Introduction Of Cloud Computing

CHAPTER- 1
1.1-Introduction

Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. Computing is being transformed into a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements, regardless of where the services are hosted. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. Cloud computing is the most recent emerging paradigm promising to turn the vision of “computing utilities” into a reality. Cloud computing is attach no logical advancement that focuses on the way we design computing systems, develop applications, and leverage existing services for building software. When you store your data some information digital or e-data like photos online instead of on your home computer, or use webmail or a social networking site, you are using a “cloud computing” service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a “cloud computing” service. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. In short, cloud computing allows for the sharing and scalable deployment of services, as needed, from almost any location, and for which the customer can be billed based on actual usage. It is based on the concept of dynamic provisioning, which is applied not only to services but also to compute capability, storage, networking, and information technology (IT) infrastructure in general. Resources are made available through the Internet and offered on a pay-per-use basis from cloud computing vendors.

Cloud computing was coined for what happens when applications and services are moved into the internet “cloud.” Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Cloud Computing is an evolutionary platform, has been served as a next generation infrastructure of the industry. It is a model which enables broad network access, resource pooling, and rapid elasticity. With the increasing demand
of security the servers are not secure enough to meet user’s demand. Hence the cloud platform is designed in such a manner so that it meets all the requirements of the user.

As per the definition provided by the National Institute for Standards and Technology (NIST) “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

![Figure 1.1 Cloud Architecture](image)

This chapter provides a brief overview of the cloud computing phenomenon by presenting its vision, discussing its core features, and tracking the technological developments that have made it possible. The chapter also introduces some key cloud computing technologies as well as some insights into development of cloud computing environments.

### 1.2 Characteristics of Cloud

In my Dissertation work this sections include cloud computing characteristics, services models, deployment models, benefits, and challenges.
The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. A simple meaning of Pooled resources a user draw from a pool of computing resources, usually in remote data centers. Services can be made for larger or smaller depending on user requirement and use of a service is measured and customers are billed accordingly.
1.3 Cloud Vender

Many companies are delivering services from the cloud. Some examples are as following:
1.3.1 Google — Has a private cloud that it uses for delivering many different services to its users, including email access, document, applications, text translations, maps, web analytics, and much more. In stark contrast to Amazon’s offerings is Google’s App Engine. On Amazon you get root privileges, but on App Engine, you can’t write a file in your own directory. Google removed the file write feature out of Python as a security measure, and to store data you must use Google’s database. Google offers online documents and spreadsheets, and encourages developers to build features for those and other online software, using its Google App Engine. Google reduced the web applications to a core set of features, and built a good framework for delivering them. Google also offers handy debugging features. Groups and individuals will likely get the most out of App Engine by writing a layer of Python that sits between the user and the database. Look for Google to add more features to add background processing services. It can be found online at code.google.com/app engine.

1.3.2 Microsoft — Microsoft SharePoint online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.

Microsoft’s cloud computing solution is called Windows Azure, an operating system that allows organizations to run Windows applications and store files and data using Microsoft’s datacenters. It’s also offering its Azure Services Platform, which are services that allow developers to establish user identities, manage workflows, synchronize data, and perform other functions as they build software programs on Microsoft’s online computing platform. Key components of Azure Services Platform include

- **Windows Azure** Provides service hosting and management and low-level scalable storage, computation, and networking.

- **Microsoft SQL Services** Provides database services and reporting.

- **Microsoft .NET Services** Provides service-based implementations of .NET Framework concepts such as workflow.

- **Live Services** Used to share, store, and synchronize documents, photos, and files across PCs, phones, PC applications, and web sites.

- **Salesforce.com** — Runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.
1.3.3 Amazon

Amazon was one of the first companies to offer cloud services to the public, and they are very sophisticated. Amazon offers a number of cloud services, including following

**Elastic Compute Cloud (EC2)**- Offers virtual machines and extra CPU cycles for your organization. AWS is mostly known for its compute and storage-on-demand services, namely Elastic Compute Cloud (EC2) and Simple Storage Service (S3). EC2 provides users with customizable virtual hardware that can be used as the base infrastructure for deploying computing systems on the cloud. EC2 instances are deployed either by using the AWS console, which is a comprehensive Web portal for accessing AWS services, or by using the Web services API available for several programming languages. EC2 also provides the capability to save a specific running instance as an image, thus allowing users to create their own templates for deploying systems. These templates are stored into S3 that delivers persistent storage on demand.

**Simple Storage Service (S3)** - Allows you to store items up to 5GB in size in Amazon’s virtual storage service. S3 is organized into buckets; these are containers of objects that are stored in binary form and can be enriched with attributes. Users can store objects of any size, from simple files to entire disk images, and have them accessible from everywhere. Besides EC2 and S3, a wide range of services can be leveraged to build virtual computing system. Including networking support, caching systems, DNS, database (relational and not) support, and others.

**Simple Queue Service (SQS)**- Allows your machines to talk to each other using this message-passing API.

**Simple DB**- A web service for running queries on structured data in real time. This service works in close conjunction with Amazon Simple Storage Service (Amazon S3) and Amazon Elastic Compute Cloud (Amazon EC2), collectively providing the ability to store, process, and query data sets in the cloud. These services can be difficult to use, because they have to be done through the command line. That said, if you are used to working in a command-line environment, you shouldn’t have much trouble using the services.

**Amazon’s virtual machines**- are versions of Linux distributions, so those who are experienced with Linux will be right at home. In fact, applications can be written on your own machine and then uploaded to the cloud. Amazon is the most extensive cloud service to date.
Amazon web services (AWS) AWS offers comprehensive cloud IaaS services ranging from virtual compute, storage, and networking to complete computing stacks.

1.4 Cloud Service Models OR reference model/ cloud delivery models

A fundamental characteristic of cloud computing is the capability to deliver, on demand, a variety of IT services that are quite diverse from each other. This variety creates different perceptions of what cloud computing is among users. Despite this lack of uniformity, it is possible to classify cloud computing services offerings into three major categories:

1.4.1 Infrastructure as a Service (IaaS) –

where the expert user implements their own software to optimize use of the computing facility. At the base of the stack, Infrastructure-as-a-Service solutions deliver infrastructure on demand in the form of virtual hardware, storage, and networking. Virtual hardware is utilized to provide compute on demand in the form of virtual machine instances. These are created at users' request on the providers infrastructure, and users are given tools and interfaces to configure the software stack installed in the virtual machine. The pricing model is usually defined in terms of dollars per hour, where the hourly cost is influenced by the characteristics of the virtual hardware. Virtual storage is delivered in the form of raw disk space or object store. The former complements a virtual hardware offering that requires persistent storage. The latter is a more high-level abstraction for storing entities rather than files. Virtual networking identifies the collection of services that manage the net-working among virtual instances and their connectivity to the Internet or private networks. IaaS solutions are sought by users who want to leverage cloud computing from building dynamically scalable computing systems requiring a specific software stack. IaaS services are therefore used to develop scalable Websites or for back-ground processing. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications. In this cloud service model Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure. It is a service which is provided by the cloud computing network to avail users with the infrastructure required by the user. As for example if a user would require any operating system, it would be provided by the cloud computing platform. In the same manner the user will have to pay for each and every MB of space getting used.

1.4.2 Platform as a Service (PaaS)- where the client customizes their application to run inside the cloud management software. Platform-as-a-Service solutions are the next step in the stack. They deliver
scalable and elastic runtime environments on demand and host the execution of applications. These services are backed by a core middleware platform that is responsible for creating the abstract environment where applications are deployed and executed. It is the responsibility of the service provider to provide scalability and to manage fault tolerance, while users are requested to focus on the logic of the application developed by leveraging the providers APIs and libraries. This approach increases the level of abstraction at which cloud computing is leveraged but also constrains the user in a more controlled environment. PaaS solutions provide scalable programming platforms for developing applications and are more appropriate when new systems have to be developed. Platform as a Service (PaaS) — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. PaaS is used to avail the users with the platform required. Take the example of the .NET platform.

1.4.3 Software as a Service (SaaS) - like Gmail, where the user simply uses the software provided. At the top of the stack, Software-as-a-Service solutions provide applications and services on demand. Most of the common functionalities of desktop applications—such as office automation, document management, photo editing, and customer relationship management (CRM) software—are replicated on the providers infrastructure and made more scalable and accessible through a browser on demand. These applications are shared across multiple users whose interaction is isolated from the other users. The SaaS layer is also the area of social networking Websites, which leverage cloud-based infrastructures to sustain the load generated by their popularity. Each layer provides a different service to users. SaaS solutions target mostly end users who want to benefit from the elastic scalability of the cloud without doing any software development, installation, configuration, and maintenance. This solution is appropriate when there are existing SaaS services that fit users needs (such as email, document management, CRM, etc.) and a minimum level of customization is needed.

In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the
service is hosted as part of the service in the cloud. All the software required by the user like Media Player, Job Schedulers etc. Table 1.1 shows the consumer activities and provider activities.

![Cloud Computing Models](image1)

**Figure 1.5 Cloud Computing Models**

![Cloud Service Model](image2)

**Figure 1.6 Cloud Service Model**

<table>
<thead>
<tr>
<th>Service Model</th>
<th>Consumer Activities</th>
<th>Provider Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS</td>
<td>Uses application/service for business process operations</td>
<td>Installs, manages, maintains and supports the software application on a cloud infrastructure.</td>
</tr>
<tr>
<td>PaaS</td>
<td>Develops, tests, deploys and manages applications hosted in a cloud environment</td>
<td>Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.</td>
</tr>
<tr>
<td>IaaS</td>
<td>Creates installs, manages and monitors services for IT infrastructure operations</td>
<td>Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS customers.</td>
</tr>
</tbody>
</table>

**Table 1.1 Cloud Service Model**

1.5 Cloud Deployment Models
Here I am introduce a brief introduction of cloud deployment model, these all the model are basically provide the facilities to user to use the cloud service in the very lower cost and without need of any other infrastructure. This is show the information or cloud technology that able to shifted this to in cloud environment. With is help of these opportunities the cloud customer are able to optimize the cost, management of infrastructure of his or her company, this all the thing are offered as on demand when the user required this. There are three Cloud models which companies can choose from, which are public Cloud computing, private Cloud computing and hybrid Cloud computing. These cloud deployment model are as follows:

1.5.1 Private Cloud – This service of cloud computing is done in offline manner now here no need of internet facilities in the private cloud model manage and work with third party auditor. Private Cloud Computing. On the other hand, Private Cloud computing reassures the organization that their information and processes are more secure since everything is managed internally. According to the National Institute of Standards and Technology (NIST) a private Cloud is a Cloud infrastructure that is operated solely for an organization. The organization or a third party can manage it. Private Clouds can exist on-site or off-site. Typically private Clouds are used when sensitive data is involved. Figure 2 below gives a basic illustration of an organization using a private Cloud.
1.5.2 Public Cloud – This is a Public cloud now here in this service model public cloud is manage and organize it’s example are Amazon cloud service. The National Institute of Standards and Technology defines a public Cloud as a Cloud infrastructure that is made available to the general public or a large industry group. Public Clouds are owned by the organization(s) selling Cloud services. Figure 1.8 below gives a basic illustration of an organization using a public Cloud., Public Cloud computing means relying on third parties to offer efficient IT services.
1.5.3 **Hybrid Cloud** – This is the combination of two cloud is call Hybrid cloud in hybrid cloud is the information are stored in private cloud environment after the manipulated by a program running in on the public cloud environment. Hybrid Cloud computing is a combination of both private and public services.

1.5.4 **Community Cloud** – The main focus is community Cloud is security and data will be shared in well organized manner its goal to provide a security requirements cloud policy, and compliance report. This is mainly done by the third party auditor.

1.5.5 **G-Cloud** – G-means Government this only based for Government Cloud service this is a kind of Private cloud that will be handle by Government field only. In this cloud environment main task is done by government agencies.

1.6. **Cloud security controls**

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:
1.6.1 Preventive controls Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

1.6.2 Detective controls Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[7] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

1.6.3 Corrective controls Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

1.6.4 Dimensions of cloud security It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts.

1.7 Security Concerns

The Cloud different service models are IAAS , PAAS , SAAS and its deployment service models are Private, Public, Hybrid, and Community these all are face a number of security issues/concerns with cloud computing but these issues fall due to:

security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The main responsibility goes both direction, it may be the cloud provider must ensure that their cloud environment is secure or not and that their user’s all the information and data are secure and ported when the user use it data and cloud application now here cloud client are make a very strong passwords and fulfill the all the authentication measures. When an the cloud manager or agencies selects to cloud application that are already store in cloud data center store data user upload his her information at on the public cloud. It’s output is very potentially sensitive and confidential data is at risk from some attacks. As a recent Cloud Security of the some attack is very major issue in cloud computing. Now the cloud service provider must ensure that all the background detail information. In order to conserve resources, cut costs, and maintain efficiency, Cloud
Service Providers often store more than one customer’s data on the same server. As a result there is a chance that one user’s private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.[2]The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist.

1.7.1 Security Issues In Public Cloud

Cloud infrastructures are just another computer network. This means that Clouds will have the same security any network infrastructure will have (intrusion detection/ prevention etc.). It is up to the Cloud vendor (whether it be you or a third party) to determine the level of security required. The International Organization for Standardization (ISO) provides some codes of practice for information security management, namely the ISO 27001 and 27002. The ISO 27001 covers all types of organizations. The ISO 27002 is also customized to the needs of the organization, but it is intended to help meet requirements identified by a security risk assessment (ISO (2), 2008). There is an ongoing debate between IT professionals of whether or not private Clouds are really more secure. According to some analysts and vendors, there’s been no shortage of debate and consternation about the security threats public Cloud computing poses. The concern can be understandable; especially if sensitive data and vital applications are in the hands of a party not directly under your preview. Besides from the common view that private Clouds should be more secure, there are Public Cloud Computing vs. Private Cloud Computing: How Security Matters 8 some interesting attributes/properties of public Clouds to consider. The NIST definition of public Clouds states that they are made available to the general public or a large industry group. Therefore, public Cloud providers are much larger targets for hackers than private Clouds. Public Clouds also attract the best security people available; the biggest and best Cloud service providers have millions of customers relying on them. They definitely would be meticulous about who they hire. Also public Cloud providers, especially larger companies like Google, Amazon, and Face book would get the latest security gear much easier than a small to midsize private company. Here are some other security issues related to Public Cloud Computing:
- Assessment of the CSP

Any small, young business can advertise Cloud-based services to the world. How are you sure that that company is capable and safe to work with? CSPs should hold industry certifications such as the SAS 70 Type II, which is an audit that provides independent 3rd party verification that a service organization’s policies and procedures are correctly designed (SAS 70, 2012).

- Security of the communication channels

Data and communication protection is paramount in Cloud computing. We use the services provided even though the security mechanisms for secure communication is abstract. Services can be accessed several ways, such as through a thin client, laptop or mobile phone. The fact that your data is easily accessible through these channels, data is transferred across multiple networks, more especially if your CSP is extremely far away from your location. All communication should be protected using encryption and key management.

- Transparency of security processes

- Some Cloud Service Providers may not explain their security processes for their own security reasons.


Your data and many others’ in danger. A perfect example is Sony’s data breaches in 2011. Sony faced customer relation fallouts, and lawsuits over its failure (Schwartz, M, 2011).

- Access control mechanisms
- Data Loss

Cross-tenant data leakage - vulnerabilities of shared network infrastructure components, such as vulnerabilities in a DNS server, Dynamic Host Configuration Protocol, and IP protocol vulnerabilities, might enable network-based cross-tenant attacks in an IaaS infrastructure (Pfleeger, Irvine, Kwon, 2012).

1.7.2 Security Issues In Private Cloud

Private Clouds have the same security concerns as public Clouds do, but typically on a smaller scale since private Clouds are operated solely for an organization. However, there are some specific concerns towards this Cloud model:

- Security Architecture
Public Cloud Computing vs. Private Cloud Computing:

- Perimeter Security and insider attacks - Very often, traditional perimeter security is not configured to protect resources from attacks that come from within the organization (Microsoft (2), 2012).

- Hypervisor vulnerabilities and network level authentication (IPSec, IPS/IDS) - Virtual machines are heavily used in Private Clouds. It is possible that those virtual machines will be able to have virtual communication with other virtual machines. Virtual machines should only be communicating with the ones they need to. Encryption and authentication mechanisms should be implemented using IPSec and/or IPS/IDS (Microsoft (2), 2012).

- Security Zones - Resources of different types and sensitivity levels should be located in separate security zones (Stawowski, M., 2007).

Based on previous studies and the definition of a private Cloud, private Clouds will immediately seem to be more secure than public Clouds because of how the infrastructure is designed. It gives the organization more control over their policies and security. According to NIST, the internal private Cloud is more suitable deployment models that offer an organization greater oversight and authority over security and privacy, and better limit the types of tenants that share platform resources, reducing exposure in the event of a failure or configuration error in a control. Private Clouds typically would suffer from perimeter complacency; thinking that because it is on the internal network, it must be secure; the Internet and viruses are still present. So, caution and security standards should not be lowered just because it is private (Bloomberg, 2012). Moreover, the private Cloud requires that to have total control over all layers of the stack, which includes any traditional network perimeter security you might want to have in place. In a private Cloud model, the Cloud services are not typically exposed to the general Internet users and remote access to private Cloud hosted resources is enabled through mechanisms used in traditional data centers. Private Cloud computing typically uses virtualization technologies to increase hardware utilization and to abstract compute, memory, network, and storage component from Private Cloud consumers (Thomas, 2011). See Table 1 below for a concise comparison of public Clouds and private Clouds.

**Security Issues Comparison**
<table>
<thead>
<tr>
<th>Public Cloud</th>
<th>Private Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low investment hurdle</td>
<td>High investment hurdle</td>
</tr>
<tr>
<td>Negative loss and control over data</td>
<td>IT organization retains control over data</td>
</tr>
<tr>
<td>Higher risk of multi-tenancy data transfer</td>
<td>Fewer security concerns</td>
</tr>
</tbody>
</table>

**Table1.2 - Security Issues Comparison**

### 1.8 Cloud Storage

Cloud storage means "the storage of data online in the cloud," wherein a company's data is stored in accessible from multiple distributed and connected resources that comprise a cloud. Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection or data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. However, cloud storage does have the potential for security and compliance concerns.

#### 1.8.1 Types of Cloud Storage

There are four main types of cloud storage:

1. **1.8.1.1 Personal Cloud Storage**
   Also known as mobile cloud storage, personal cloud storage is a subset of public cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere. It also provides data syncing and sharing capabilities across multiple devices. apple's i Cloud is an example of personal cloud storage.

2. **1.8.1.2 Public Cloud Storage**
   Public cloud storage is where the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data center. The cloud storage provider fully manages the enterprise's public cloud storage.

3. **1.8.1.3 Private Cloud Storage**
   A form of cloud storage where the enterprise and cloud storage provider are integrated in the enterprise's data center. In private cloud storage, the storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider.
provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

1.8.1.4 Hybrid Cloud Storage
Hybrid cloud storage is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.