APPENDIX 1

CLOUD COMPUTING PHYSIOGNOMIES

A 1.1 CLOUD COMPUTING BENEFITS

A 1.1.1 Cost Savings

The biggest reason for shifting to cloud computing is cost. Any company or enterprise has to face sizable costs for configuring, installing, upgrading and maintaining the IT infrastructure. Cloud computing replaces capital and ongoing costs with a fixed monthly fee, typically around one fifth of the current amount.

A 1.1.2 Remote Working

One of the biggest IT challenges that companies and enterprises have been facing is how to deliver applications and data remotely. Cloud computing does it permanently and securely.

A 1.1.3 Efficiency

Organizations that adopt cloud computing work more efficiently because the task of maintaining and servicing an complicated IT infrastructure is removed, leaving them to concentrate on their core business and at the same time getting better response times and less down time.
A 1.1.4 Flexibility

No company or business can predict the future. Cloud computing brings flexibility to applications which can be turned on and off as required, making their cost a direct reflection of their value to the business. Also, infrastructure and servers can be scaled up or down as and when required based on business needs.

A 1.1.5 Future Proofing

If businesses can increasingly shift their IT resources to the cloud, many cloud-based app stores can crowd source their future apps development, thereby reducing their need for large internal IT functions or expensive research tech shops to predict and produce their future IT services and apps.

A 1.1.6 Morale Boosting

Internal IT functions don’t exactly enjoy the IT maintenance, helpdesk, support, and operation functions. And the users are never really satisfied with the service. Outsourcing all these to cloud-based service providers could prove a morale booster.
A 1.1.7 Resilience without Redundancy

Buying a new server in case of failure and keeping an unused server idle is a cost-issue and also time consuming. Cloud computing service can deal with this redundancy requirement.

A 1.2 CLOUD CHARACTERISTICS

A 1.2.1 On-demand Self-services

Consumer can unilaterally provision the capabilities like server, storage etc., as needed automatically, requiring no human interaction. The on demand self-service has enabled the customers to use the services whenever required without the interaction of customer and provider. Amazon Web Services (AWS), Google, Salesforce.com, Microsoft, IBM are some of the cloud service providers who provide “on demand self-services”. For example, if additional computing power is needed for an application to support heavy load, then the process normally has to follow few standard steps in an organization. Initially, a hardware vendor will be called and new machines are ordered. After receiving the prescribed hardware device(s), installation of operating system, network connections, firewall/proxy rules configuration, etc. are done. Later, installation of the application is performed and machines are added to the pool. This can be viewed as simple and routine process; but it requires lot of interactions between both internal and external teams. This burden of time and manual dependency had been promptly addressed through on demand self-service by cloud computing.
A 1.2.2  Broad Network Access

In general, cloud services are available on the Internet and their access is supported through a standard mechanism. Internet has been in use already for more than two decades and cloud has provided advances in the usage of Internet from heterogeneous clients like desktops, laptops, mobile phones and tablets, etc.

A 1.2.3  Resource Pooling

Resource pooling allows providing both virtual and physical services by service providers through multi-tenant model. The customers have no knowledge about the location of the resources provided. The examples of such resources are email services, memory, network bandwidth, storage, processing, virtual machines, etc. Resource pooling enables the cloud providers to achieve high resource utilization and application density. As a result, resource price falls. Resource pooling can be shifted easily. At times the customer can request resources from the pool and return it back to the pool after utilizing so that somebody else can use it.

A 1.2.4  Rapid Elasticity

Cloud computing has ability of resource scalability or providing computing power as needed by the customers. Based on demand, one’s resources can scale outward and inward. Capabilities are provisioned and released elastically. Provisioning capabilities appear unlimited to the customer. Elasticity is related to resource pooling and easy to expand and contract the application resources. The elasticity leads to save money
since it is automated for contraction and expansion. In traditional case the elasticity is achieved as follows: When the load increases, power up more machines and add to the server pool; when the load decreases remove servers from the pool and power off. It is more expensive to add and remove the servers from the pool. When the load is heavy it results in errors and the requests are dropped. But in cloud, resource adding and removing is easier because they are all virtualized and completely dynamic in nature.

A 1.2.5 Measured Service

In cloud, services are provisioned to users as ‘measured service’ by the cloud service provider; and based on the consumption individual customers are charged. This helps in improved capacity planning, resource optimization, access control and reduced billing. Cloud systems control the resources and they are optimized to the service type. Resource usage can be controlled, monitored and transparent to consumer of the utilized service. The resource usages are monitored and measured by the cloud service providers through which they can bill their customers. Measured service is considered to be important because it can assist in preparing the budget of each current application for future growth. It can also help in preparing budget for the upcoming projects with similar applications. Developers and application architects use it for lower utilization of the resource. Cloud service providers optimize resources of datacenter and have higher density for all hardware by using this service. But in the traditional approach it does not showcase the capacity utilization, network capacity and the storage.
A 1.2.6 Dynamic Computing Infrastructure

Dynamic computing infrastructure is required by cloud computing. The dynamic infrastructure consists of foundations like scalable, secure physical infrastructure and standardized. To ensure availability there should be redundancy levels. For running services, server virtualization is leveraged by virtualized environments. Through software automation these services are provisioned and de-provisioned. The workloads of these service are moved when the demands for capacity varies. At last the infrastructure is utilized whether provided by internal or external. When maintaining the security and reliability it looks critical for dynamic computing infrastructure to support the service provisioning and de-provisioning. But with the basement of integrated technological mix, cloud computing is balancing dynamic computing infrastructure to the greater extend as compared to early contestants.

A 1.2.7 IT Service-centric Approach

Cloud computing performs IT service-centric approach. This is in contrast with system-centric models. The users of the cloud would prefer to access the instance of application quickly. The users can access the computing environments which are designed around the service by removing the server-centric view. The user adoption and business agility is enabled by IT Service Centric approach.
A 1.2.8 Minimally or Self-managed Platform

A self-managed technology platform should be used by the provider to provide a cloud efficiently for its constituents. Self-management is enabled by best-of-breed clouds through software automation, leveraging the capabilities as shown below:

- To deploy the services and to tear them down for reuse a provisioning engine is used.
- Reserving and scheduling mechanisms for resource capacity.
- Managing, configuring, reporting capabilities to ensure resources are allocated or reallocated to multiple users.

These capabilities enable agility but also enacting critical administrative control.

A 1.2.9 Consumption-based Billing

Based on consumption of the resources the customers are charged in cloud computing. The mechanisms that capture information for billing are provided by the cloud computing platforms. This helps the customer to keep their costs down. These characteristics are necessary to produce private cloud which reduces support costs, operating costs, increase business agility.
A 1.2.10 Multi-tenancy

Multi-tenancy enables cost and resource sharing which increases the capacity of load, utilization and efficiency for systems. Multi-tenancy refers to the need for service levels, governance, segmentation, isolation, policy-driven enforcement for constituencies of the consumer. The consumers from the same organization utilize the service offered by the provider.

A 1.2.11 Managed Metering

Uses metering for managing and optimization of service and provide billing and reporting. During the billing period consumer services are billed for which they have used. It allows cloud computing for service deployment and sharing of services. Bill is provided to customer for the services which they have actually used.

A 1.3 CLOUD SERVICE MODEL

A 1.3.1 Infrastructure as a Service

The consumer has the ability to provision network, processing, storage, and other fundamental computing resources. In IaaS, the consumer can deploy and run arbitrary software which includes applications and operating systems. The consumer has control over storage, deployed applications, and operating systems but not the underlying cloud infrastructure.
IaaS reduces money and time required to install new hardware systems i.e. equipment is outsourced to support operations. This is a provision model in which service provider is responsible for the storage, running and maintenance of the equipment. A company can run its databases, operating systems, applications and other software on top of the selected infrastructure, and they have no direct access to those machines. The cloud infrastructure is managed by the cloud service provider and also the process of scaling up or down is done by the provider if needed.

IaaS is similar in concept to a traditional dedicated hosting service, with two major differences: Organizations pay for only what’s used on a utility basis and they tap into a highly scalable pool of resources. In other words, organizations can increase their productivity while eliminating underutilization costs.
Challenges

Out of the box IaaS only provides basic security (load balancing, perimeter firewall, etc.). Applications moving into the cloud need higher levels of security provided at the host. Security responsibilities of both the service provider and the consumer vary based on different CSP’s. Amazon’s Elastic Compute Cloud (EC2) includes vendor responsibility for security up to the hypervisor which means that they can only address security controls such as physical security, virtualization security and environmental security. IaaS solution provided by Amazon also has some limitations. One major problem with Amazon Web Services is its low level of abstraction.

A 1.3.2 Platform as a Service

In cloud infrastructure, the customer has the capability to deploy consumer- acquired applications created using tools and programming languages that are supported by the provider. The consumer does not control the underlying cloud infrastructure including network, operating systems, storage or servers but has control over the applications deployed onto the cloud and possibly application hosting environment configurations.
Fig. A 1.2. PaaS Service Offerings.

PaaS provides computational resources through the platform such as Operating System. PaaS is built upon the principles of Infrastructure as a Service by providing an environment where applications can be built and deployed in a secure, rapid and high quality manner. The business needs Information Technology to rapidly develop, deploy, and maintain new applications to remain competitive and PaaS helps organizations in the same. PaaS eliminates the capacity concerns and hardware dependency. It also provides a simplified deployment model.
Challenges

In PaaS model the developers have been given control by the providers to build applications on top of the platform, whereas any security below the application level such as network and host intrusion prevention will be in the provider’s scope. The provider needs to verify that the data remains inaccessible between applications. PaaS model offers developers a service that provides a complete software development lifecycle management. Everything else is abstracted away from the eyes of the developers. The disadvantage of PaaS is that this abstraction can be helpful for a hacker to leverage the PaaS cloud infrastructure for a malware command.

A 1.3.3 Software as a Service

In SaaS, consumer has the capability to use applications provided by the cloud provider (CSP). Through various client devices, these applications can be accessed by using a thin client interface (e.g. web based e-mail). The consumer does not control the underlying cloud infrastructure including servers, network, operating systems, storage, or even individual application capabilities. Customer relationship management (CRM), IT service management, intrusion prevention, Spam filtering, e-mail, human resources management and calendaring are some of the common applications delivered as cloud software services.
Challenges

One of the main issues with SaaS applications is integration. SaaS applications provide services for business areas like enterprise resource planning (ERP). As a result, companies have to face serious problems with forecasting automated business processes and accurate data where functionality sharing and real-time data is needed. Some SaaS providers have developed application programming interfaces (APIs) to overcome integration challenges. Due to API modifications and updates, accessing and managing data via an API requires coding and maintenance. Another challenge with SaaS applications is data locality. In SaaS, consumers use the applications to process their business data. The problem is that the
customer will not be aware of where the data is getting stored. Due to data privacy laws and compliance in various countries, locality of data becomes very important in part of the enterprise architecture.

### A 1.4 CLOUD DEPLOYMENT MODELS

Based on the implementation of cloud computing, the entire cloud can be divided into four. They are Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud [4].

![Deployment Model – Outline](image)

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Infrastructure Managed By</th>
<th>Infrastructure Owned By</th>
<th>Infrastructure Located</th>
<th>Accessible and Consumed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
<td>Off-Premise</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Private/Community</td>
<td>Organization</td>
<td>Organization</td>
<td>Off-Premise</td>
<td>Trusted</td>
</tr>
<tr>
<td></td>
<td>Third Party Provider</td>
<td>Third Party Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hybrid</td>
<td>Both Organization &amp; Third Party Provider</td>
<td>Both Organization &amp; Third Party Provider</td>
<td>Both On-Premise &amp; Off-Premise</td>
<td>Trusted &amp; Untrusted</td>
</tr>
</tbody>
</table>

1. Management includes governance, operations, security, compliance, etc.
2. Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment
3. Infrastructure Location is both physical and relative to an Organization’s management umbrella and speaks to ownership versus control
4. Trusted consumers of service are those who are considered part of an organization’s legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Fig. A 1.4. Deployment Model – Outline.

### A 1.4.1 Public Cloud or External Cloud

This model of cloud implementation is known as true cloud hosting. In this hosting, the entire services, infrastructure and resources are provided
to various clients all over the world by a third-party provider. These resources are located at an offsite location. Through web application or web services the users can access and use the cloud resources. Some resources can be accessed only as per the pay-per-user license policy. Mostly the services are provided by a vendor free of charge. Generally this kind of deployment is used in the business grounds. The reason is that the user should have mechanism to manage load spikes, to host service based applications, to use the entire infrastructure efficiency for deployment and testing and also to manage the concurrent access of these applications from all over the world. The public cloud allows users to access the resources from anywhere they need in a cheaper price. For these reasons, the public cloud is considered as the best. The one and best advantage of this deployment model is that it is highly economical.

A 1.4.2 Private or Internal Cloud

In private cloud deployment the hosting is built and managed only for a specific client. The hosting infrastructure can be at a third-party location or on-premises. In the security point of view private cloud has got tremendous value but not much in terms of economy. Here actually the consumer will be able to build and manage their own infrastructure. Here the resources are stored and accessed by a limited number of users in the vendors own datacenter which is monitored by a firewall. The private cloud has all the advantages of the public cloud. But only one limitation is that it is hosted inside a firewall. In security aspects, it provides a great advantage because it allows both the internal and external consumers to use the resources in a secure and well defined local environment. Due to this high value of security, this model is adopted by a number of organizations. Several SaaS applications provide options to their clients
to maintain their resources on their own premises to assure data privacy is managed and maintained according to the requirements of the particular business.

A 1.4.3 Hybrid Cloud

This hybrid cloud deployment model combines the advantages of both private and public cloud such as secured applications and data hosting of private cloud and cost benefits and resource sharing of public cloud. The main advantage of hybrid cloud is that it supports cloud bursting. Cloud bursting refers a process where, when the existing cloud set up is not able to handle the network load it provides a fall back option to support the network load. There by the hybrid cloud migrate the workloads between the public and private hosting. This process will not provide any inconvenience to the users.

A 1.4.4 Community Cloud

Here as the name implies, the cloud infrastructure is shared by a number of organizations who are following same policy and compliance considerations. Since it is shared by a large group it reduces the costs compared to private cloud. If a number of organizations want to access similar kind of data, then they can deploy such resources in community cloud, such that once permission has been granted to each organizations, they can access the updated data at anytime from anywhere. Example: Various state-level government departments requiring access to the same data relating to the local population or information related to
infrastructure, such as hospitals, roads, electrical stations, etc., can utilize a community cloud to manage applications and data.

A 1.5  Types of Virtualization

A 1.5.1 Server (Hardware) Virtualization

Server virtualization represents the technology of flexible construction of virtual servers with no hardware limitations and thus reduces the total cost of ownership, hence making it easier to use virtual servers in the changing business environment. Server virtualization offers the consolidation of many servers into one physical server. It provides Multi-tenancy i.e. one server can perform the job of multiple servers, as single server can be shared among multiple environments. The advantages of server virtualization are cost, less physical server requirement, and 70 to 80 percent utilization of existing. There are three ways for creating virtual servers. They are,

- **Full Virtualization**
  It is a type of server virtualization done by means of hypervisor. Here the direct interaction of CPU of physical server and disk space happens. This provides platform for the virtual servers and OS. The important aspect of this kind of virtualization is that the hypervisor will provide complete independence of each virtual server to other running on the same physical machine.

- **Para-virtualization**
  It is a light weighed type of virtualization. Here, virtualized servers can know each other. Each virtual server is dependent on other virtual server. The hypervisor is to manage guest
operating system that does not require resources of large computing, because every operating system get information about the requirement of other OS on same physical server they are hosted.

- **OS Virtualization**

  It is another way of virtualization, which is recognized as more effective and efficient. It performs virtualization at the operating system level. It does not need the use of a hypervisor. In the absence of hypervisor, the virtualization capabilities are monitored by the hosting operating system that carries out all the operations of the hypervisor in its virtualized form. One and important drawback of the process is that here all the guest servers must run on same operating system that is deployed. It may cause some performance issues. In this kind of virtualization the concept of homogeneous environment arises. Each server in its virtualized form remains independent of all other virtual servers. The reason is that the entire guest OS should be of the same kind, called homogeneous environment.

### A 1.5.2 Client (Desktop) Virtualization

Client virtualization is implemented with a workstation desktop or laptop which is generally specified as client. It will be a tough task for a system administrator to manage. The client virtualization can be of the following:
• **Remote (Server-Hosted) Desktop Virtualization**
  This type of virtualization is implemented by hosting a working environment on a server in the data center thereby giving access to the end users across the network based on their needs.

• **Local Desktop Virtualization**
  The local desktop virtualization model is configured in such a way that the operating environment runs locally above physical hardware and provides support for multiple client-side virtualization aspects. These activities can be monitored and given a thread of execution in the end user system.

• **Storage Virtualization**
  Storage virtualization is handled by system administrator who performs the separation between logical storage (virtualized partitions of stored data) and physical storage. Location independence is achieved by storage virtualization by separating the physical location of the data. Three categories of data storage are:
  o **Direct-Attached Storage (DAS):** Direct-Attached Storage is one of the traditional methods. In this method physical server is being attached with hard drives.
  o **Network-Attached Storage (NAS):** In Network-Attached Storage the administrator has a key machine that provides data storage to other machines and it is kept on the network. This method provides a single source of data, which is helpful for supporting data backup.
  o **Storage Area Network (SAN):** Storage Area Network helps to transfer data on its high performance network by deploying specialized software and hardware.
A 1.5.3 Data Virtualization

Data Virtualization provides instant access to data. It integrates diverse data without any costly copies or added data management complexity. The advantages of data virtualization are,

1. Instant access to whole data
2. Multiple times faster when compared to traditional data integration
3. Quick start and successful scaling with easy-to-adopt overlay to existing infrastructure
4. Reduces complexity and saves money

A 1.5.4 Application Virtualization

Virtualization in an application separates the OS from the application. Then the application will run on server or other remote computer rather than on computer in which it is deployed. The main benefit of application virtualization is that it is possible to run incompatible applications at same time. It is also possible by the user to run an application which is not designed for the computer’s OS from which they are accessing it.

A 1.5.5 Network Virtualization

Network Virtualization is the process of combining all of the resources within one network. It allows administrator of the network to share resources across all the users. The network is being divided into many
different channels, where each contains network’s bandwidth. It makes it easier for the administrator to assign resources as the users need them.

A 1.6 TYPES OF HYPERVERSOR

A 1.6.1 Type 1 Hypervisor

The hypervisor of this type is deployed as a bare-metal installation. The bare-metal installation refers that the first interface to be installed on a server as the operating system should be the hypervisor. By this the user can achieve the advantages that the hypervisor will be in touch directly with the underlying physical server hardware. Those resources then undergo Para-virtualization and are delivered to the running VMs. Type 1 hypervisor provides higher level of efficiency and security in virtualization.

Figure A 1.5 shows one physical system with a type 1 hypervisor running directly on the system hardware, and three virtual systems using virtual resources provided by the hypervisor. [Image Source: Wikipedia]
A 1.6.2 Type 2 Hypervisor

Type II hypervisors are known as hosted hypervisor. In this type the software is not installed onto the bare-metal. The hypervisor is implemented on top of an already live operating system. Type II hypervisors provide virtualization services like I/O device support and memory management. The use of this kind of hypervisor is found to be greater in client systems that support very large range of I/O devices. Since the hypervisor is installed and run in a live operating system, there have been a lot of questions regarding the performance of this kind. Anyway it has been found that the latency is minimal and the hypervisor can still perform optimally.
Fig. A 1.6 shows one physical system with a type 2 hypervisor running on a host operating system and virtual systems using the virtual resources provided by the hypervisor. [Image Source: Wikipedia]

A 1.7 CLOUD ARCHITECTURE

A 1.7.1 Front End Platforms

The front end platforms are called clients or cloud clients. The cloud client includes servers, fat or thick clients, zero clients and mobile devices. These clients communicate with the cloud database through an application accessed through the web.

- **Zero Clients**
  These are clients that run via the network. The zero clients initialize the network. It also helps to gather required
configuration files and gives information about the storage of Operating System binaries. These clients are highly depend on the network quality. If it goes down, the client device becomes useless.

- **Fat Clients**
  Fat-client refers to a multi-tier client server in which the client application part always execute on the stand alone system and the server part of the application reside on a server along with the application code.

### A 1.7.2 Back End Platforms

- **Cloud Storage:** In this back end, data is stored in users system and also in virtualized pools, so that different clients from the world can access it and use. The data is hosted in virtual pools by third parties. This cloud storage is generally owned by big hosting giants, so if a user or organization wants to host their resources they probably should buy or lease storage space from the hosting companies. The hosting companies virtualize the applications and resources in such a way the customers want and make them to be exposed as storage pools. In these storage pools, the customers store their data files and objects. These pools may span across multiple storage servers. The data security depends upon the hosting organizations.
A 1.7.3 Cloud Based Delivery

This architecture mainly specifies the services that are delivered by the cloud environment to the external world. The entire cloud services can be classified into mainly five. They are as follows:

- **Infrastructure as a Service (IaaS):** The abilities to provide provision on applications and resources like hardware, storage, processors and other fundamentals. Through Virtualization, CSP’s are able to split, assign and resize resources to build systems as demanded by consumers. Other services provided by IaaS are Operating System, Firewall, Router and Load Balancer. Service provider supply resources on-demand from their large pools mounted in data centers.

- **Platform as a Service (PaaS):** The ability to provide the entire infrastructure is being needed to run applications on Internet. It always has IaaS as a backbone. Basically PaaS is defined as delivery solution for a service and computing platform. The size of the hardware resources demanded by execution is made in a transparent manner. It includes operating system, programming language, and web server and database.

- **Software as a Service (SaaS):** The ability to provide software as a solution, also known as On Demand or Web Based or Line Software in this pre-made, along with required software, operating system and network are provided. The users have the freedom to run the software from their cloud clients via the network. It make unnecessary to have a software physical copy on your devices. It make easier to have same software in all devices without installation in each device. SaaS has PaaS as a backbone.
• **Network as a Service (NaaS):** The ability to provide network/transport connectivity services or inter-cloud network connectivity services by optimizing the resource allocations and considering computing resources and network as a unified whole.

• **Development as a Service (DaaS):** It has the ability to provide development tools which are shared among communities. It seems to be equal to locally installed development tools.

A 1.7.4 Cloud Networking

This architecture component refers to the connectivity aspects of cloud environment to the external world. The connectivity is established via networks like Internet, intranet and inter-cloud. The cloud networking offers:

- High bandwidth
- Agile network
- Network security

Cloud provides efficient security mechanisms in connectivity. But when it comes with multi-tenancy it is impossible to maintain confidentiality because it always deals with the segregation of multiple customers.
A 1.8 ADVANTAGES OF CLOUD COMPUTING IN THE CURRENT SCENARIO

A 1.8.1 Cost Efficient

Cloud computing reduces the cost for maintenance and upgradation. Traditional software costs more for companies in finance. For establishment it costs more for getting license. The cloud is cheaper than the traditional and significantly lowers the IT expenses. Managing and maintaining cost may reduce by moving to cloud computing. By using the service provider services rather than purchasing the systems for the business, the cost is reduced. It reduces the operating systems cost because,

- System upgradation cost, new software included.
- Need not to pay wages for expert staff.
- Reduce the cost of energy consumption.
- Few delay in time.

A 1.8.2 Flexibility of Work Practices

In cloud computing the employees can work more flexibly. For example, the employees can access data on holiday or from home. When the employee is off-site then also employee can access data by connecting to virtual office easily. Network dependency means the Internet dependency and independence from office. Employees can able to access data without having wired servers. Cloud computing provides flexibility for workers and for changes implementation with low cost. Because hard-wired
infrastructure is not needed for organizations that cost more and experiment room.

A 1.8.3 Collaboration Efficiency

Collaboration efficiency in a cloud environment gives the business ability to share and communicate. If the project works in different locations, cloud computing is useful to give third party access, employees and contractors. It is easy to share the records with advisors when using cloud computing.

A 1.8.4 Access to Automatic Updates

Updates are automatically done for IT requirements that may include service fee. The systems are regularly updated with latest technology based on the cloud service provider. The versions are up-to-date in the software and processing power.

A 1.8.5 Reliability

The reliability in cloud computing is to provide in-house systems. The vendor provides technical support for 24/7 and experienced staff for infrastructure support and the benefit reaches the entire client. In regards of organization which has on-site IT people it is more reliable.
A 1.8.6 Scalability

The business may scale up or down in operation and also need storage quickly. Based on these situation cloud allows flexibility as the needs change. The cloud provider will provide purchase or upgrade of the software. Using cloud it will reduce the time which definitely helps to run the business.

A 1.8.7 Business Continuity

The business continuity planning protects the data and systems. When there occurs a natural disaster or a power failure the data stored in cloud is protected and backed up in safe location. Accessing data quickly allows to conduct the business, reduces the productivity loss.

A 1.8.8 Innovation

Users pay attention to innovation process because users do not want to manage the resources manually. The phases like prototype and testing are quick development paced in cloud computing.

A 1.8.9 Multiple Users at One Time

Cloud computing reduces the global waste. Multiple users can share the resources so it is environmental friendly. The time taken is decreased and the available resources are increased.
A 1.8.10 Customize Settings

The cloud computing allows the user to customize the applications. This is a great benefit because the online business is very competitive.

A 1.9 PROBLEMS IN CLOUD COMPUTING

A 1.9.1 Data Integrity

One of the major threats in storing the data in cloud is that it can be accessed from anywhere by anyone. Cloud does not differentiate a sensitive data from that of a common data. Hence there occurs a data integrity problem in cloud computing.

A 1.9.2 Data Theft

Since it is cost effective and more flexible, most of the cloud vendors prefer leasing a server from third party cloud service providers instead of acquiring a server on their own. As customers are not well aware of those things, there is a high possibility of data being stolen from the external server by an unauthorized user.

A 1.9.3 Privacy Issues

Customer’s Personal information need to be protected from other operators. A vendor should make sure of who is accessing the data and
who is maintaining the server in order to secure the customer’s personal information.

A 1.9.4 Infected Application

Vendor should make sure that he/she is having the complete control over the server for monitoring and maintenance. This will prevent any malicious user from uploading any infected applications onto the cloud infrastructure.

A 1.9.5 Data Loss

If there is a financial crisis, the vendor may be forced to close the cloud infrastructure which in turn will result in loss of data to the customers. Therefore customer will not be able to access his critical data stored in the cloud. Hence, data loss proves to be a major issue in cloud computing.

A 1.9.6 Data Location

Customer is not aware of where his own data is stored in the cloud as nothing is transparent to him. Vendor does not reveal any information regarding the location of data to the customers. Data need not be stored in the same location where customer lives.
A 1.9.7 Security on Vendor Level

Vendor should make sure that server is well protected from the external malicious threats. A cloud infrastructure is good only when it is free from security threats.

A 1.9.8 Security on User Level

Even though the vendor has provided a good security layer for the customer, the customer should make sure that because of its own action, there shouldn’t be any loss of data or tampering of data for other users who are using the same cloud. Computing on the cloud requires vigilance about security, manageability, standards, governance, and compliance:

- **Cloud Security**: The same security principles that apply to on-site computing apply to cloud computing security.
- **Identity Management**: Managing personal identity information so that access to computer resources, applications, data, and services is controlled properly.
- **Detection and Forensics**: Separating legitimate from illegitimate activity.
- **Encryption**: Coding to protect one’s information assets.
- **Cloud Manageability**: The consumer would need a consistent view across both on-premises and cloud-based environments. This includes managing the assets, provisioning as well as the quality of service (QOS) received from the service provider.
- **Cloud Standards**: A standard is an agreed-upon approach for doing something. Cloud standards ensure interoperability, so the
user can take tools, applications, virtual images, and more, and use them in another cloud environment without having to do any rework. Portability lets the user take one application or instance running on one vendor’s implementation and deploy it on another vendor’s implementation.

- **Cloud Governance and Compliance:** Governance defines who’s responsible for what and the policies and procedures that the user or groups need to follow. Cloud governance requires governing the CSP’s own infrastructure as well as infrastructure that they don’t totally control. Cloud governance has two key components: understanding compliance and risk and business performance goals.

- **Data in the Cloud:** Managing data in the cloud requires data security and privacy, including controls for moving data from point A to point B. It also includes managing data storage and the resources for large-scale data processing.