International Journal of Research in Advent Technology, Vol.5, No.5, May 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

Principles and Paradigms of Storage-Cloud

Aniruddha S Rumale[1], Dr. Dinesh N Chaudhari
Assistant Professor, Computer Engg Department SVPM's COE, Malegaon Bk, Baramati[1],
Professor, Computer Engineering Department, JDIET, Yavatmal,[2]
Email: arumale@gamil.com[1] ,dnchaudhari2007@rediffmail.com[2]

Abstract- Today more and more population is becoming online. Everyone is trying to use cloud-storage or storage-cloud for storing their data. Storing data in cloud is risky, as one's data may get stolen or abused by untrusted third parties. An user need to knew about cloud computing and storage-cloud with its benefits as well as risks, which will promote better utilization of cloud. Cloud Service Provider(CSP) also need to look into the several issues that are unavoidable in cloud computing, to implement a better cloud environment.

This paper discusses various principles and paradigms of cloud computing, particularly storage-cloud. The paper explains the concept of cloud computing, its various delivery and deployment models, and generic architectures of cloud computing. Cloud computing is basically an advanced distributed computing system. There are several transparencies issues related with it, which are discussed in brief with their importance in cloud computing. failure to maintain any of the transparencies can cause a reasonable damage to cloud's effectiveness and implementation. Being business model of technology, cloud also need to keep track of calculation of payment based on PAYG. Users's data on cloud needed to be kept private and secure, so that no illegitimate user can have easy access to it. Cloud itself need to be aware of different attacks, and required to safeguard against those. A cloud infrastructure include many things like building, cooling system, legal sanctions, etc, which are non-technical parts of the system. We explained all these things keeping storage-cloud at center.

Index Terms-Cloud Computing,;Cloud Security; Storage-cloud; cloud storage; cloud transparencies

1. INTRODUCTION

Introduction to cloud computing is necessary to understand the concept of cloud computing. Cloud computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths [1]. Cloud computing heavily depends upon networking. In its simplistic form: It is a client server application, where one(Server) provides the services and other(client) uses it. In cloud computing, server offers 'Something as a Service' to client(s) on per usage basis [2]. So, we can say that, primarily Cloud computing is commercialized client server architecture, where the company with more resources act as service provider or server; and companies and individuals with no or less resources uses these offered services on per usage basis [3].

2. CONCEPT

Cloud Computing is the current advancement in the field of Distributed Computing. It involves high-performance network, Internet, Grid/cluster to form a backbone architecture of the server [4], [5] through which cloud offers its services [6]–[8]. Cloud computing provides the capability to use computing and storage resources on a metered basis and reduces the investments in an organizations computing infrastructure [8], [9]. Cloud Computing can be explained with the concept of using Electricity. When plugging an electric appliance into an outlet, One care neither how electric power is generated, nor how it gets to that outlet. This is possible because electricity is virtualized, i.e. it is readily available from a wall socket that hides power generation stations and a huge distribution grid.

When extended to information technologies, the above concept means delivering useful functions while hiding how their internals work. Cloud Computing itself to be considered fully virtualized [10], must allow computers to be built from distributed components such as processing, storage, data, and software resources.

Cloud Computing in its simplest meaning is an advanced client-Server mechanism with Service Oriented Architecture(SOA) [11], where server provides services to client and client(cloud-user or CU) pay the charges for used services to server(Cloud-service-provider or CSP) [5]. Five main principles of cloud computing are given in table I.

PAYG's types are:

1. Fixed Billing: irrespective of usage a client need to pay fixed amount per month or after specific period.

2. Per second/Minute billing: charges are calculated based upon the session time from login to logout, irrespective of service usage.
3. Per Usage Billing: Charges are calculated only when user uses some service of cloud. Simply login and then logout from cloud without using any service won't account for any charges. This PAYG model is usually associated with some minimal fixed charges, generally called as service continuation charges.

Table *I*: Five main principles of cloud computing

Principle	Explanation
Pooled Resources	Resources like Infrastructures, Platforms, and Services are gathered and made available to any subscribing users.
Virtualization	High utilization of hardware assets or resources as none of them remain ideal because many subscribing users can use them at any given point in time.
Elasticity	Due to Distributed Nature and SOA of Cloud computing; Cloud Computing enables user as well as service providers to add/remove any user/resource to/from the cloud dynamically without affecting its working.
Automation	Build, deploy, configure, provision, and move, all resources without manual intervention.
Metered Billing	Per-usage business model; pay only for what one uses; also called as Pay As You Go(PAYG).

3. MODELS

NIST defines cloud computing [6] as: "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and customers and can be ubiquitously accessed from any connected devices over the internet."

Based on this definition, NIST classifies cloud computing in three types of delivery model and four types of deployment models.

A. Delivery Models

Software as a Service(SaaS): The cloud user uses an application, but does not control the operating system, hardware or network infrastructure on which it's running. Very basic model, Generally known as Service Oriented Architecture(SOA) or SaaS. [11], [12]

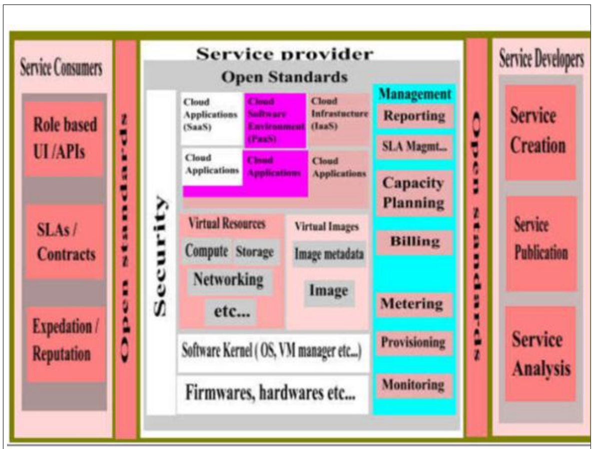

Figure 1: Logical depiction of cloud computing

Platform as a Service (PaaS): The cloud users uses a hosting environment for their applications. They controls the applications that run in the environment and may have some control over the hosting environment, but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework whereupon cloud user can do some operations locally. [13], [14]

Infrastructure as a Service (IaaS): This is the most versatile form of cloud computing and it is really difficult to manage it. Here cloud users uses "fundamental computing resources" such as processing power, storage, networking components or middleware. They can control the operating system, storage, deployed applications and few networking components such as firewalls and load balancers etc. But this creates many problems of security, and so usually the core cloud-infrastructure and mechanisms are kept out of total control of the cloud-users. [5], [15] The logical view of cloud computing with these three basic delivery models is as shown in figure1

B. Deployment Models

Public Cloud: Public cloud services are generally available to cloud-users from a third party service provider via the Internet. They may be free or fairly inexpensive to use. A public cloud does not mean that a users data is publicly visible. It typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions[3],[6].

Private Cloud: Private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. it also provide more control to cloud-users as well as provider as access is designated and always within the restricted network of the particular organization, which is deploying it[3],[6].

Community Cloud: A group of organizations or persons that have shared interests, such as specific security requirements or a common mission generally sets for community cloud. It is just like private cloud except the network used may not be owned by the community[3],[6].

Hybrid Cloud: A combination of private and public cloud; where core and sensitive part of cloud is private while rest is public. Generally used by organizations to outsource their non-business-critical information as public cloud, while business-critical information as private cloud[3],[6].

4. GENERIC ARCHITECTURES

Any of the above cloud computing models may have either of the following generic architectures for cloud.

A. Microkernel Architecture: In this architecture, kernel is implemented using only the minimal set of basic operations or services, to provide scope for designing complex system services on top of it. This adds great flexibility in usage of the system and makes modification and enhancement easy [3]. Again due to basic nature of microkernel, with little modification, it can, in parallel, port more than one operating systems unlike monolithic kernel. This is generally called as“bare metal hypervisor” in cloud computing. This enables CSP to use same hardware in more than one way, i.e. now CSP can provide entirely different operating systems from the same hardware. Adding new resources or services become relatively easy due to micro kernel. A generic architecture of cloud computing based on microkernel model is shown in figure2.

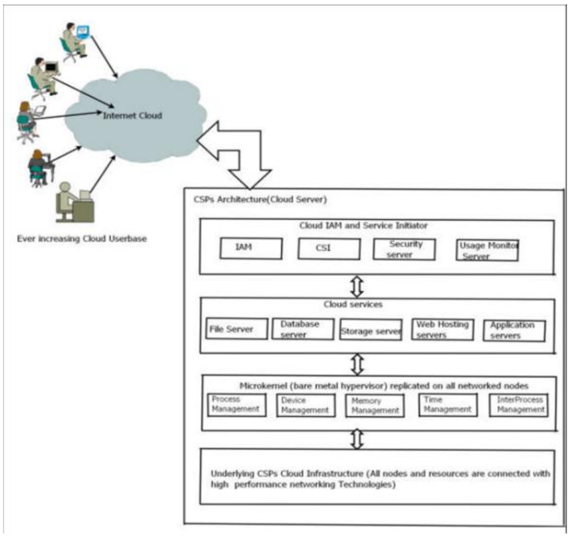
Internet Cloud
Ever increasing Cloud Userbase
CSPs Architecture(Cloud Server)
Cloud IAM and Service Initiator
IAM
CSI
Security server
Usage Monitor Server
Cloud services
File Server
Database server
Storage server
Web Hosting servers
Application servers
Microkernel (bare metal hypervisor) replicated on all networked nodes
Process Management
Device Management
Memory Management
Time Management
InterProcess Management
Underlying CSPs Cloud Infrastructure (All nodes and resources are connected with high performance networking Technologies)

Figure 2: Generic architecture of cloud computingbased on microkernel model

B. Virtualization Architecture: For commercial success of cloud computing it is necessary that CSP's infrastructure must emulate or simulate popular hardware(like intel processor architectures) as well as software(like Unix, Windows operating system). This emulation will help in writing new software for different operating systems or entirely for different hardware. This enables CSP to run all existing software on cloud and offer them as a service to end user[3].

Virtualization allow simultaneous execution of many different heterogeneous systems on cloud. Thus virtualization help in emulating the existing operating systems or required hardware as per the user's need. Virtutalization plays a very important role in cloud computing. Such emulations or simulations are generally termed as virtual machines and are considered as backbone of cloud computing [16], [17].

In Hardware virtualization or platform virtualization, a complete virtual machine is created; that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Linux or other operating system;

and thus respected operating system based software can be run on the virtual machine. A generic view of Cloud computing using virtualization concept is depicted in figure3.

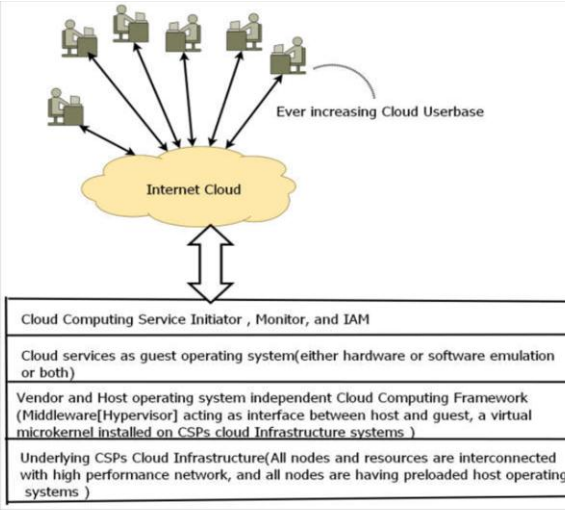
Ever increasing Cloud Userbase
Internet Cloud
Cloud Computing Service Initiator , Monitor, and IAM
Cloud services as guest operating system(either hardware or software emulation or both)
Vendor and Host operating system independent Cloud Computing Framework (Middleware[Hypervisor] acting as interface between host and guest, a virtual microkernel installed on CSPs cloud Infrastructure systems)
Underlying CSPs Cloud Infrastructure(All nodes and resources are interconnected with high performance network, and all nodes are having preloaded host operating systems)

Figure 3: A generic view of Cloud computing usingvirtualization concept

5. ISSUES

Some of the main issues of cloud computing Infrastructure are a) Transparency, b) Flexibility, c) Reliability, d) Scalability, e) Heterogeneity, f) Security, g) Virtualization, and h) Performance. Addressing these issues correctly create a stable and reliable Cloud Computing environment. Cloud computing entirely depends upon Internet and Networking, and so any error in addressing networking issues simply kills cloud computing [3].

As prescribed by ISO(International standard Organization), there are total eight transparencies required to be maintain by any advanced distributed systems like cloud computing. These eight transparencies[2],[3] are:

Access transparency: A cloud computing client environment must provide access policies similar to local access. User in any case must not need to know whether resource or service in use is remote or local.

Location transparency: Location transparency allows end user to access the services and resources provided by cloud provider from anywhere in the world and that from any machine with enough processing power and Internet connectivity. It implements two sub transparencies: a) Name Transparency: It means the name of resource or service must not reveal anything about its physical location; and b) Mobility Transparency: This implies the unique username given to each CU for accessing the services or resources offered by CSP from anywhere.

Replication Transparency: Data redundancy (replication of data), service redundancy (replication of servers), and resources redundancy (hardware replication to handle problems due to hardware failure) must be kept hidden from end user of cloud.

Failure Transparency: Even in case of partial failure at CSP, a cloud must have to provide performance to Cus.

Migration Transparency: The process and data migration done by cloud for delivery of the intended services must be automatic and hidden from the CUs.

Concurrency Transparency: A cloud server usually serves thousands of users at any given time. Concurrency transparency ensures that each user will get an impression of SSI(Single System Image). Thus every user will feel as a sole user of the entire cloud.

Scaling Transparency: The scaling transparency ensures the expansions/reduction in userbase and infrastructure without disrupting activities of system.

Performance Transparency: Goal of this transparency is to provide the desired performance to end user in possibly all manageable circumstances like partial failures, or ongoing reforms at cloud servers.

Flexibility[2] ensures ease of modification and enhancement. It can not be achieved without proper implementation of discussed transparencies. Reliability of cloud depend upon its fault handling capacity. Thus a reliable cloud system require to detect, recover, avoid, and tolerate faults. A CSP infrastructure should have to be scalable to adopt increased service load. In cloud computing, A CSP may need to employ dissimilar or heterogeneous hardware and software to form its infrastructure. For commercial success of cloud computing it is necessary that CSPs infrastructure must emulate or simulate popular hardware as well as software to reduce the cost and to ensure the performance via heterogeneity. This is achieved by virtualization. Virtualization is the next core of cloud computing infrastructure after networking[2],[3].

As Participants of cloud, CSPs and CUs, are generally came from different locations far from each other and relay on the Internet for overall cloud computing experience. Assuring a better performance in cloud is a really a tremendous task to complete. A CSP need to consider all eleventh hour situations in its performance assurance systems with traditional solutions for performance like batching, caching, concurrency, parallelism, congestion management and so on.

Cloud Computing involves a vast data storage and transfer [18]. It also involves high performance networks and heavy communication among users and service-providers. This make every cloud vulnerable to security threats [19]–[22] like illegal login in to the cloud, data theft, and all other existing security challenges like denial of services, sniffing, hacking etc, refer tableII and section V. Many organizations and researchers worldwide are trying to overcome these security problems to make the cloud computing more trusted [23], [24]. A proper security measures for data-storage in cloud [25]–[28] and connectivity (login-logout) with cloud [29], [30] are very necessary for trusted cloud computing.

6. STORAGE-CLOUD

Storage-cloud falls in the category of IaaS and PaaS. Storage infrastructure is offered as a service by CSP to store and retrieve the data. Storage and retrieval of data is the one biggest problem that every organization faces. Any organization will have following types of data like:

Accounts data: This contains vital information of financial status of the organization from its birth onwards. Information about payroll, inventories, debts, loans , taxation details etc, can be used as weapon against the parent organization by her competitors. At the same time loosing such data may creates many problems, in some cases death to the organization. To store such data on dayto-day, month-to-month, year-to-year and so on basis, requires a large storage capacity and a good data security system. Not all organizations are capable to invest the capital require for this; and so they always uses services from trusted third parties [31], [32].

Non-Accounts data: This contains vital information about ongoing projects, patents, marketing strategies deployed, legislative issues, personal information of employees and so on. A breach in this information may cost either to an employee or to an organization a nightmare. Many progressive organizations gives equal or even higher importance to this Non-Accounts data with Accounts data. And to keep such data confidential and secure, much of the data-storage capacity and security-systems capacity is required. Just like in Accounts data case, organizations also uses Trusted third party resources to store and secure such Non-Accounts data. [31]–[33]

Storage Network Industries Association(SNIA)coined “storage as cloud or storage-cloud” concept, keeping in view the needs of data-storage and data-security requirements. This concept is similar to that of DataWareHousing, where we generally access data through Datamart(virtual database) instead of directly accessing it from master database. A storage-cloud can be seen as a grid of many DataWarehouses combined using some indexing mechanism. It handles security of data in terms of storage, by using redundancy principle to store the uploaded data in storage-cloud; and in terms of access, by providing an encryption-decryption and secure access channel mechanism. Hardware of storage-cloud can be a cluster/grid of disks, or independent Storage Area Network(SAN).

7. SECURITY ISSUES IN STORAGE-CLOUD

To be an effective and efficient storage-cloud, the system must provide the proper security to the data. Security issues need to be addressed by a storage or other cloud computing system [6]–[8], [19]–[24] are as listed below:

Security in Cloud: Data or information stored within cloud need to be kept secure. This can be achieved by (a) using data-redundancy principle with encryption, by maintaining more than one encrypted copies of the same data. (b) Using antiviruses, antispammers, honeypots, Firewalls etc, to protect data from corruption. Security in cloud is thus very important to make the cloud trusted.

Security for the Cloud: What, if the cloud itself get attacked? a good compartmentalization and integration of various cloud services is necessary. Cloud itself must be protected from unauthorized use and access. Authentication of users and incoming and outgoing traffic plays very important role in this case.

Security by the Cloud: End user must have to get the secure access and privacy when he uses the cloud. This issue won’t get addressed properly if above two Issues won’t get implemented with utmost care. This require a dedicated IAM or secure channel application for CU.

Apart from the above generalized issues of cloud computing, followings are the few more issues that also need to be addressed properly. a) Integration: Look for integration points with security and identity management technologies you already have, such as Active Directory, and controls for role-based access and entity-level applications. b) Privacy: A cloud service must includes data encryption, effective data anonymization, and mobile location privacy. c) Identity and access: A Cloud must have the means of preventing inadvertent access. d) Compliance: Cloud must have vendor certification and compliance with industry and government standards that affect users agency. e) Service integrity: Cloud must protect software from corruption (malicious or accidental) and always ensure the security of the written code. f) Jurisdiction: The location of a cloud providers operations can affect the privacy laws that apply to the data it hosts. Does users data need to reside within users legal jurisdiction? Governments records management and disposal laws may limit the ability of agencies to store official records in the cloud.

8.COMPONENTS

Clients, Internet, CSP Infrastructure are a major components of the cloud computing. Where CSP infrastructure can be seen as an integration of (i) Services, (ii) Applications, (iii) Platforms, (iv) Storage, (v) Computing Infrastructure, and (vi) Other Infrastructures[2]. In its abstract view a cloud computing can be seen as evolved version of distributed computing system as shown in figure 4.

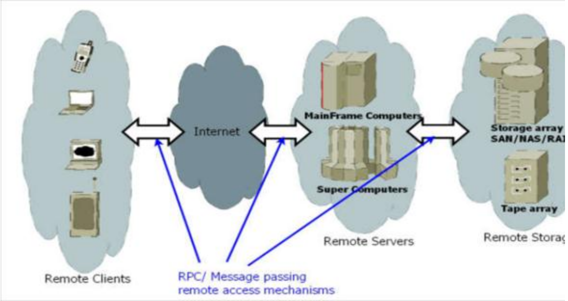

Figure 4: Abstract view of Cloud Computing orDistributedComputing Systems Components

Clients: Cloud computing is a commercialized application of advanced distributed computing system, and so clients plays a very important role in it. A client can be dedicated and an independent program fixed to a single or more machines via machine fingerprinting. It usually utilizes Internet, VPN(Virtual private networking) and SSL(Secure socket layer) with other secure protocols to connect with CSP. A Client can be generic, accessible from anywhere and any platform via Browsers using WEB based interfaces, may or may not be using any secure channel for communication with CSP [3], [34]. There are many issues in designing the client program for Cloud computing; some common issues are discussed below.
I) Technology used for design: Different technologies like, HTML, XML, AJAX, Java, .Net, PHP, SOAP, REST, Mashup, SQL, NoSQL, etc, can be used for designing client and server programs in cloud computing. One need to choose the proper intermix of these technologies to assure maximum performance.
II) User friendly and portable: A heavyweight, difficult to use and manage client program can cause in lost CUs. CSP needs to keep the client program as compact as possible with all necessary features and simple CUI(Commandline User Interface) and GUI(Graphical User Interface).
III) Secure: Client program must have to be secure. This requires cleaning all traces of communication(usually all temporary data or files used in communication) immediately after usage, so that no third party can enter the system using such traces.
IV) Where to execute services: Not all services offered by cloud computing require the high end computing power of CSP; such services can be executed completely at client terminal. But executing services require them to embedded in client, which make client a heavyweight and may be unportable. So client need to cache all such services at CUs terminal for execution whenever called.

Internet: Internet is an interconnect used by cloud computing over which neither CSPs nor CUs have any control. Internet is the backbone of cloud computing. It provides many intelligent and time tested etworking protocols to Cloud computing with all the threats those are possible due to use of it. Few threats using Internet are briefed out in table II. All Internet technologies plays very crucial and important role in cloud computing. Security protocols or measures taken to made Internet more secured are important in assuring secure data transfer among CUs and CSPs. WEP, WPA/WPA2 and other security measures needed to be deployed in access points of Internet, while advanced encryption and decryption schemes need to be applied to data before transmission over Internet.

CSP Infrastructure: CSP infrastructure comprises software and hardware. Software part comprises services, applications, platforms etc, while hardware comprises storage and other Infrastructure like computing hardware, networking, buildings, cooling systems and so on [34]. To provide computational and storage services, CSP infrastructure is formed using a grid/cluster of the computational and storage resources as shown in figure 5. Here the hardware, like processors and storage, forms a stable grid and clusters are dynamically formed on the grid by grid I/O controller or CSP monitor program to provide particular service to the users.

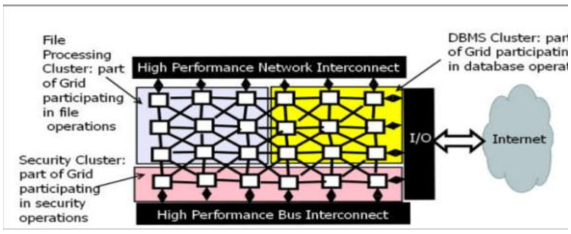
File Processing Cluster: part of Grid participating in file operations
High Performance Network Interconnect
DBMS Cluster: par of Grid participatin in database operat
I/O
Internet
Security Cluster: part of Grid participating in security operations
High Performance Bus Interconnect

Figure 5: A simple block diagram for storage andcomputational grid/cluster for CSP's infrastructure basedon similarity index

Table *II*: Common Security threats of using Internet

Denial of Services	Attackers prevents the normal use of Network by flooding it with garbage communication. This attack is common in ACK(Acknowledgement) based communication.
Man in the middle	Attacker can use the data acquired using eavesdropping to pose himself as legitimate party bypassing the real one or simply read and forward the data to legitimate party. Such read data then can be used for some personal or financial gains.
Masquerading	Attacker can pose as authentic user to gain some privileges unauthentically.
Message modification	Attacker can modify the messages acquired in eaves dropping and then retransmitting them by posing as authenticate user
Message replay	Attacker can retransmit the messages acquired in eavesdropping unnecessarily by posing as authenticate user
Traffic analysis	Attacker can passively monitors network communication for data and user's credentials for identifying traffic pattern to decide his attacking strategies.

1) Services: Cloud is based on a terminology of 'anything as a Service' model. Thus many services can be a part of CSP infrastructure. Such services need to be user specific as well as generic. Properly designed service can only result in better usage of cloud computing. CSP can create a secure IAM(Identification and Access management), and can offer it as a service to CU.

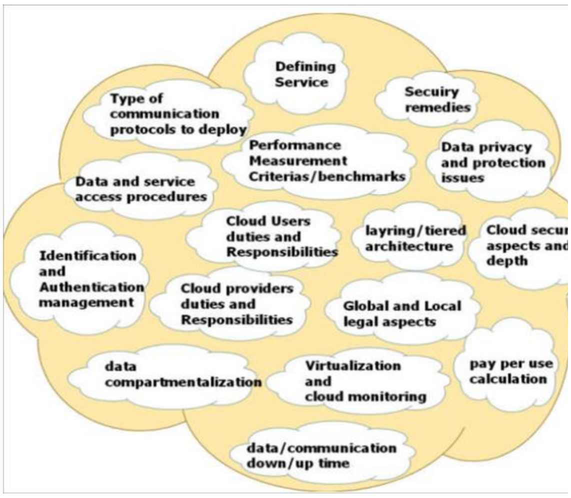
Defining Service
Type of communication protocols to deploy
Secuiry remedies
Performance Measurement Criterias/benchmarks
Data privacy and protection issues
Data and service access procedures
Cloud Users duties and Responsibilities
layring/tiered architecture
Cloud secu aspects and depth
Identification and Authentication management
Cloud providers duties and Responsibilities
Global and Local legal aspects
data compartmentalization
Virtualization and cloud monitoring
pay per use calculation
data/communication down/up time

Figure 6: Common salient points to considerwhile drafting SLA

All the services of cloud computing are offered as per some service level agreements(SLA). SLA is documentation of how to use and deploy the services of cloud computing without breaking the local and global laws. It is generally used as SRS (System/Software Requirement Specification) for Cloud computing, and also as legal contract between CU and CSP. SLA based security is theoretically possible, as in theory CUs play dominant role in it. Practically CSPs plays very dominant role in SLA based architecture of cloud computing due to sheer economic and infrastructural power. Usually a CSP creates different types of SLA based packages(from providing low to high security and from fixed to dynamic PAYG systems). The CU only need to choose the one module of services out of offered SLA based services. So right now CSP-SLA based clouds are only in existence

It is unlikely to have user-SLA based cloud due to (a) complex nature of such cloud, as for each user it plays using different SLA, (b) economically weak condition and non-unity of users to force such user-SLA on CSP, and (c) hesitation of users in going through all legal details required to draft such SLAs. Every CU must need to check for some common salient features of SLA as depicted in figure 6. These are the common points used by CSPs while drafting SLA.

2) Applications: Many applications can be offered as a service by CSP. This Need to proper deployment of Applications to cope with multitenant usage is essential. Applications, like graphic designer, or CRM(Customer Relationship Management) suite, or document creation and management software are the part of CSP infrastructure. Offering applications as a service is well established cloud computing model, generally called as Software as a Service (SaaS).

3) Platforms: The cloud operating system or architecture is itself can be termed as a platform. By this definition we can say that, "Platform can be seen as any operating system or middleware or Integrated Development Environment(IDE) using which or on which a developer can develops and deploy an application(s)." Offering platform as a Service(PaaS) is another basic model of cloud computing.

4) Storage: Datacenter or Storage of CSP has two parts, hardware and software. Hardware consists of utilization of Storage grids or SAN(Storage Area Network), NAS(Network attached Storage), RAID(Redundant Arrays of Inexpensive Disks) etc. Software part of storage includes (i) Cloud File system, which manages allocation, deallocation, isolation, replication(implementation of RAID principle at software level) and many such storage and memory utilization policies; (ii) Utilization of databases, SQL or NOSQL or combo architecture; (iii) maintaining various operations done on data. CSP can offer its efficient storage system as a service, this falls in Infrastructure as a service(IaaS) model of cloud computing.

5) Computing Infrastructure: Without Computing infrastructure, no cloud exist. Software part of this is the distributed operating system or cloud operating system which controls all computing power. CSP generally uses supercomputers, Grids, Clusters, MPP(Massively Parallel Processors) etc, to create the high end computing power required to act as CSP. Using a single machine you can imitate the cloud, but full functionality of cloud is simply out of reach without high end computing power. This Computational power then can be offered as service to the CU using IaaS model of cloud computing.

6) Other Infrastructures: Many other infrastructural implementations plays very important role in cloud computing infrastructure development. Not all of it can be offered as a service, but all are essential for a successful cloud operations. Though these infrastructures won't play any direct role in digital way of cloud computing, not mentioning them is total injustice with these requirements. These other infrastructures can't be the part of 'as a service' model of cloud computing, but are very essential and must for cloud computing.

a) Building An earthquake resistible building(s) with proper provision for ventilation, fire hazards, cooling systems etc, to keep all the hardware and thus software involved in CSP infrastructure safe. The buildings should and must provide a dust free environment, as the dust deposited on electrical and electronic equipments and other infrastructure can cause a problem to cloud operations in more than one way.

b) Uninterrupted power supply(UPS) UPS plays very core role; you know without electricity nothing works. An UPS for 24×7 from External source like Government or electrical company is must. In case such service is not available from outside, CSP need to implement one for its own utilization. Without provision for UPS, a cloud system may face many problems, even total collapse of operation is possible.

c) Heat dissipation system Trillions of users access Internet daily. While operating on their data and using cloud services, tremendous heat get generated at CSP's Datacenters and computing-ends. Without proper heat dissipation system this heat can simply burn out the entire cloud into ashes. This makes such system an essential part of the CSP infrastructure.

9.EXISTING SYSTEMS

From the Introduction of cloud computing one can say that, 'it is practically impossible to create a complete cloud computing experience using simulation or emulation. It is also difficult to create a real cloud infrastructure using a handful of virtual or real machines, because practically CSP infrastructure requires high performance computational & sharable resources, and storage grids; costing in billion dollars. Other infrastructure requirements like cooling systems, buildings, UPS etc, costs accordingly; and maintenance of the entire storage-cloud costs accordingly. Figure 7 and 8 shows you photographs of some real life storage-cloud infrastructure.

At present Google's storage-cloud shown in figure 7, has 777,000 cores, assuming the entire Compute Engine cluster consists of 8-core CPUs, equates to 96,250 computers. As per the Internet search Microsoft's storage-cloud or datacenter in Dublin, refer figure 8b has around 1 million servers with power consumption of two terawatt-hours (TWh) per year.

(a) Inside view (b) A closer look (c) A Google's server room in Council Bluffs, Iowa. Photo:Connie Zhou

Figure 7: Google's storage-cloud real photographs obtained from Internet Search

(a) Inside view (b) In Dublin, Ireland(Cranes size will depict its massiveness) (c) In San Antonio, Texas (The size of the cars will depict its massiveness)

Figure 8: Microsoft's storage-cloud real photographs[35]

That's about the same amount of power used by 177,000 average US homes per year. The initial built-up cost estimated by Microsoft for it was approximately 70 billion US dollars. This shows that designing any real cloud infrastructure is just beyond the capacity of any single researcher. This also undeniably signifies the importance of security of cloud computing. Many IT giants like google, microsoft, IBM are in the business of Cloud computing:IaaS. Other relatively small CSPs, which are now dominating the Cloud are listed in Table III.

SUMMARY & CONCLUSION

The thorough understanding of any subject is very necessary for serious research. It will obviously help in building the prototype of real system, with which the further development of the subject can be carried out by research. By following this philosophy, we tried our best to explain the vastness and complexity of cloud computing with coverage of its some of the many factors.

Paper introduced cloud computing with its basic concept in section 2. A globally accepted NIST definition and classification of cloud computing models are discussed in section 3. Delivery models are based upon, 'what is offered as a Service', by CSP. While Deployment models are based upon, 'how the cloud is accessed and operated by CSPs and CUs'.

Table III: Some existing CSPs

Joyent	**www.joyent.com** is a complete company offering all 3 aspects of cloud, viz, IaaS, Saas, and PaaS. provides public cloud service with Amazon and private cloud services with Dell.
Rackspace	**www.rackspacecloud.com/**cloud hosting products provides Scalable virtualized storage infrastructure. It has more than 90000 clients. One of largest IaaS provider company.
OpenStack	OpenStack is an open source cloud computing plat form project started in the summer of 2010 by IaaS vendor Rackspace and NASA. It's got three core component projects up and running, with two more incubating and another 16 coming from the wider community. Using openstack means, your applications will not ever be locked to a proprietary vendor. Openstack had the backing of 159 companies and more than 2800 people actively contributing to its code base. Further details can be obtained from **www.openstack.com**
GoGrid	Company offers ready to deploy windows and Linux cloud servers with a good SLA provisions. Details are available on **http://www.gogrid.com/**
ElasticHosts	It provides virtual servers based on Linux KVM, running on their own server farms,which are located in three fully independent data centers across two continents.**www.elastichosts.com**
SymetriQ	Offers dedicated virtual servers for IaaS like process ing power, storage, bandwidth, etc. . . Further details are available on **www.symetriq.com**
Amazon Web	Amazon EC2 is standard setter in public IaaS provider with its own

Services	infrastructure. Details can be obtained at **http://aws.amazon.com/**

Cloud computing infrastructure architectures are very complex to define but can be simplified with block diagrams. For better understanding of cloud computing section 4 explained cloud computing's microkernel based and virtualization based. Some core issues like: a) Transparency, b) Flexibility, c) Reliability, d) Scalability, e) Heterogeneity, f) Security, g) virtualization, and h) Performance; of cloud computing are discussed in section 5.

In section 6, We tried to explain the storage-cloud in its brief. Section 7 is the focus of research, and three aspects of security are explained in brief with other security measures in cloud computing. The section 8 with figure 4 is used to explained the entire cloud computing with its major components and subcomponents.

Section 9 is used to show the real life examples of few existing storage-cloud systems to emphasize the fact that no individual researcher can implement a cloud infrastructure in its entirety due to tremendous capital requirement.

REFERENCES

[1] Gautam Shroff, ENTERPRISECLOUDCOMPUTING: Technology, Architecture, Applications. Cambridge University Press, The Edinburgh Building, Cambridge CB2 8RU, UK, 2010. ISBN 978-0-521-76095-9 Hardback, ISBN 978-0-521-13735-5 Paperback.

[2] R. Buyya, J. Broberg, and A. Goscinski, eds., CLOUD COMPUTING : Principles and Paradigms. John Wiley & Sons, Inc., Hoboken, New Jersey, 2011.

[3] A. S. Rumale, Dr. D. N. Chaudhari, and Dr. V. M. Thakare, Cloud Computing: Principles and Paradigms. IASER, first ed., Oct 2015.

[4] ITU-T, "Distributed computing: Utilities, grids & clouds," tech. Rep., International Telecommunication Union : Telecommunication Standardization Policy Division ITU Telecommunication Standardization Sector, 2009. ITU-T Technology Watch Report-2009, pp.1-13.

[5] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing: Infrastructure as a service," International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 23199598, vol. 1, pp. 1–7, February 2013.

[6] W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing. Draft Special Publication 800-144, Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, 2011. pp. 1-60.

[7] V. J. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics. Syngressis, an imprint of Elsevier, 225 Wyman Street, Waltham, MA 02451, USA, 2011.

[8] D. M. I. Williams, "Risks of cloud computing," in A Quick Start Guide to Cloud Computing : Moving your business into the cloud , New Tools for Business, pp. 39–55, Kogan Page Limited, 2010.

[9] S. Fox, D. Follette, G. Raja, and P. Stubbs, "Securing Cloud Solutions Using Claims-Based Authentication," in PROFESSIONAL SharePoint R 2010 Cloud-Based Solutions, pp. 309–335, John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2011-12.

[10] "Cloud Computing Security : Making Virtual Machines Cloud-Ready ." A Trend Micro White Paper May 2010, pp. 1-12.

[11] ASP-Team, Cloud Computing Certification Kit Specialist : Software as a service and Web Applications: The art of Service. The Art of Service Pty Ltd, 2011. pp. 1-219.

[12] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing: Software as a service," 2nd IEEE International Conference on Electrical , Computer and Communication Technologies, 22-24 February,2017, SVS College of Engineering, Coimbtore, Tamilnadu, India, pp. 1–6, 2017. 978-1-5090- 3239-6/17/$31.00 c 2017IEEE.

[13] ASP-Team, Cloud Computing Certification Kit Specialist : platform management and Storage management: The art of Service. The Art of Service Pty Ltd, 2011. pp. 1-204.

[14] A. S. Rumale and D. D. N. Chaudhari, "Cloud computing: Platform as a service," International Journal of Advances in Computing and Communication Technologies (IJACCT), vol. 1, no. 1, pp. 46–49, 2014.

[15] G. Reese, Cloud Application Architectures : Building Infrastructures and Applications in the Cloud. OReilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472 , 2009. pp. 1-206.

[16] Kai Hwang and Geoffrey C. Fox and Jack J. Dongarra, Distributed and Cloud Computing: From Parallel Processing to the Internet of Things. China Machine Press with Elsevier (Singapore) Pte Ltd, 2012. ISBN 978-0-12-385880-1, pp:1-207.

[17] Rajkumar Buyya and Christain Vecchiola and S. Thamarai Selvi, Mastering Cloud Computing: Foundations and Applications Programming. Morgan Kaufmann an imprint of Elsvier, 225 Wyman Street, Waltham, MA 02451, USA, 2013. ISBN: 978-0-12-411454-8, pp:1-560.

[18] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, and J. Molina, "Controlling data in the cloud:outsourcing computation without outsourcing control," CCSW 09, November 13, 2009, Chicago, Illinois, USA. Copyright 2009 ACM 978-1-60558-784-4/09/11, pp. pp. 23–29, 2009.

[19] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in IEEE International Conference on Cloud Computing, pp. 109–116, 2009.

[20] I. Potoczny-Jones, "Cloud security risk agreements for small businesses," tech. rep., Galois, Inc. Portland, OR, 2011.

[21] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui, "A secure cloud backup system with assured deletion and version control," in 3rd International Workshop on Security in Cloud Computing (CloudSec) (in conjunction with ICPP'11), pp. 1–8, 2011. Authors copy.

[22] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Fade: Secure overlay cloud storage with file assured deletion.," in Proceedings of SecureComm 2010, Singapore, pp. 1–18, 2010. Authors copy.

[23] Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," 2nd International Conference on Signal Processing Systems (ICSPS), pp. pp. 1–6, 2010.

[24] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud computing system based on trusted computing platform," International Conference on Intelligent Computation Technology and Automation, IEEE, pp. pp.12–18, 2010.

[25] A. Gordon, "Storage security tutorial with a focus on cloud storage," tech. rep., Storage network industry association, 2011. pp. 21-34.

[26] A. Gordon, "Cloud storage security introduction," tech. rep., Storage network industry association, 2010. pp. 22-28.

[27] SNIA-team, "Managing data storage in public cloud," tech. rep., Storage network industry association, 2009. pp. 53-60.

[28] S. MORROW, "Data security in the cloud," in CLOUD COMPUTING Principles and Paradigms, pp. 573–592, John Wiley & Sons, Inc, 2011.

[29] J. Tseng, "The role of wan optimization in cloud infrastructure," tech. rep., Storage network industry association, 2010. pp. 45-53.

[30] S. Pate and T. Tambay, "Securing the cloud: using encryption and key management to solve today's cloud security challenges," tech. Rep., Storage network industry association, 2011. pp. 34-45.

[31] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," in IEEE INTERNET COMPUTING : Trust & Reputation Management, pp. 14–22, Oct. 2010.

[32] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," in HPL2011 & IEEE ICFP(IEEE Cloud Forum for Practitioners) 2011, pp. 1–8, July 2011. A Cloud & Security Lab paper.

[33] Y. CHEN, W.-S. KU, J. FENG, P. LIU, and Z. SU, "Secure distributed data storage in cloud computing," in CLOUD COMPUTING Principles and Paradigms, pp. 222–248, John Wiley & Sons, Inc, 2011.

[34] C. Wu and R. Buyya, Cloud Data Centers and Cost Modeling: A Complete Guide To Planning, Designing and Building a Cloud Data Center. Morgan Kaufmann (an imprint of Elsevier), 225 Wyman Street, Waltham, MA 02451, USA, 2015. ISBN: 978-0-12-801413-4, pp: 1-817.

[35] Sebastian Anthony, "Microsoft now has one million servers less than Google, but more than Amazon, says Ballmer," 19 July 2013.

Aniruddha S. Rumale , received his BE in Computer science & engineering in 1998 from Amravati University, and ME in CSE in 2008 from Pune University. He also completed his MBA in HR from YCMOU, Nashik in 2012. At present he is pursuing his Ph.D. From Amravati University under the guidance of Dr. D. N. Chaudhari. He is working with Shivnagar Vidya Prasarak Mandal's College of Engineering, since 2000, and has 14+ years of teaching experience with more than 40 papers authored in various National / International conferences & journals . His primary research interest is Cloud Computing.

Dr. Dinesh N Chaudhari ,is working as Professor and Dean in computer engineering department of Jawaharlal Darda Institute of Engineering & Technology, YAVATMAL. He is recognized Ph.D. guide at Amravati University and has more than 20 years of academic experience. His interests are in cloud computing, computer networking and security; and he has written many papers in national/international conferences and journals.