ABSTRACT
With cloud computing, web application providers can easily move their applications to cloud data centers. On-demand cloud elasticity allows cloud users to acquire or release computing resources on demand. For complex computational workloads, this makes auto-scaling of resources possible for providers especially under dynamic workload. In all cases, cost optimization for system resources and Quality of Service (QoS) remains the top concern. This paper discussed cloud computing as a smart alternative to legacy computing models. Its taxonomy, characteristics, Security Objectives, Service level agreements, benefits and challenges are presented. A conceptual framework for cloud collaboration among the various states of Nigeria is presented. Startups and other low scale enterprises will readily benefit from cloud based collaboration.

Keywords
Cloud Datacenter, Collaboration, Disruptive Technology, Big Data, Social Networks.

1. INTRODUCTION
The 21st century society has been re-organized such that essential services (utilities) are easily provided for easy access. Such utility services as water, electricity, gas, and telephony, computing is critical for daily life routines [1]. Everyone must frequently depend on these services whenever the end-user has need for them. This form of on-demand computing can be used in various implementation frameworks offering better advantages over legacy systems [2].

Cloud computing is a model for enabling network user’s on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned and released to the client without direct service provider interaction [3]. It is essentially the use of virtual servers made available over the internet. While this form of computing entrusts remote services with a user’s data, software and computation, slow migration towards usage has remain obvious. This is mainly due to the infrastructure and support costs involved in the entire ecosystem. However, cloud computing platforms have attributes depicting both clusters and Grids [1] having its self-inflicted characteristics such as active support for virtualization, dynamically scalable services with on-line Web Service interfaces even for other forms of integration. Besides, it offers room for value added services by building on Cloud compute, storage, and application services.

The aim of this work is to provide fundamental explanations on cloud terminologies for market oriented architectures, while presenting the characteristics, advantages of this computing paradigm for emerging disruptive technologies.

The emphasis of this paper will be on market oriented architectures and disruptive computing models.

2. CLOUD TAXONOMY
2.1 Classical Cloud Computing Taxonomies
There are essential concepts associated with cloud computing. These include:

i. Back office: This is a concept whereby technology is used to simplify and save cost for companies by taking the technical issues out of the equation so that businesses can focus their energy on creating a superior product or service. This is commonly known as back office tasks. They are generally rudimentary data parsing procedures that are time consuming as well as tedious. Back office applications are software that an organization uses to administer operations that are not related to any direct sales effort and interfaces that are not seen by consumers. An example of a back office service that is out today is Amazon’s Web Services platform [2].

ii. Web 2.0: Web 2.0 cloud computing is a blanket term, but it is usually associated with some type of social networking technology – that is, a large number of social users that are interconnected via their relations with the people and things they find interesting. It describes a second generation of the World Wide Web focused on the ability for people to collaborate and share information online. It basically refers to the transition from static HTML web pages to a more dynamic web that is more organized. One of the biggest Web 2.0 companies today is Facebook [4].

iii. On-demand computing: On demand computing is a business terminology often referred to as back office processing power. For example, a remote data processing center that processes payroll functions for a company located thousands of miles away. It is an enterprise-level model of technology and computing in which resources are provided on an as-needed and when-needed basis. This type of model is usually created to overcome the challenges facing enterprises that need to meet fluctuating demands.

iv. Thin client: A thin client is a term used for a terminal that connects to the cloud. This could be a computer, a cell phone or even an mp3 player. It can be referred to as software as well. As long as the device can connect to the cloud, it is known as a thin client for all intents and purposes. The meaning behind its being “thin” is that it does not require much processing power to be a client to the cloud itself.
v. **Workload migration:** Workload migration is the concept of optimizing server farm technology to be data and energy efficient [5]. With so much processing ability coupled with an enormous amount of power consumption, companies managing server farm technology are finding that they need IT people who are well versed in workload migration technology to be able to manage all that this entails. Some cloud computing companies tout services to help companies with workload migration, offering services that assist their clients with the “internal cloud” process.

vi. **Server farm:** A server farm is a cluster of computers whose sole purpose is to provide processing power greater than what a single machine would be able to do on its own [5]. A perfect example of this would be what companies use for web hosting of individual websites. Even though there is one website the server farm provides failover capability in case something was to happen to any single machine hosting the website. It is ideal for server farms to be located near a reliable source of power.

vii. **Market oriented Entities** - In cloud computing, market-oriented resource management [6], [7] is used to regulate the supply and demand of Cloud resources in order to achieve market equilibrium (satisfying demand equality to supply availability), while offering positive feedback in terms of economic incentives for both Cloud consumers and providers, and promoting QoS-based resource allocation mechanisms. This differentiates service requests based on their utility [1]. Also, consumers can gain from efficient cost reduction of providers creating a non-monopolistic market leading to lower cost/prices driven market structure. Figure 1 illustrates the high-level architecture for supporting market oriented resource allocation in Data Centers and Clouds.

From Figure 1, the following elements have been identified [1]:

- **Users/Brokers:** Users or brokers acts on their behalf to submit service requests from anywhere in the world to the Data Center and Cloud for processing.
- **SLA Resource Allocator:** This acts as the interface between the Data Center/Cloud service provider and external users/brokers. It requires the interaction of the following mechanisms to support SLA-oriented resource management:
  i. **Cloud Service Request Examiner and Admission Control (CSREC)** which examines sent requests for QoS requirements and then deterring either to accept or reject such requests. This eradicates resource overloading while gathering status information regarding resource availability (from the VM Monitor mechanism) and workload processing (from the Service Request Monitor mechanism) in order to make resource allocation decisions efficiently. Then, it assigns requests to VMs and determines resource entitlements for allocated VMs.
  ii. **Cloud Pricing:** The Pricing mechanism decides how service requests are charged. For instance, requests can be charged based on submission time (peak/ off-peak), pricing rates (fixed/changing) or availability of resources (supply/demand). Pricing serves as a basis for managing the supply and demand of computing resources within the Data Center and facilitates in prioritizing resource allocations effectively.
  iii. **Cloud Accounting:** The Accounting mechanism maintains the actual usage of resources by requests so that the final cost can be computed and charged to the users. In addition, the maintained historical usage information can be utilized by the Service Request Examiner and Admission Control mechanism to improve resource allocation decisions.
  iv. **VM Monitor:** The VM Monitor mechanism keeps track of the availability of VMs and their resource entitlements.
  v. **Dispatcher:** The Dispatcher mechanism starts the execution of accepted service requests on allocated VMs.
  vi. **Service Request Monitor:** The Service Request Monitor mechanism keeps track of the execution progress of service requests.
  vii. **VMs:** Multiple VMs can be started and stopped on-demand on a single physical machine to meet accepted service requests, hence providing maximum flexibility to configure various partitions of resources on the same physical machine to different specific requirements of service requests. In addition, multiple VMs can concurrently run applications based on different operating system environments on a single physical machine since every VM is completely isolated from one another on the same physical machine.
  viii. **Physical Machines:** The Cloud Data Center comprises multiple computing servers that provide resources to meet service demands.
Essentially, cloud computing used in commercial offerings enable crucial business operations of companies to maximize profits. In this case, there are critical QoS parameters to be considered in a service request, such as time, cost, reliability and trust/security. In context, QoS requirements cannot be static and may change over time due to continuing changes in business operations and operating environments. In short, there should be greater importance on customers since they pay for accessing services in Clouds. In addition, the state-of-the-art in Cloud computing has no or limited support for dynamic negotiation of SLAs between participants and mechanisms for automatic allocation of resources to multiple competing requests. Commercial offerings of market-oriented Clouds must be able to:

- Support customer-driven service management based on customer profiles and requested service requirements,
- Define computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs,
- Derive appropriate market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain SLA oriented resource allocation,
- Incorporate autonomic resource management models that effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations, and

Leverage VM technology to dynamically assign resource shares according to service requirements.

### 2.3. Classical Cloud Characteristics

There five essential characteristics according to National Institute of Standards and Technology (NIST). These include [8]:

i. **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

ii. **Broadband Network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

iii. **Resource Pooling**: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

iv. **Rapid Elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

v. **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

vi. **Agility**: This improves with users’ ability to re-provision technological infrastructure resources.

vii. **Application programming interface (API) accessibility**: API accessibility to software could enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.

viii. **Cost Optimization**: Cost is showed to be reduced in a public cloud delivery model. Also, capital expenditure is converted to operational expenditure This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks.

ix. **Device and location independence**: This enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone)

x. **Virtualization Technology**: This allows servers and storage devices to be shared and utilization is increased. Applications can be easily migrated from one physical server to another.

xi. **Multi-tenancy**: This enables sharing of resources and costs across a large pool of users, hence allowing for:

i. Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

ii. Peak-load capacity increases (users need not engineer for highest possible load-levels)

iii. Utilisation and efficiency improvements for systems that are often only 10–20% utilized

iv. **Reliability**: This is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

xii. **Scalability and Elasticity**: This is via dynamic (“on-demand”) provisioning of resources on a fine-grained, self-service basis near real-time without users having to engineer for peak loads [9].

xiii. **Performance Monitoring**: Performance is monitored in a consistent manner for loosely coupled architectures used in construct web services as the system interface.

xiv. **Security Improvement**: This could improve due to centralization of data, and increased security-focused resources, etc [10]. However, there are still persist concerns about loss of control over certain sensitive data, and the lack of security for stored kernels. According to [11], security is still better than other traditional systems, in part because providers
are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users’ desire to retain control over the infrastructure and avoid losing control of information security.

xv. **Maintenance of cloud computing:** For applications, this is easier, because they do not need to be installed on each user's computer and can be accessed from different places. This work will now present related cloud market oriented computing below.

### 2.4. Market Oriented Cloud Computing Technologies

There are various market oriented computing models beside Cloud computing. Each of these models/technologies shares certain perspective with cloud computing:

- **Grid Computing Model:** In [12], Grid computing is defined as a distributed computing paradigm that coordinates networked resources to achieve a common computational objective. It is the collection of loosely coupled, heterogeneous, and geographically dispersed computer resources from multiple locations to reach a common goal. It is a distributed system with non-interactive workloads that involve a large number of files. This model if originally driven by scientific applications which are usually computation-intensive. Cloud computing is similar to Grid computing in that it also employs distributed resources to achieve application-level objectives. However, cloud computing takes one step further by leveraging virtualization technologies at multiple levels (hardware and application platform) to realize resource sharing and dynamic resource provisioning.

- **Utility Computing Model:** It involves the provision of resources on-demand and customers are charged based on usage rather than a flat rate. Cloud computing can be perceived as a realization of utility computing. It adopts a utility-based pricing scheme entirely for economic reasons. With on-demand resource provisioning and utility based pricing, service providers can truly maximize resource utilization and minimize their operating costs.

- **Virtualization Model:** Virtualization is a technology that abstracts away the details of physical hardware and provides virtualized resources for high-level applications. A virtualized server is commonly called a virtual machine (VM). Virtualization forms the foundation of cloud computing, as it provides the capability of pooling computing resources from clusters of servers and dynamically assigning or reassigning virtual resources to applications on-demand as shown in figure 2.

- **Autonomic Computing Model:** Originally coined by IBM in 2001, autonomic computing aims at building computing systems capable of self-

Figure 2: Cloud Virtualization server clusters [2]

Based on these background, Cloud computing is proposed for the deployment of vibrant mission critical applications. It is now clear that cloud computing leverages virtualization technology to achieve the goal of providing computing resources as a utility. It shares certain aspects with grid computing and autonomic computing but differs from them in other aspects. Therefore, it offers unique benefits and imposes distinctive challenges to meet its requirements.

### 3. CLOUD COMPUTING ARCHITECTURE

This section describes the architectural, business and various operation models of cloud computing.

#### 3.1. Layered Model of Cloud Computing

In a typical architecture of a cloud computing environment, there are five major sub layers namely:

i. **Facility Layer:** This include: Heating, ventilation, air conditioning (HVAC), power, communications, and other aspects of the physical plant comprise the lowest layer, the facility layer.

ii. **Hardware Layer:** This layer is responsible for managing the physical resources of the cloud, including physical servers, routers, switches, power and cooling systems. In practice, the hardware layer is typically implemented in data center. A data center usually contains thousands of servers that are organized in racks and interconnected through switches, routers or other fabrics [12]. Typical issues at hardware layer include hardware configuration, fault tolerance, traffic management, power and cooling resource management.

iii. **Infrastructure Layer:** This is known as the virtualization layer. This layer creates a pool of storage and computing resources by partitioning the physical resources using virtualization technologies such as Xen, KVM and VMware. The infrastructure layer is an essential component of cloud computing, since many key features, such as
dynamic resource assignment, are only made available through virtualization technologies.

iv. Platform Layer: This is built on top of the infrastructure layer; the platform layer consists of operating systems and application frameworks. The purpose of the platform layer is to minimize the burden of deploying applications directly into VM containers. For example, Google App Engine operates at the platform layer to provide API support for implementing storage, database and business logic of typical web applications.

v. Application layer: At the highest level of the hierarchy, the application layer consists of the actual cloud applications. Different from traditional applications, cloud applications can leverage the automatic-scaling feature to achieve better performance, availability and lower operating cost. Compared to traditional service hosting environments such as dedicated server farms, the architecture of cloud computing is more modular. Each layer is loosely coupled with the layers above and below, allowing each layer to evolve separately. This is similar to the design of the OSI reference model.

3.2. Service Model of Cloud Computing

Cloud computing has functional service models discussed below.

i. Software as a Service (SaaS): The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface [5]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of SaaS include: Google Apps, Microsoft Office 365, Onlive, GT Nexus, etc.

ii. Platform as a Service (PaaS): Again, the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Examples of PaaS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku.

iii. Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). Offering virtualized resources (computation, storage, and communication) on demand is known as Infrastructure as a Service (IaaS) [12]. Infrastructure services are considered to be the bottom layer of cloud computing systems. Amazon Web Services mainly offers IaaS, which in the case of its EC2 service means offering virtual machines with a software stack that can be customized similar to how an ordinary physical server would be customized. Users are given privileges to perform numerous activities to the server, such as: starting and stopping it, customizing it by installing software packages, attaching virtual disks to it, and configuring access permissions and firewalls rules [13].

3.3. Deployment Models of Cloud Computing

This section will discuss the various deployment models found in cloud based computing. They include:

i. Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and it will require the organization to re-evaluate decisions about existing resources. When it is done right, it can have a positive impact on a business, but every one of the steps in the project raises security issues that must be addressed in order to avoid serious vulnerabilities. They have attracted criticism because users still have to buy, build, and manage them and thus do not benefit from less hands-on management. [14] essentially lacking the economic model that makes cloud computing such an intriguing concept[15].

ii. Community cloud: This type of cloud infrastructure is provisioned for exclusive use by a specific community of consumers. For example, organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

iii. Public cloud: This is the type of cloud infrastructure provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model.

iv. Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables
data and application portability (e.g., cloud bursting for load balancing between clouds). By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without depending on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure [17].

3.4. Cloud Architectural Datacenters

According to Cisco [18], a data center, refers to the computation power and storage, is central to cloud computing and contains thousands of devices like servers, switches and routers. The data center is home to the computational power, storage, and applications necessary to support an enterprise business [4]. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered. Another important aspect of the data center design is flexibility in quickly deploying and supporting new services so as to be able to support new applications in a short time frame. This can result in a significant competitive advantage. For such a design serious consideration has to be given to areas such as port density, access layer uplink bandwidth, true server capacity, and oversubscription, etc. The data center network design is based on a proven layered approach, which has been tested and improved over the past several years in some of the largest data center implementations in the world. The layered approach is the basic foundation of the data center design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance as depicted in figure 3.

![Figure 3: Basic layered design of Data Center Network Infrastructure [18].](image)

The various layers of the data center design include: the core, aggregation, and access layers. These have been well articulated in [19]. The core layer provides the high-speed packet switching backbone for all flows going in and out of the data center; the aggregation layer module provide important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy, the access layer is where the servers physically attach to the network. Basically, the design of data center network architecture should meet the following objectives [20], [21].

- Uniform high capacity: The maximum rate of a server-to-server traffic flow should be limited only by the available capacity on the network-interface cards of the sending and receiving servers, and assigning servers to a service should be independent of the network topology. It should be possible for an arbitrary host in the data center to communicate with any other host in the network at the full bandwidth of its local network interface.
- Free Virtual Machine migration: Virtualization allows the entire VM state to be transmitted across the network to migrate a VM from one physical machine to another. A cloud computing hosting service may migrate VMs for statistical multiplexing or dynamically changing communication patterns to achieve high bandwidth for tightly coupled hosts or to achieve variable heat distribution and power availability in the data center. The communication topology should be designed so as to support rapid virtual machine migration.
- Resiliency: Failures will be common at scale. The network infrastructure must be fault-tolerant against various types of server failures, link outages, or server-rack failures. Existing unicast and multicast communications should not be affected to the extent allowed by the underlying physical connectivity.
- Scalability: The network infrastructure must be able to scale to a large number of servers and allow for incremental expansion.
- Backward compatibility: The network infrastructure should be backward compatible with switches and routers running Ethernet and IP. Because existing data centres have commonly leveraged commodity Ethernet and IP based devices, they should also be used in the new architecture without major modifications.

For the data center design model, these are the identified models:

i. **Multi-tier model**: This is the most common design in the enterprise setup that is dominated by HTTP-based applications in a multi-tier approach. It is based on the web, application, and database layered design supporting commerce and enterprise business ERP and CRM solutions. The multi-tier model uses software that runs as separate processes on the same machine using inter-process communication (IPC) or on different machines with communications over the network. Typically, the following three tiers are used: Web-server, Application and Database. The multi-tier model relies on security and application optimization services to be provided in the network.

ii. **The server cluster model**: This model grew out of the university and scientific community to emerge across enterprise business verticals including financial, manufacturing, and entertainment. The server cluster model is most commonly associated with high-performance computing (HPC), parallel computing, and high-throughput computing (HTC) environments, but can also be associated with grid/utility computing. These designs are typically based on customized, and sometimes proprietary, application architectures that are built to serve particular business objectives. Rather than the three-layered approach discussed
in figure 3, the work in [20], [21] proposed server-centric, recursively defined network structure.

### 3.5. Service Level Agreement

Another vital taxonomy found in cloud computing is the Service Level Agreement (SLA) [23]. SLA defines the interaction between a cloud service provider and a cloud service consumer. It contains the following details:

- A set of services the provider will deliver
- A complete, specific definition of each service
- The responsibilities of the provider and the consumer
- A set of metrics to determine whether the provider is delivering the service as promised.
- An auditing mechanism to monitor the service
- The remedies available to the consumer and provider if the terms of the SLA are not met.
- How the SLA will change over time

In the cloud marketplace, there are two types of features expressed: The Off-the-shelf agreements and negotiated agreements between a provider and consumer to meet that consumer's specific needs. If it is unlikely that any consumer with critical data and applications will be able to use the first type. Therefore the consumer's first step in approaching an SLA (and the cloud in general) is to determine how critical their data and applications are. Most public cloud services offer a non-negotiable SLA. With these providers, a consumer whose requirements aren't met has two remedies:

1. Accept a credit towards next month's bill (after paying this month's bill in full), or
2. Stop using the service.

Clearly an SLA with these terms is unacceptable for any mission-critical applications or data. On the other hand, an SLA with these terms will be far less expensive than a cloud service provided under a negotiated SLA. Key factors to be considered in an SLA include the following:

- **Security:** The security-related aspects of an SLA should be written. A cloud consumer must understand their security requirements and what controls and federation patterns are necessary to meet those requirements. In turn, a cloud provider must understand what they must deliver to the consumer to enable the appropriate controls and federation patterns.
- **Data Encryption:** If a consumer is storing vital data in the cloud, it is important that the data be encrypted while it is in motion and while it is at rest. The details of the encryption algorithms and access control policies should be specified in the SLA.
- **Privacy:** Basic privacy concerns are addressed by requirements such as data encryption, retention and deletion. In addition, an SLA should make it clear how the cloud provider isolates data and applications in a multi-tenant environment.
- **Data Retention and Deletion:** Many organizations have legal requirements that data must be kept for a certain period of time. Some organizations also require that data be deleted after a certain period of time. Cloud providers must be able to prove that they are compliant with these policies.
- **Hardware Erasure and Destruction:** A common source of data leaks is the improper disposal of hardware. If a cloud provider's hard drive fails, the platters of that disk should be zeroed out before the drive is disposed or recycled. On a similar note, many cloud providers offer the added protection of zeroing out memory space after a consumer powers off a virtual machine.
- **Regulatory Compliance:** Many types of data and applications are subject to regulations. Some of those are laws, while others are industry-specific. If regulations must be enforced, the cloud provider must be able to prove their compliance.
- **Transparency:** Under the SLAs of some cloud providers, the consumer bears the burden of proving that the provider failed to live up to the terms of the SLA. A provider's service might be down for hours, but consumers who are unable to prove that downtime is not eligible for any sort of compensation. For critical data and applications, providers must be proactive in notifying consumers when the terms of the SLA are breached. This includes infrastructure issues such as outages and performance problems as well as security incidents.
- **Auditability:** Many consumer requirements include adherence to legal regulations or industry standards. Because the consumer is liable for any breaches that occur, it is vital that the consumer be able to audit the provider's systems and procedures. An SLA should make it clear how and when those audits take place. Because audits are disruptive and expensive, the provider will most likely place limits and charges on them.
audited after the fact. The metrics of an SLA must be objectively and unambiguously defined. Cloud consumers will have an endless variety of metrics depending on the nature of their applications and data. Although listing all metrics is impossible, some of the most common are:

- **Throughput** – How quickly the service responds
- **Reliability** – How often the service is available
- **Load balancing** – When elasticity kicks in (new VMs are booted or terminated, for example)
- **Durability** – How likely the data is to be lost
- **Elasticity** – The ability for a given resource to grow infinitely, with limits (the maximum amount of storage or bandwidth, for example) clearly stated
- **Linearity** – How a system performs as the load increases
- **Agility** – How quickly the provider responds as the consumer’s resource load scales up and down
- **Automation** – What percentage of requests to the provider are handled without any human interaction
- **Customer service response times** – How quickly the provider responds to a service request. This refers to the human interactions required when something goes wrong with the on-demand, self-service aspects of the cloud.

xiii. **Machine-Readable SLAs:** A machine-readable language for SLAs would enable an automated cloud broker that could select a cloud provider dynamically. One of the basic characteristics of cloud computing is on-demand self-service; an automated cloud broker would extend this characteristic by selecting the cloud provider on demand as well. The broker could select a cloud provider based on business criteria defined by the consumer.

xiv. **Human Interaction:** Although on-demand self-service is one of the basic characteristics of cloud computing, the fact remains that there will always be problems that can only be resolved with human interaction. These situations must be rare, but many SLAs will include guarantees about the provider’s responsiveness to requests for support. Typical guarantees will cover how many requests the consumer can make, how much they will cost and how soon the provider will respond.

### 3.6. Cloud Security Objectives

In this section, the major security objectives for a cloud computing implementation include the following:

- **Protect customer data from unauthorized access, disclosure, modification or monitoring.** This includes supporting identity management such that the customer has the capability to enforce identity and access control policies on authorized users accessing cloud services. This includes the ability of a customer to make access to its data selectively available to other users.
- **Protection from supply chain threats.** This includes ensuring the trustworthiness and reliability of the service provider as well as the trustworthiness of the hardware and software used.
- **Prevent unauthorized access to cloud computing infrastructure resources.** This includes implementing security domains that have logical separation between computing resources (e.g. logical separation of customer workloads running on the same physical server by VM monitors [hypervisors] in a multitenant environment) and using secure-by-default configurations.
- **Design Web applications deployed in a cloud for an Internet threat model and embedding security into the software development process.**
- **Protect Internet browsers from attacks to mitigate end-user security vulnerabilities.** This includes taking measures to protect Internet-connected personal computing devices by applying security software, personal firewalls, and patch maintenance.
- **Deploy access control and intrusion detection technologies at the cloud provider, and conduct an independent assessment to verify that they are in place.** This includes (but does not rely on) traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes restricting physical access to network and devices; protecting individual components from exploitation through security patch deployment; setting as default most secure configurations; disabling all unused ports and services; using role-based access control; monitoring audit trails; minimizing the use of privilege; using antivirus software; and encrypting communications
- **Define trust boundaries between service provider(s) and consumers to ensure that the responsibility for providing security is clear.**
- **Support portability such that the customer can take action to change cloud service providers when needed to satisfy availability, confidentiality, and integrity requirements.** This includes the ability to close an account on a particular date and time, and to copy data from one service provider to another.

Organizations can protect sensitive user data in the cloud by:

- **Use of Strong Encryption standard:** The goal of encryption is to ensure that data stored in the cloud is protected against unauthorized access. Strong encryption technology like the Advanced Encryption Standard (AES), is difficult to break through. AES encryption with a key length of 256 bits should be implemented for better security of users’ data
- **Effective Key Management:** Encryption keys should be managed efficiently by using advanced key management technologies. Enterprises should manage their encryption effectively by efficient key assignment, periodic key rotation, and re-encryption of data with new keys
- **Access Control:** Encrypting data at rest, use and in transit reduces the risk of external attacks. Internal attacks should also be taken care of. By putting the
Cloud service provider in charge of encrypting sensitive user data, the enterprises are opening doors for new internal attacks. Employees must be given access to the information that is required or relevant to their responsibilities. They should be trained to manage and deal with encrypted data effectively by following the security procedures of the organization.

- Compliance with Security policies and procedures: Enterprises must encrypt sensitive user data based on industry compliance guidelines.

4. BENEFITS OF CLOUD COMPUTING
In a vibrant ecosystem, the identified benefits of cloud computing are presented below:

- **Flexibility:** With the idea of a server rental model in place, it is easier to become more flexible in terms of technology resources [24]. The reason is that with cloud computing, businesses can scale with technology. Decision on how much storage space to use and how much processing power is required is rapidly fixed. While working to update software applications, the process can be pushed out much faster and more efficiently. Administrators can choose when to update an application enterprise-wide all in real time and how much they want to spend on IT with cloud technology.

- **Scalability:** With cloud computing one person can go from small to large quickly. Research organizations would be a great example in that they would be able to process heavy amounts of data at a specified time, and then go back to the norm—all without requiring those heavy servers. It is better for many organizations to simply rent the use of powerful computing as opposed to buying equipment outright. Cyclical and seasonal businesses would be a great fit for the rent-a-server structure that cloud computing avails to them. One cyclical business, like tax preparation, would be able to utilize their resources within the first six months of the year—when they are busy—and then retract their usage instantly when they are not needed.

- **Capital Investment:** IT spending takes a large portion of money out of general funds that companies could use for other pressing business needs such as marketing, research and development and human resources. With cloud computing, many rudimentary IT purchases for things like hardware will no longer be an issue as long as that task or set of tasks can be performed by the cloud.

- **Portability:** In today’s global economy organizations need to have people on the ground, far from headquarters, to manage things. With cloud computing technology, organizations are able to use their computing power wherever their people are as long as users are able to access thin clients. With thin client technology the scale of geography and time variation is flattened somewhat and this allows companies that are trying to globally integrate to be able to be more flexible than ever before.

- The redundancy of cloud computing will help system administrators to ensure constant uptime.

- Cloud computing makes the use of software collaboration tools easier thus increasing productivity. Using this method, projects can be worked on in real time with several people all at once.

- The best part is that when files are saved it is done on the cloud where it is stored for safekeeping.

- The price of energy has increased to a large degree with the fast pace of globalization. As such, cloud computing can also achieve the goal for organizations to have energy efficiency. It is more efficient for power hungry servers to all be in one location so that data center managers can better optimize them using power saving procedures. This can be done through a variety of methods which could include having servers in a timed power saving mode to reduce power usage to even being located near a renewable energy source.

One element that may indeed have some appeal for organizations would be companies who do research that requires sudden spikes in computing power. Research and development departments, in this case, would be able to employ cloud processing for huge spikes of data testing that would need to be done on a periodic basis without requiring heavy infrastructure investment.

5. CHALLENGES FACING CLOUD COMPUTING
Till date, there are myriads of problems facing disruptive cloud computing paradigm especially with the advent of Internet of things and fog/edge computing. This work has enumerated some these challenges below.

i. **Dependability:** While unlikely, it is very possible that data could be lost. It is very important to look deeply into a vendor’s back up plans should something happen. Ideally knowledge of the geographical location where the data is stored would be helpful but many cloud providers are reluctant to give out this sensitive information. This could be a problem for companies that rely on the cloud to keep critical business functions up and running. One solution around dependability would be to host the most critical functions within the company while much of the non-critical processing can be done through a cloud vendor [5].

ii. **Security:** Being able to keep important data secure has always been a priority in IT, but with a technology that takes information outside of the virtual secure walls of most corporations, security becomes an issue. The usage of thin clients could possibly be high-jacked if people are careless with data.

iii. **Little or no reference:** Because of privacy concerns, cloud vendors for the most part are unable or unwilling to present case studies about companies that are currently using their services. As a matter of fact, there are very few large companies that are publicly reporting their usage of cloud computing at a large scale level. This leaves many organizations feeling shy about using cloud computing resources.

iv. **A bigger issue may lie in the event of a disaster recovery or backup failure issue.** Most server farms are located in a well planned and secure location but one cannot be too careful to ponder the fact that something could always go wrong. The possibility is always out there to consider.

v. **Big Data is another challenging area for cloud based applications.** Emphasis should be laid on it.
6. CLOUD COMPUTING CONCEPTUAL FRAMEWORK

Figure 4 shows a developed/ simulated proof of concept for cloud convergence. This is used to provide inter-state services to end-users in various locations. From the model, a centralized cloud broker that submits all forms of service requests from anywhere in any state to the cloud headquarters and the service processing center. The presence of a SLA Resource Allocator facilitates externalizations with states outside the defined boundary. The CSREC always examines requests for QoS requirements. Once, validation is signaled, outside the defined boundary. The CSREC always examines requests from anywhere in any state to the cloud headquarters centralized cloud broker that submits to end cloud convergence. This is used to provide inter-state services. From the model, a conceptual Interstate cloud service provisioning model. The benefits of figure 4 inclu

7. CONCLUSION AND FUTURE WORK

In this paper, a classical discussion on cloud based taxonomies is presented while discussing the metrics and the shortcomings. A conceptual Cloud computing platform for secure remote inter-state collaboration is presented. This is geared towards limiting some of the challenges. Generally, Cloud services has created a disruptive day-to-day work lives. Entrepreneurs in various locations can use cloud services to build and run their small businesses and work with people from different parts of the states/globe. This is effective, efficient and affordable. From the findings of Forbes Insights [25], the capacity to collaborate across diverse boundaries, time zones or even beyond organizational borders is a critical determinant of success. This work opines that location based collaboration based on cloud technology will bring about most diverse, efficient and distributed teams together, thus bringing an end of faceless employment, improved service delivery and reduce development times. With cloud collaboration, on-site and off-site services can be achieved on time. The use of Bring Your Own Device (BYOD) and remote inter-state work-sharing will further set up a disruptive transactional engagement. Much small business (e.g., startups and their teams) will immensely benefit from this computing model.

8. REFERENCES


