California State University, Fresno
Lyles College of Engineering
Electrical and Computer Engineering Department

READING REPORT

Cloud Computing

Instructor: Dr. Nan Wang

Course Title: Ece 174

Date Submitted: 12/07/2020

Prepared By:

Nirmala Sinha

INSTRUCTOR SECTION

Comments: ____

____

____

____

Final Grade: Team Member 1: ____________________

Team Member 2: ____________________

Table of Contents

Table of Figures

I. Objective:

The objective of this project is to understand modern computer architecture and its working. For more learning on computer architecture, the cloud computing topic was selected. This paper will share information on cloud computing, its architecture, issues, benefits, working, advantages and disadvantages, etc. This report will also talk about the cloud computing service provided by Amazon Web Services. Through this paper, the reader will learn about the benefits of AWS for cloud computing, infrastructure, Network Security, docker, etc.

II. Background :

A. Introduction Cloud Computing :

In today's world, technology is considered one of the most incredible things. Every day, people work to implement a new device or an application to make a user's life easier. This paper talks about one of the implementations that made human life much more comfortable.Cloud computing is a technology that allows the user to store its data, applications, and other useful resources, files on the internet. This way, the user can access its data from anywhere around the globe. The term cloud in the technology field allows the user to store information in a virtual space rather than store information on a local disk or memory.

Clouds are also considered a data center or multiple data centers, allowing people to save their data (hardware or software). These centers are connected via a network. In these centers, the data can be modified, organized, and structured by the user. These centers allow the user to access their data from the cloud remotely. The concept of the cloud was first initiated in the 1950s. In the 1950s, cloud computing providers were low budget, and the provider used to have a data center as a building. In the 1960s, John McCarthy introduced the cloud and its usage to the general public. This led to a profitable business model. Later clouds were used to represent more extensive groups of networks such as ATM and VPN in the 1990s [9]. Cloud computing is an old concept which is suitable for storing data on different servers. Around 2006-2007 many multinational companies started providing users cloud storage services at a low cost. The implementation and usage of cloud computing have made many lives more comfortable. Clouds are efficient and cost affected when compared to the traditional data center.

One of the most significant advantages of using cloud computing is it allows the user to use it as a backup [6]. Suppose, by any accident, the user loses any documents, files, or any vital information which he/she has uploaded to the cloud. In that case, the user is still able to recover it from the cloud. There are three different types of cloud available such as public cloud, private cloud, and hybrid cloud, as shown in Figure 1 below.

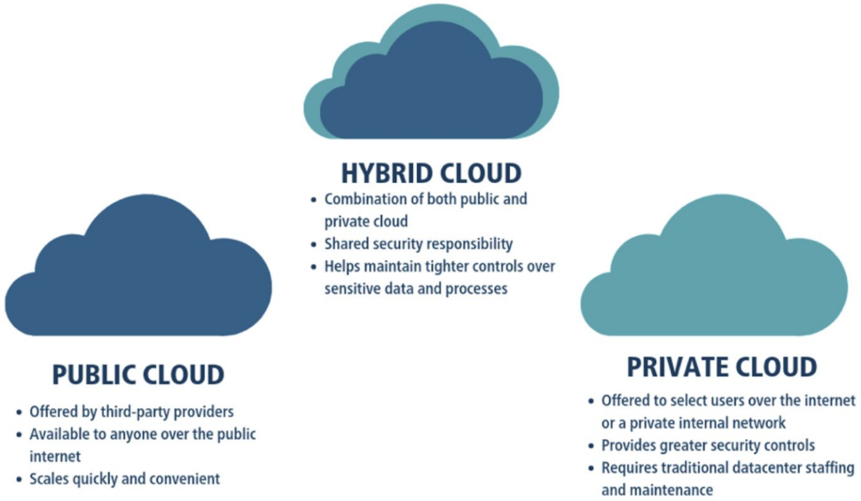
HYBRID CLOUD
• Combination of both public and private cloud
• Shared security responsibility
• Helps maintain tighter controls over sensitive data and processes
PUBLIC CLOUD
• Offered by third-party providers
• Available to anyone over the public internet
• Scales quickly and convenient
PRIVATE CLOUD
• Offered to select users over the internet or a private internal network
• Provides greater security controls
• Requires traditional datacenter staffing and maintenance

Figure 1: Types of cloud deployment

Figure 1 above illustrates the types of cloud deployment. A public cloud service is a service that is provided to the people for free over the internet. These services allow people to store and access resources over the internet. In public cloud service, scalability and sharing are quickly done. People can buy the services they want to utilize in a public cloud. In a public cloud, sharing and synchronization of data are also more comfortable when compared to other services. However, it is considered to be the least secure when compared to other cloud services. The implementation of security needs to be checked from both the side, provider, and user sides.

Whereas a private cloud is most likely to be used by companies, control is given to a user, and that user is allowed to access and customize the cloud according to their needs. Its security system is easier to manage and maintain. As compared to public clouds, the resources and applications are well organized in private clouds [5].

There are also hybrid clouds in which users are provided with both services public and private. When the hybrid cloud is in a private cloud, it can join and access one or more external cloud services at a time [5]. It is considered to be more safe and secure when compared to the other clouds. It also allows the user to access data over any online service or internet.

Advantages	Disadvantages
Cost - pay for only time period	Security
Accessibility	Control
Zero Hardware requirement	Bandwidth issues

Figure 2: Basic Advantages and Disadvantages

Cloud can be used for various reasons. The basic advantages of cloud computing is shown on the left side and disadvantages of cloud computing are shown on the right side in Figure 2 shown above.

There are various advantages of cloud computing, as listed above. Usually, the user has to pay for cloud computing services only for the time period they are using. The prices for cloud computing are not fixed; they all depend on the user budget and service they asked for. Cloud computing allows users to access the data from any geographical location. The last point in the table above means no hardware is required. The cloud itself stores and keeps the backup of the files. At the same time, the disadvantages of cloud computing are security. Security for cloud computing is one of the critical issues; this will be discussed in detail ahead. Another disadvantage of cloud computing is bandwidth issues. Most of the time, users try to put large amounts of data into small servers, which leads to bandwidth issues.

Figure_ helps to understand the usage of clouds in today's world and also explains how they can be a threat to the user.

B. Cloud Computing Architecture

In this section of the paper, the architecture of the clouds will be discussed. A cloud computing system is divided into two sections, as shown in Figure 3below. The first section is called the front end section, and the other team is the back end section. Both units are connected via the internet or through a network [5]. Front end section of the cloud mainly deals with the client's computer and source, which is required to access the cloud [9]. On the other hand, the back end primarily deals with hardware. The rear end creates a shadow for the storage of data.

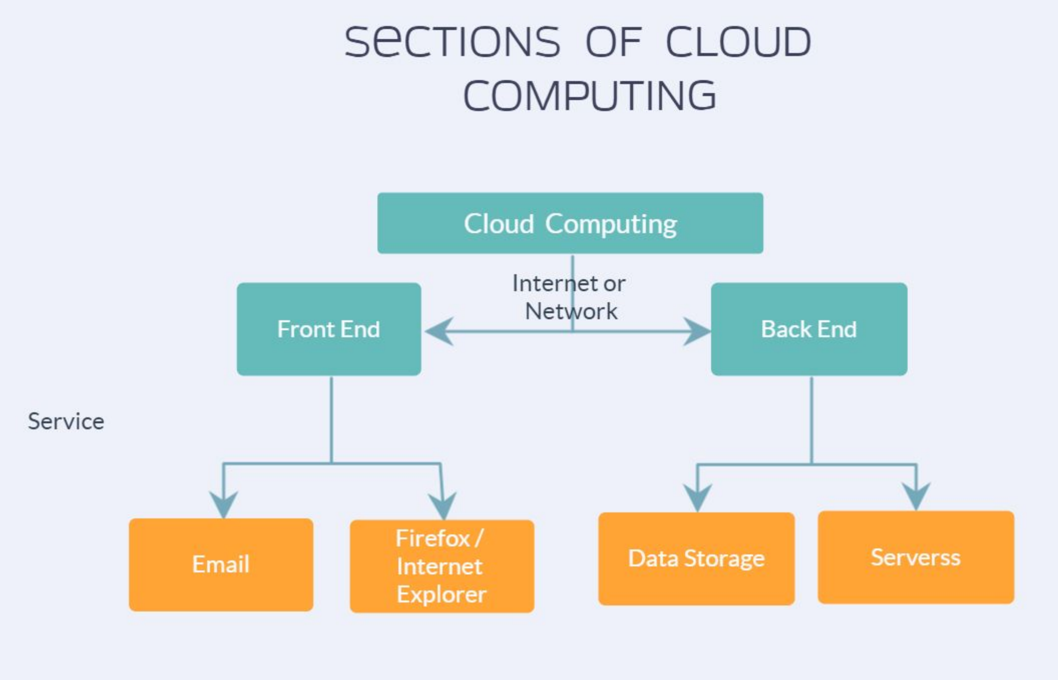

Figure 3 : Sections of Cloud Computing

To ensure that everything runs smoothly, especially when traffic is detected on the site. A server administrator runs a certain kind of software called middleware. This software allows the associated computers to receive and transmit data to each other [5]. A cloud is divided into five layers and three different services, as shown in Figure 3 below. The three services are Infrastructure-as-a-Service, Platform-as-a-Service, and

Software-as-a-Service [4].

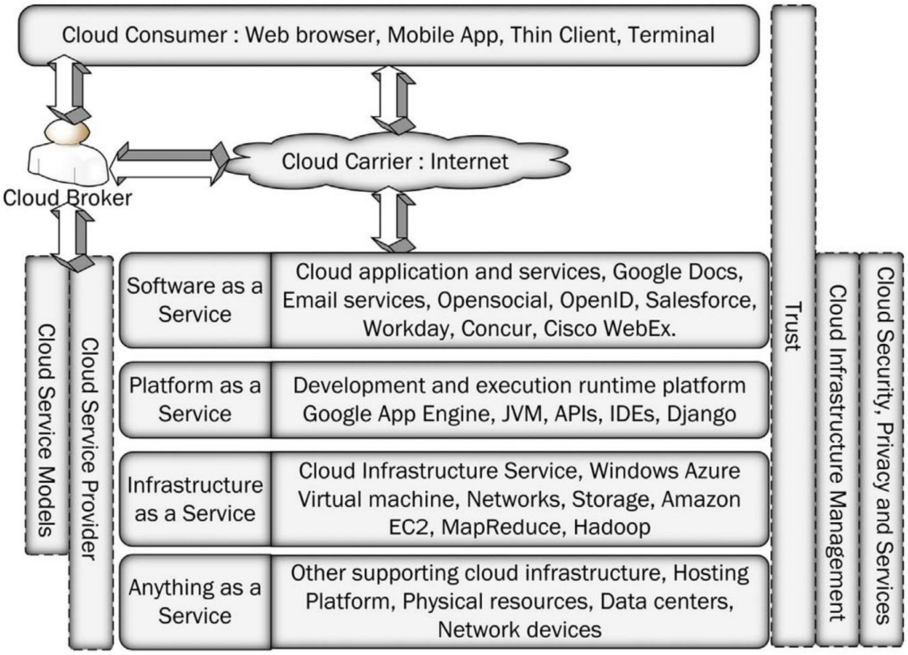
Cloud Consumer : Web browser, Mobile App, Thin Client, Terminal
Cloud Carrier : Internet
Cloud Broker
Cloud Service Models
Cloud Service Provider
Software as a Service
Cloud application and services, Google Docs, Email services, Opensocial, OpenID, Salesforce, Workday, Concur, Cisco WebEx.
Platform as a Service
Development and execution runtime platform Google App Engine, JVM, APIs, IDEs, Django
Infrastructure as a Service
Cloud Infrastructure Service, Windows Azure Virtual machine, Networks, Storage, Amazon EC2, MapReduce, Hadoop
Anything as a Service
Other supporting cloud infrastructure, Hosting Platform, Physical resources, Data centers, Network devices
Trust
Cloud Infrastructure Management
Cloud Security, Privacy and Services

Figure 4: Layers of cloud computing

- Infrastructure-as-a-Service (IaaS):

  This service provides a framework for the cloud. Many resources are shared in this service, such as memory, disk, network, etc. [4]. The hardware resources are accessed using virtual technologies as shown in Figure 4. Iaas ensures that the user does not have to buy any extra disk or memory or doesn't have to manage the cloud's hardware resources. Users need to pay for the period they are accessing the service. Iaas is also known as the Hardware-as-a-Service. Companies like Amazon Web Services host an application that produces different and unique IP addresses. This helps them to block the storage on demand [6]. The user reaches out to the API's to start, use, or stop the virtual repository provided through the Iaas.

- Platform-as-a-Service (PaaS):

  Platform-as-a-Service is a model where the users can rent the hardware via the internet [6]. Because of this service client doesn't experience any problem in installing or purchasing software/ hardware. Thus platform-as-a-service helps the user to take advantage of their fast service delivery. PaaS also allows its users to develop, build, test, run, update, etc. PaaS ensures that the user and authorized team members can share resources using the middle layer..

- Software-as-a-Service (SaaS):

  SaaS is considered to be the highest level of cloud computing services. It is also known as "software on demand" [6]. SaaS provides the user with various programming applications over the web. This eliminates the need for installing, maintaining, and operating applications over their personal computers. The SaaS service providers ensure the maintenance of applications such as upgrade of software, updates, server, network access, etc.

C. Cloud Computing Security :

Security of data is one of the critical issues. With day to day, increasing technology security and privacy has become one of the biggest concerns in the technology industry. Cloud computing brings a significant security issue with it. The user neither has any control when data is uploaded to the cloud, nor the user has any information where it is being stored. Cloud computing provides different services that ensure to protect the client's data as well as their personal data. Though nowadays, there are many services available that help the user to secure their data. In this report, some of them will be discussed, as shown in the Figure 5 below.

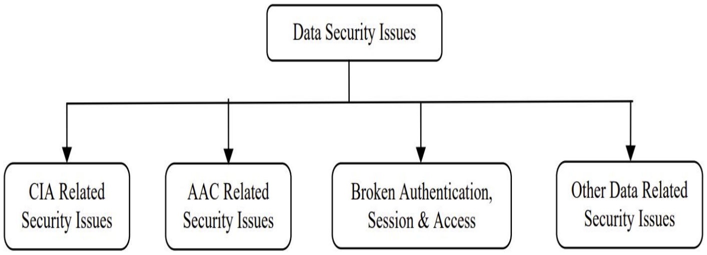
Data Security Issues
CIA Related Security Issues
AAC Related Security Issues
Broken Authentication, Session & Access
Other Data Related Security Issues

Figure 5: Data Security Issues.

a. <u>*Confidentiality Integrity and Availability (CIA)* :</u>

Data is considered to be a core component of business in today’s world. Loss of data not only impacts the client but also affects the company through which the data was lost. The CIA ensures that user's data is protected and is only accessed by the user or authorized team. As a result the cloud provider ensures that maintenance, accuracy, trustworthiness, etc till the data life cycle [7]. Maintaining the CIA in cloud computing is very tough and complicated compared to other systems on computers.

b. *Authentication and Access Control (AAC):*

Authentication and Access Control is a process that verifies and ensures if it is an authenticated authority who is trying to access the data. In many enterprises the credentials are stored in an Active directory or Lightweight Directory Access Protocol [7]. Usually CSP (cloud service provider) includes a high security AAC process that is used to secure the data. Most of the time the password can be cracked by the hacker using different attacks such as phishing attacks or brute force attacks.

c. *Broken Authentication and Access Control:*

Broken Authentication and Access Controls appear because of the incorrect submission of passwords more than a limited number of chances. For example: While logging into amazon account, when the user accidentally enters the wrong password more than three times. It sends an email to the user's linked account notifying the user that someone has been trying to log in their accounts. After such kind of activity, sometimes the service provider also asks the user to opt for a dual authentication system. To ensure security and make their account highly secure.

d. *Information Centric Security (ICS):*

In the Information Centric Security system it highly secures the user's data rather securing their accounts. It encrypts the user's data allowing only the user or authorized people to access the data using the key generated and provided by the system to the user. The ICS preserves the user data and observes if any irrelevant activity is performed with the user's account or data [8].

D. AWS (Amazon Web Service Cloud computing):

In recent years, Amazon is considered as one of the fastest-growing brands [12]. Amazon is counted as the most significant cloud computing provider in the world. People have been very impressed with the excellent and secure cloud computing services provided. In this paper, one of the sections will discuss the network security that amazon offers.

There are many benefits to AWS cloud computing. The IT resources provided by AWS are low cost, and zero investment is required for the help they grant to their users. Moreover, they arrange flexibility in their terms; this allows the user for an easy upgrade in demand for resources.

Amazon Docker is one of the essential concepts to discuss. Docker is a software platform that allows the user to build, analyze, test the application [11].

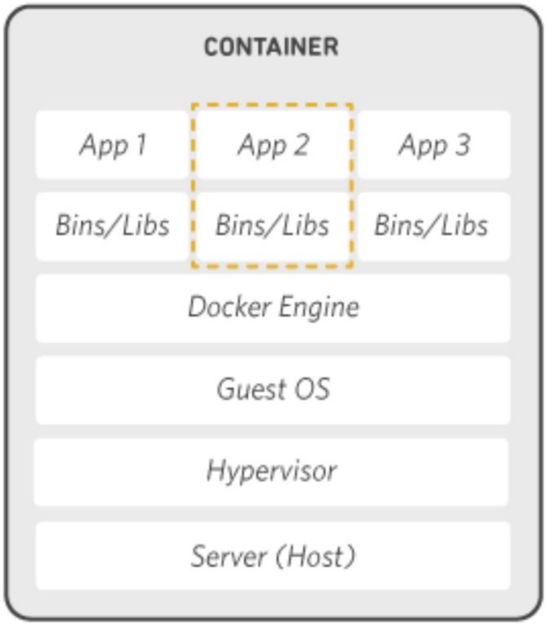

Figure 6: Docker

As shown in Figure 6 above. Docker is considered to be a container that contains the required libraries, tools, documentation, etc. It also shares the same kernel. The docker provided by AWS is affordable and helps the application to deploy quickly. Docker is divided into six levels. The lowest level is the server, and the highest level is considered to be Applications.

Also, AWS makes it easier for the user to deploy applications, data, files, information, etc., on the server quickly. AWS ensures that the data provided by the user is protected by any means. Customer trust and confidence is crucial for Amazon. In the following topic, readers will gain information about the network security Amazon uses.

1. *Secure Network Architecture :*

   Secure Network Architecture is obtained by the system using Firewalls that prevents the attack. These record and administer the communication with external devices and networks. Access Control List is used to manage the flow of information provided by Amazon Information Security[9].

2. *Secure Access Point :*

   Secure Access Point is one of the approaches that show AWS has a limited number of access points [10]. This limited access allows AWS to manage and monitor communication and network traffic well. API endpoints are used by the customer to access. HTTPS is usually used by AWS to create secure communication with better storage systems.

3. *Transmission Protection:*

   In this method, users can use HTTP or HTTPS to connect with AWS using SSL(Secure Socket Layer). It is a cryptographic protocol that ensures that the connection is safe, and it is created to protect the data or information from getting leaked or hacked by an unauthorized person. A user who needs more security is often directed to Amazon Virtual Private Cloud (AVPC). This system uses TP to protect and provide extra layer protection to data.

4. *Amazon Corporation Segregation:*

   Amazon corporation segregation is segregated from AWS as ACS has a complex network setup. This service also ensures that nobody can access the network, even the developer or managers. To access any of these service networks, the person has to go through a bunch of steps. After following all the steps, the AWS ticketing system allows the person to have access to the networked files to work on.

5. *Fault- Tolerant Design:*

   This system ensures that any sort of failure that occurs in hardware or software should not impact much on the user. AWS allows the user to store data geographically, providing the system having any effect from failure in that particular zone[10].

6. *Network Monitoring and Protection :*

   Amazon network monitoring and protection is considered one of the best services provided by Amazon to users. This service controls and monitors the system, which can detect unusual activity or unauthorized access to any user's account. This helps the user to notify of any unusual activity by sending an alert message.

At the end note, AWS provides provisions for data protection, threats, monitoring, access management, etc. Overall compared to other cloud computing services, Amazon is considered one of the best cloud computing service providers.

III. Conclusion

As a conclusion from this report, the reader will gain knowledge on cloud computing, its types, infrastructure and characteristics of cloud computing. This paper also discusses the architecture and security of the cloud. After reading this report a reader will have a better understanding of AWS cloud computing system. This report allows the student the working of cloud computing as well which can be compared to the topics and architecture taught in class.

The main objective of this paper was to encourage students to implement a report on a modern computer architecture model that helps them to understand the concepts, different structures, characteristics of modern architecture.

IV. References :

1. Frankenfield, Jake. “How Cloud Computing Works.” *Investopedia*, Investopedia, 16 Sept. 2020, www.investopedia.com/terms/c/cloud-computing.asp.
2. Griffith, Eric. “What Is Cloud Computing?” *PCMAG*, PCMag, 29 June 2020, www.pcmag.com/news/what-is-cloud-computing.
3. IntelSessions. “Public Cloud vs Private Cloud vs Hybrid Cloud.” *YouTube*, YouTube, 26 Nov. 2014, www.youtube.com/watch?v=3WIJ4axzFlU.
4. Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud computing: security issues and research challenges." *International Journal of Computer Science and Information Technology & Security (IJCSITS)* 1.2 (2011): 136-146.
5. Jadeja, Y., & Modi, K. (2012, March). Cloud computing-concepts, architecture and challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. 877-880). IEEE.
6. Arora, Pankaj, Rubal Chaudhry Wadhawan, and Er Satinder Pal Ahuja. "Cloud computing security issues in infrastructure as a service." *International journal of advanced research in computer science and software engineering* 2.1 (2012).
7. Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana. "Exploring data security issues and solutions in cloud computing." *Procedia Computer Science* 125 (2018): 691-697.
8. Narula, Saakshi, and Arushi Jain. "Cloud computing security: Amazon web service." *2015 Fifth International Conference on Advanced Computing & Communication Technologies*. ieee, 2015.
9. Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." *Journal of Network and Computer Applications* 79 (2017): 88-115.
10. <https://d0.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf> [Accessed 7 December 2020].
11. Mouat, Adrian, and Tamagawa Ryūji. “Docker.” *Amazon*, Orairījapan, 2016, aws.amazon.com/docker/.
12. “Amazon Workers Denounce Working Conditions.” *World Socialist Web Site*, www.wsws.org/en/articles/2017/04/17/amaz-a17.html.