Karbor, which protects the data, and if something happens to the data, the restore feature is provided by this service. [8]

1.9 Scenarios of the mentioned types of security.

For every tool, the user needs to decide on what the service is going to be in use. Every service is there for a purpose; the individual needs to take care of which service is going to use. 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 to manage the users of the enterprise. For instance, permit group A to access items A but not permitting group B to access 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 mentioned some services offered by the AWS, which are the client-side encryption and server-side encryption. These features are in need, so when the data is either going to be sent or received, data always be protected so that no unwanted access goes through the data. For instance, if group a is going to send data to group b, the data is encrypted, so group c does not have access to the data while either going to group b or received by the group a. While switching to OpenStack, the is a different service because OpenStack is an open-source platform but 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) used to troubleshoot the code is Bandit. For instance, there is malicious code, and Bandit informs the user about the code. [8,10]

1.10 Specifications of the Machines.

For every tool, the user needs to consider for what purpose the service 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 goes when implementing your 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 (Read-Only Memory) and 500 GB SSD for storage to implement and test cloud topologies. [3]

In another paper (Emeakaroha et al, 2015) used Intel Xeon 2.4 GHz, with 12 GB of RAM and 1 TB of storage to experiment with IoT while making use of the cloud infrastructures. In another paper, which Real-time QoS is 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, the scenarios are visible that in every scenario, the specifications differ from each other. [4,19]

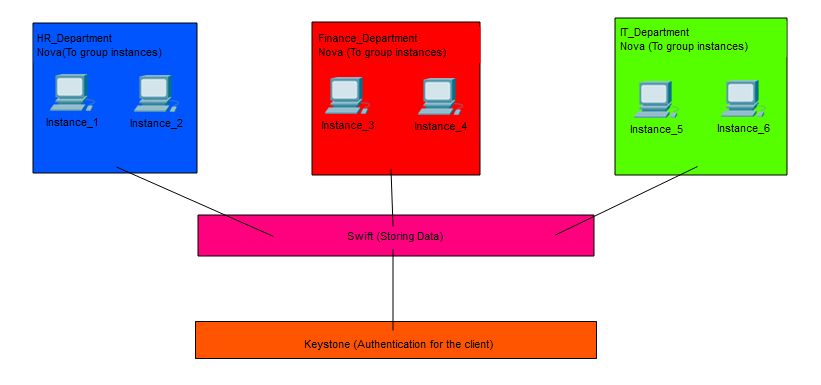
Diagram: Explaining the importance of security in the infrastructure.

Figure 3

1.11 Plan of topology to be utilized.

In every topology, can be either a physical topology or cloud topology, a plan should be presentable for the type of security that is going to be in use before even implementing the environment. In Figure 3, the instances are storing the data, and after the utilization of authentication (Keystone) to identify the user and to lock their data, so no unwanted access takes place. (Saranya et al, 2016) Also in every situation, the user needs to know all the risks that can take place when making use of the cloud infrastructures, what kind of measure is going to take place and after the type of service that is going to be in use to protect their precious data according to Figure 4. Therefore, security should always take place to gather the trust of the client and make the client feel comfortable when utilizing cloud services. [12] The only way to see whether security functions well is first to implement the planned topology and after the test to see whether the security feature is chosen is compatible and functions well within the topology or it does not function the way the user thought.

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

Figure 4: Levels of how to consider to encrypt the data before assigning the encryption.

