1. Introduction

Cloud computing is a relatively new way of referring to the use of shared computing resources, and it is an alternative to having local servers handle applications. Cloud computing groups together large numbers of servers and other resources and typically offers their combined capacity on an on-demand, pay-per-cycle basis. The end users of a cloud computing network usually have no idea where the servers are physically located—they just spin up their application and start working. Cloud computing is fully enabled by virtualization technology (hypervisors) and virtual appliances. A virtual appliance is an application that is bundled with all the components that it needs to run, along with a streamlined operating system. In a cloud computing environment, a virtual appliance can be instantly provisioned and decommissioned as needed, without complex configuration of the operating environment.

This flexibility is the key advantage to cloud computing, and what distinguishes it from other forms of grid or utility computing and software as a service (SaaS). The ability to launch new instances of an application with minimal labor and expense allows application providers to:

- Scale up and down rapidly
- Recover from a failure
- Bring up development or test instances
- Roll out new versions to the customer base
- Efficiently load test an application

A cloud is a pool of virtualized computer resources.

A cloud can:

- Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications
- Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines
- Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures.
Monitor resource use in real time to enable rebalancing of allocations when needed

A Cloud is a virtual space available to deploy the applications, whereas Cloud Computing is a general term for anything that involves delivering hosted services over the Internet. At its simplest, it is delivering the resources and capabilities of information technology dynamically as a service. Cloud Computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. It generally incorporates Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS).

The main components of security are confidentiality, integrity and availability. Confidentiality is the assurance that information can only be accessed by the intended and authorized recipients. Access control mechanisms can be used to preserve confidentiality. Cryptography can for example be used to make the information unreadable to anyone except the parties who hold the cryptographic key to unscramble the data.

Integrity is the assurance to an entity that data has not been altered (intentionally or unintentionally) during transmission, from origin to destination. Integrity mechanisms can be divided into two classes: prevention and detection mechanisms. Prevention mechanisms seek to maintain integrity by thwarting any unauthorized attempts to modify the data, while the purpose of detection mechanisms is to signal if the data’s integrity is breached.

Availability is the assurance to authorized users that information or resources can be used as desired.Attackers can deliberately deny access to a service by carrying out denial of service (DoS) attacks. Such attacks try to break the usual access patterns to make the system unavailable. Protecting against these attacks is challenging as it is difficult to predict what constitutes expected patterns of use.