ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 10, October 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Survey on Cloud Computing and its Security

M. Nirmala[1]
Assistant Professor, IT dept
Kits,Singapur,Huzurabad
Karimnagar – India

R. Bharathi[2]
Assistant Professor, IT dept
Kits,Singapur,Huzurabad
Karimnagar – India

M. Srujana[3]
Assistant Professor, CSE dept
Kits,Singapur,Huzurabad
Karimnagar – India

Abstract: Cloud computing is a new paradigm in which computing resources such as processing, memory and storage are not physically present at users location. Instead, a service provider owns and manages these resources, and user accesses them via internet. For example Amazon Web Services (AWS) lets user's stores personal data via its Simple Storage Service (S3) and perform computations on stored data using Elastic Complete Cloud (EC2). Today's most of the business organizations and educational institutions use cloud environment. Cloud computing providers have setup several data centers at different

geographical locations over the Internet in order to optimally serve needs of their customers around the world.

This paper introduces internet-based cloud computing, exploring the characteristics, service models, deployment models , cloud storage ,cloud security as well as the benefits and challenges associated with cloud computing.

Keywords: Cloud computing, Service models, NIST, Elastic Complete Cloud (EC2) , Deployment models, Cloud storage and Cloud security.

I. Introduction

Cloud computing is a type of Internet -based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility over an electricity network.

II. Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Examples of cloud services are online file storage, social networking sites and webmail. By using Cloud computing users can use data and services from around the world in a pay-as-you-go model.

Since the Cloud is a broad collection of services, organizations can choose where, when, and how they use Cloud Computing. Cloud computing services are mainly classified into three main categories. Commonly referred to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

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.

Broad 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).

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.

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 unlimited and can be appropriated in any quantity at any time.

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.

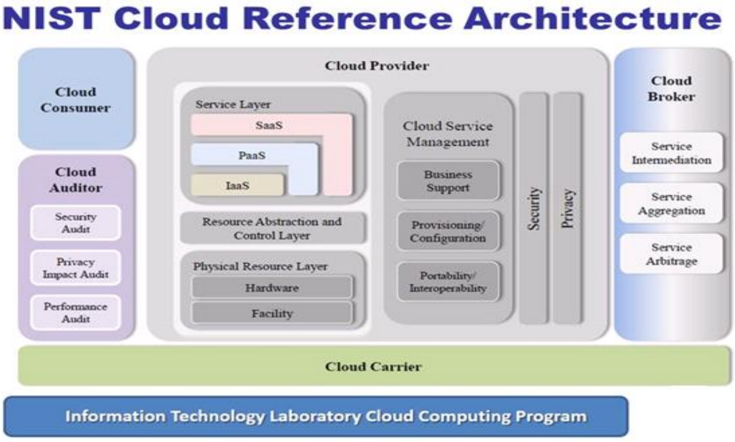


Fig 1: NIST Cloud Reference Architecture

Figure 1 presents an overview of the NIST cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing. The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing. Figure 1: The Conceptual Reference Model As shown in Figure 1, the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing.

Cloud Consumer: A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.

Cloud Provider: A person, organization, or entity responsible for making a service available to interested parties. Cloud Auditor A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

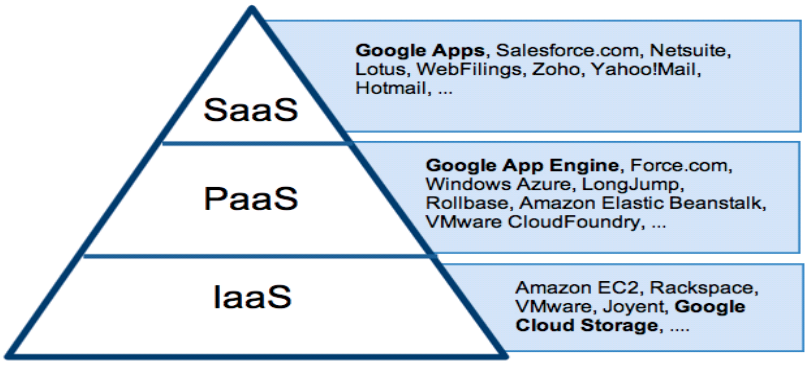
Cloud Broker: An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud Carrier: An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Elastic Compute Cloud: As the name implies EC2 rents cloud of computers to the users with flexibility of choosing the configuration of the virtual machine like RAM size, local disk size, processor speeds etc. Machines that deliver EC2 services are actually virtual machines running on top of XEN platform. Users can store a disk image inside S3 and create a virtual machine in EC2 using tools provided by Amazon. This virtual machine can be easily instantiated using a java program and can also be monitored. As EC2 is based on XEN it supports any linux distribution as well as other OSs. Amazon does not promise about reliability of the EC2 computers. Any machine can crash at any moment and they are not backed up. Although these machine generally don't crash according to the experience of the users but it is safe to use S3 to store information which is more reliable and replicated service. EC2 security model is similar to that of S3. The only difference is that the commands are signed with an X 509 private key. But this key is downloaded from AWS account so the security depends fundamentally on the AWS username and password.

2.1 The Cloud Computing Stack

Cloud Computing is often described as a stack, as a response to the broad range of services built on top of one another under the moniker "Cloud". The generally accepted definition of Cloud Computing comes from the National Institute of Standards and Technology (NIST).Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.NIST also offers up several characteristics that it sees as essential for a service to be considered "Cloud"


SaaS
Google Apps, Salesforce.com, Netsuite, Lotus, WebFilings, Zoho, Yahoo!Mail, Hotmail, ...
PaaS
Google App Engine, Force.com, Windows Azure, LongJump, Rollbase, Amazon Elastic Beanstalk, VMware CloudFoundry, ...
IaaS
Amazon EC2, Rackspace, VMware, Joyent, **Google Cloud Storage**, ...

Source: Gartner AADI Summit Dec 2009

Fig 2: Service Models of Cloud Computing

SaaS applications are designed for end-users, delivered over the web. PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient. IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems

2.1 IaaS

It stands for Infrastructure as a service. Infrastructure as a Service (IaaS) is the delivery of hardware and associated software as a service.. it can be purchased with either a contract or on a pay-as-you-go ba-sis.

2.2 PaaS

It stands for Platform as a service. Pass facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure. it provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely**.**

2.3 SaaS

It stands for software as a service. It is currently the most popular type of cloud computing service. It provides high flexibility and scalability, high performance better availability, and less mainte-nance.

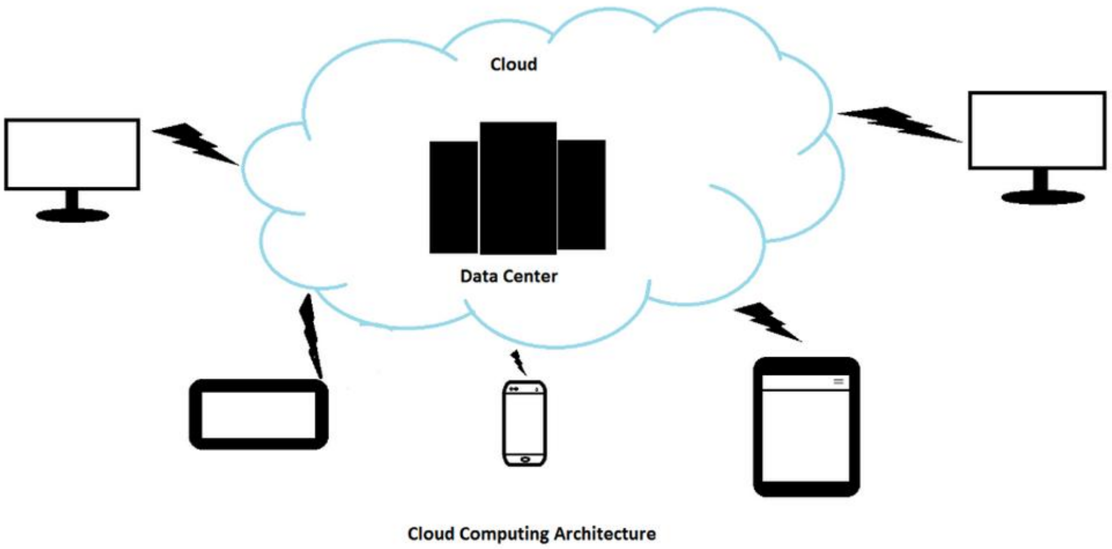


Fig 3:Cloud Computing Architecture

2.4 Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (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).

The benefits of private clouds:

Higher security and privacy: public clouds services can implement a certain level of security but private clouds - using techniques such as distinct pools of resources with access restricted to connections made from behind one organization’s firewall, dedicated leased lines and/or on-site internal hosting - can ensure that operations are kept out of the reach of prying eyes

- **More control**: a private cloud is only accessible by a single organization, that organization will have the ability to configure and manage it inline with their needs to achieve a tailored network solution.

- **Cost and energy efficiency**: implementing a private cloud model can improve the allocation of resources within an organization by ensuring that the availability of resources to individual departments/business functions can directly and flexibly respond to their demand.
- **Improved reliability**: even where resources (servers, networks etc.) are hosted internally, the creation of virtualized operating environments means that the network is more resilient to individual failures across the physical infrastructure.
- **Cloud bursting**;:some providers may offer the opportunity to employ cloud bursting, within a private cloud offering, in the event of spikes in demand. This service allows the provider to switch certain non-sensitive functions to a public cloud to free up more space in the private cloud for the sensitive functions that require it. Private clouds can even be integrated with public cloud services to form hybrid clouds where non-sensitive functions are always allocated to the public cloud to maximize the efficiencies on offer.

Drawbacks:

- Larger upfront costs
- Maintenance costs - IT
- Scalability

Community Cloud: The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.

Public Cloud: The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

The main benefits of using a public cloud service are:

- Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
- Scalability to meet needs.
- No wasted resources

Drawbacks:

- Not as flexible
- Can be expensive wit heavy usage
- “less” secure

Hybrid Cloud— The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, & also the need to offer services the cloud.

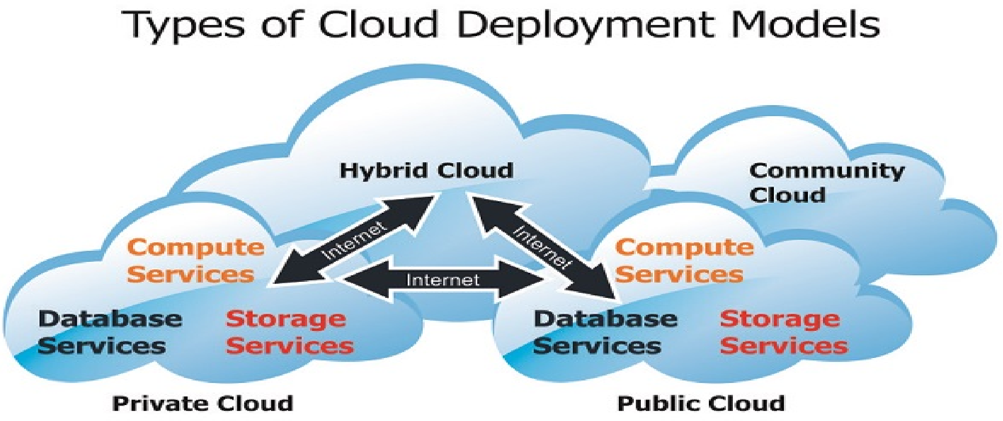


Figure 4: Public, Private, and Hybrid Cloud Deployment Example

2.5 Characterstics:

Cloud computing exhibits the following key characteristics:

- **Agility** for organizations may be improved, as cloud computing may increase users' flexibility with re-provisioning, adding, or expanding technological infrastructure resources.
- **Cost** reductions are claimed by cloud providers. A public-cloud delivery model converts capital expenditures(e.g., buying servers) to operational expenditure. This purportedly lowers barriers to entry , as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is "fine-grained", with usage-based billing options. As well, less in-house IT skills are required for implementation of projects that use cloud computing
- **Device and location independence**: enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from anywhere.
- **Maintenance**: cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places (e.g., different work locations, while travelling, etc.).
- **Multitenancy**: enables sharing of resources and costs across a large pool of users thus allowing for:
  - **centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  - **peak-load capacity** increases (users need not engineer and pay for the resources and equipment to meet their highest possible load-levels)
  - **utilization and efficiency** improvements for systems that are often only 10–20% utilized.
- **Performance**: is monitored by IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web. Services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer
- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery

- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads. This gives the ability to scale up when the usage need increases or down if resources are not being used.
- **Security** can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels . Security is often as good as or better than other traditional systems, in part because service providers are able to devote resources to solving security issues that many customers cannot afford to tackle or which they lack the technical skills to address. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems 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.

III. CLOUD COMPUTING BENEFITS

- Faster implementation and time to value
- Anywhere access to applications and content
- Rapid scalability to meet demand
- Higher utilization of infrastructure investments
- Lower infrastructure, energy, and facility costs
- Greater IT staff productivity and across organization
- Enhanced security and protection of information assets

Advantages of cloud computing:

1) Lower-Cost Computers for Users

2) Improved Performance

3) Lower IT Infrastructure Costs

4) Fewer Maintenance Issues

5) Lower Software Costs

6) Instant Software Updates

7) Increased Computing Power

8) Unlimited Storage Capacity

9) Increased Data Safety

10) Improved Compatibility Between Operating Systems

11) Improved Document Format Compatibility

12) Easier Group Collaboration

13) Universal Access to Documents

14) Latest Version Availability

Disadvantage of cloud computing:

1) Requires a Constant Internet Connection

2) Doesn’t Work Well with Low-Speed Connections

3) Can Be Slow

4) Features Might Be Limited

5) Stored Data Might Not Be Secure

Cloud storage:

In public:

- Store and Forget'
- 'Infinite' size
- Access via Web Browser

In Private:

- Faster access
- Easier access
- Access via Network Places

We can access the cloud using

Cloud Storage: Web Browser/Windows Explorer

- Web Interface
- A folder in Network Places

Cloud Applications: Web BrowserWeb Interface

Cloud Computing: Remote DesktopBest with newer Windows versions (e.g. Win7/Server 2008 R2)

Cloud Storage:

Cloud storage is a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). Users generally pay for their cloud data storage on a per-consumption, monthly rate. Although the per-gigabyte cost has been radically driven down, cloud storage providers have added operating expenses that can make the technology more expensive than users bargained for. Cloud security continues to be a concern among users. Providers have tried to deal with those fears by building security capabilities, such as encryption and authentication, into their services.

2.6 Service Security:

Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer’s identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system or provide an identity management solution of their own.CloudID, for instance, provides a privacy-preserving cloud-based and cross-enterprise biometric identification solutions for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, Para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

2.6 DATA SECURITY:

There are a number of security threats associated with cloud data services, not only covering traditional security threats, e.g., network eavesdropping, illegal invasion, and denial of service attacks, but also including specific cloud computing threats, e.g., side channel attacks, virtualization vulnerabilities, and abuse of cloud services. To throttle the threats the following security requirements are to be met in a cloud data service.

Data Confidentiality

Data confidentiality is the property that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

Data Access Controllability

Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to cloud. Legal users can be authorized by the owner to access the data, while others can not access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

Data Integrity

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

Cloud computing security challenges:

i)DataProtection: Securing your data both at rest and in transit

ii)User Authentication: Limiting access to data and monitoring who accesses the data

iii)Disaster and Data Breach: Contingency Planning

IV. Cloud Computing Provoders

A. Microsoft Live@edu for education

Microsoft Live@edu is intended for educational needs. It provides a set of hosted collaboration services for the educations institutions. The hosted service includes collaboration services, communication tools, mobile, desktop, and web-based applications. It has the feature of data storage capabilities. Office Live Workspace, Windows Live SkyDrive, Windows Live Spaces, Microsoft Shared View Beta, Microsoft Outlook Live, Windows Live Messenger and Windows Live Alerts are the part of Live@edu suite. By means of free registration process universities, colleges and schools can enroll in the program. Microsoft Live@edu is mainly for the institutions for enabling facilities for their academic activities.

B. Google Apps for Education

Google Apps is a collection of web-based programs and file storage that run in a web browser, without requiring users to buy or install software. Users can simply log in to the service to access their files and the tools to manipulate them. The communication tools of Google Apps are Gmail, Google Talk, and Google Calendar and the productivity tools are Google Docs: text files, spreadsheets, and presentations, iGoogle and Google Sites to develop web pages. The tools are free, or users can pay for a Premium Edition that adds more storage space and other features. An Education Edition includes most of the extras in the Premium Edition and is offered at no cost to K–12 (designation for the sum of primary and secondary education and higher education). Google Apps allows institutions to use their own domain name with the service and to customize the interface to reflect the branding of that institution. In this way, a college or university can offer the functionality of Google Apps in a package.

C. Amazon Web Services for Education (AWS):

Amazon Web Services provides the cloud services in categories of Compute, Software, Content Delivery, Database, Storage, Deployment & Management, Application Services and Workforce. Compute service includes Amazon Elastic Computer Cloud (EC2), Amazon Elastic Map Reduce, Auto Scaling and Elastic Load Balancing. Amazon Elastic Compute Cloud delivers scalable, pay-as-you-go compute capacity in the cloud. Amazon Elastic MapReduce is a web service that enables businesses, research hers, data analysts, and developers to easily and cost-effectively process vast amounts of data. Auto Scaling allows user to automatically scale your Amazon EC2 capacity up or down according to conditions. Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. In Software, AWS Marketplace is an online store that helps customers find, buy, and immediately start using software that runs on the AWS cloud. It includes software from trusted vendors like SAP, Zend, Microsoft, IBM, Canonical, as well as many widely used open source offerings including Word press, Drupal, and MediaWiki.In Content Delivery, Amazon CloudFront is a web service that makes it easy to distribute content with low latency via a global network of edge locations.

V. Conclusion

This paper introduces the definition of could computing and its main service offered in IT and other fields, summarizes the characteristics, and focused on the key technologies such as the data storage, data management and programming model. The ultimate goal of cloud computing is to provide calculation, services and applications as a public facility for the public, So that people can use the computer resources just like using water, electricity, gas and telephone. Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. The success of the cloud computing model depends hugely on the ability of cloud providers to keep promises made to users.

ACKNOWLEDGEMENT

We are grateful to all the anonymous referees for their useful suggestions and we would also like to thank the State education department for their outstanding support towards the digital technology.

References

1. M. Haynie, "Enterprise cloud services from Cloud Computing," Micro Focus, Tech. Rep., 2009
2. Amazon, "Amazon Elastic Compute Cloud (EC2)," AmazonWeb Services LLC, Tech. Rep., 2009. [Online]. Available:http://aws.amazon.com/ec2/
3. Google, "Google App Engine: Run your web apps on Google's infrastructure." Google, Tech. Rep., 2009. [Online]. Available:http://code.google.com/appengine/
4. NIST Definition of Cloud Computing v15,csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
5. P. Mell and T. Grance. NIST definition of cloud computing.National Institute of Standards and Technology. October 7,2009.
6. P. Mell and T. Grance. Effectively and securely using the cloud computing paradigm. National Institute of Standardsand Technology. October 7, 2009.
7. G. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. vol. 4607, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.
8. M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.
9. Security guidance for critical areas of focus in cloud computing. http://www.cloudsecurityalliance.org/csaguide.pdf
10. Google app engine. http://code.google.com/appengine/

AUTHOR(S) PROFILE

M. Nirmala, received B.Tech (CSIT) and M.Tech (CSE) from NIT(WGL), India. Now she is working as an Asst.prof in Kamala Institute of Technology & science. Her research area includes the Cloud Computing and Networking.

R. Bharathi, received B.Tech (CSIT) and M.Tech (CSE) from JNTUH, India. Now she is working as an Asst.prof in Kamala Institute of Technology & science. Her research area includes the Cloud Computing, MANETS and Networking.

M. Srujana, received B.Tech (CSE) and M.Tech (CSE) from JNTUH, India. Now she is working as an Asst.prof in Kamala Institute of Technology & science. Her research area includes the Cloud Computing and Networking.