Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.280 – 290

RESEARCH ARTICLE

Comparative Study on Cloud Computing (CC) and Mobile Cloud Computing (MCC)

Niranjanamurthy M[1], Charan Raj U[2], Raghavendra E[3], Sowmya R[4], Suhas Jadhav J[5]

[1]Assistant Professor, Department of MCA, MSRIT, Bangalore-54, INDIA

[2]Student, Department of MCA, MSRIT, Bangalore-54, INDIA

[3]Student, Department of MCA, MSRIT, Bangalore-54, INDIA

[4]Student, Department of MCA, MSRIT, Bangalore-54, INDIA

[5]Student, Department of MCA, MSRIT, Bangalore-54, INDIA

[1] niruhsd@gmail.com; [2] udaycharanraj18@gmail.com; [3] princeraghavendra555@gmail.com; [4] sowmya.10nov@gmail.com; [5] aerosuhas412@gmail.com

Abstract -- Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirement. Normally cloud computing services are delivered by a third party provider who owns the infrastructure. The advantages to mention but some of them include resilience, scalability, efficiency, flexibility and outsourcing non-core activities. Cloud computing offers an innovative method for business model for organizations to adopt IT services without upfront investments. Despite the potential gains which are achieved from the cloud computing, the organizations around are too slow in accepting or adjusting to it because of the security issues and challenges associated with it. Security is one of the crucial issues which hamper the growth of cloud. The idea of providing/handing important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. Mobile Cloud Computing (MCC) is the combination of mobile computing, wireless networks and cloud computing to bring rich computational resources to network operators, mobile users and even cloud computing providers. In this paper we discussed Cloud Computing, Mobile Cloud Computing, Security Risks and Solution of Cloud Computing, Research Issues in MCC, Security Issues and Solutions in MCC, Advantages of MCC.

Keywords: Cloud Computing, Security Risks, Mobile Cloud Computing and Solution of Cloud Computing, Research Issues in MCC, Security Issues and Solutions in MCC, Advantages of MCC

I. INTRODUCTION

Cloud computing is internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and the online access to computer services or resources. Clouds can be classified/organised as private/hybrid and public.

Mobile cloud computing (MCC) at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device.

The real or a major value of cloud computing is that it makes your library related software and data available transparently and everywhere including in latest available smart phone devices.

We are all aware, country like India faced problems like digital divide and off course very low internet bandwidth. So, usage of new technology can be reached to limited or only to some area of educational area.

Mobile cloud applications transfers or move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client.

Reason of Mobile Cloud Computing:

- Mobile devices face many resource challenges (storage, battery life, bandwidth etc.)
- Cloud computing provides advantages to user's by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on-demand fashion.
- Mobile cloud computing provides mobile users with data storage and processing services in clouds, which makes us necessary the need to have a powerful device
- configuration (e.g. CPU speed, memory capacity and so on), as all resource intensive computing can be done in the cloud.

In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as technology grows more and more information on individuals and companies are placed in the cloud, worries or concerns are beginning to grow about just how safe an environment it is now. Despite of all the hype which is surrounding the cloud, customers are still unwilling to deploy their business in the cloud. Security/threat issues which is common in the cloud computing has played a major role in slowing down its acceptance, in fact the security is ranked first as the greatest challenging issue of cloud computing as depicted in figure 1

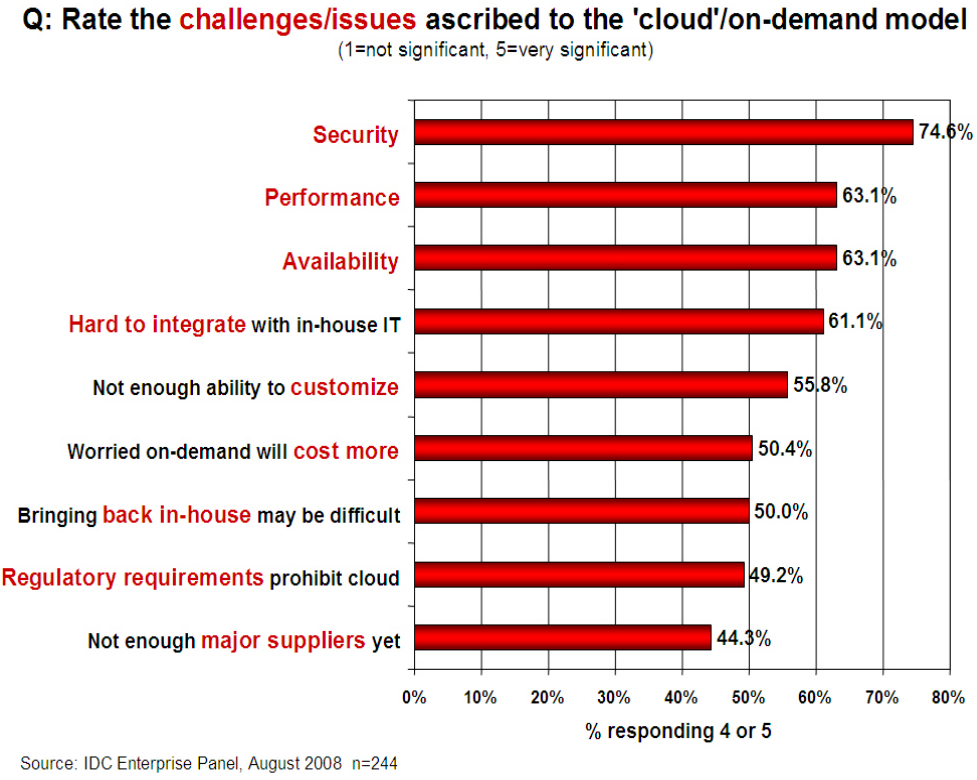

Fig. 1. Challenges and issues in Cloud Computing

Mobile cloud computing (MCC) is a technique or a model, in which mobile applications are built, powered and hosted using cloud computing technology.

A Mobile cloud approach enables developers to build applications designed specifically for mobile users without being bound by the mobile operating system and the computing or memory capacity of a Smartphone. Mobile cloud computing are generally accessed via a mobile browser from a remote web server, normally without the need of installing a client application on the user/recipient phone.

Cloud Storage Comparison

Storage Service Comparison on a Annual Basis			
Service Provider	Free	First Payment tier	Second Payment tier
Amazon	5GB	20GB ($10)	50GB ($25)
Apple iCloud	5GB	25GB ($40)	50GB ($100)
Box	5GB	25GB ($120)	50GB ($240)
Dropbox	2GB	100GB ($100)	200GB ($200)
Google Drive	5GB	25GB ($30)	100GB ($60)
Microsoft SkyDrive	7GB	27GB ($10)	57GB ($25)
Mega	50GB	400GB ($120)	2TB ($240)

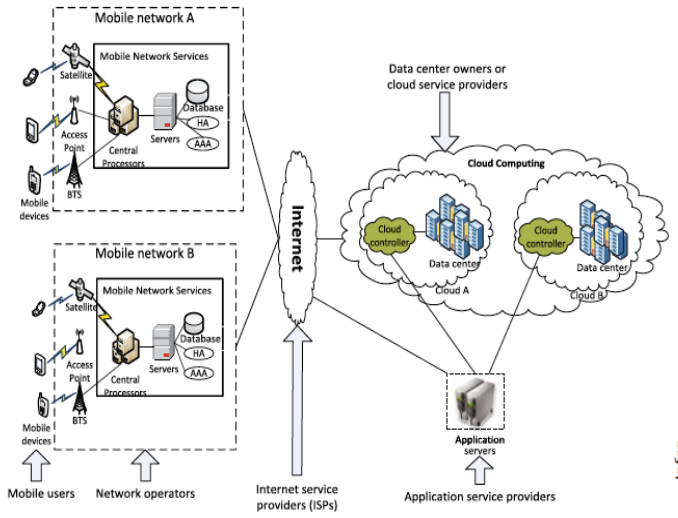

Figure1.1: MCC Architecture

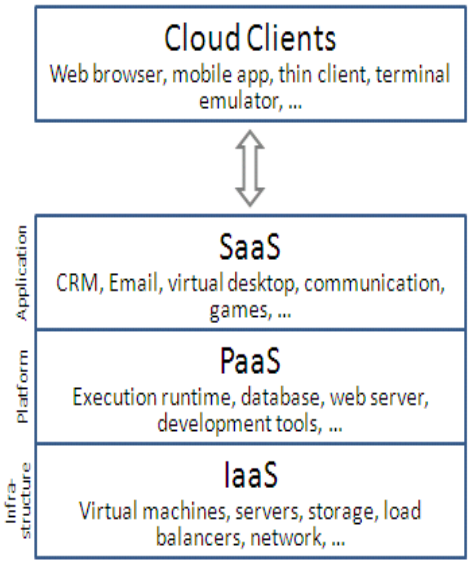

Figure1.2: CC fundamental models

II. AIM OF THE STUDY

- To know what is Cloud computing Mobile Cloud Computing
- To know the types of cloud computing
- To understand the security threats of cloud computing and Mobile Cloud Computing
- Understand the Solution of Security threats, risks in CC and MCC

III. RELATED WORK

Software development organizations contain design and quality, marketing, assurance team, project management, development. It is significant for the various teams inside the

organization to understand the benefits and limitation of incorporating various usability testing methods within the software development life cycle. Few reasons for poor usability include effort prioritization conflicts from development and design team and project management. Some aspects of the usability engineer is to get involved as the heuristic evaluator

A. Cloud Deployments Models:

In the cloud deployment model, platform, storage, networking and software infrastructure are provided as services that scale up or down depending on the requirement. The three main deployment models in Cloud Computing model are:

Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up inside an organization's private data centre. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for [2] cloud users to use and share. It varies from the public cloud in that all the cloud resources and applications are managed by the organization alone, identical to Intranet functionality. Usage on the private cloud can be much more secure than that of the public cloud because of its specified internal disclosure. Only the organization and nominated stakeholders may have access to operate on a specific Private cloud [2].

Public cloud

Public cloud describes cloud computing in general, through which resources are dynamically provisioned on a self-service basis over the Internet, a fine grained via web applications/web services, by an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is customarily based on a pay-per-use model, identical to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud upsurge. Public clouds are not much secure or less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks [2].

Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, provisioned as a single unit, centrally managed, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides higher security control of the data and applications and allows various parties to access information over the Internet. Hybrid cloud also has an open architecture that allows interfaces with other management systems. It can define configuration combining a regional device, such as a Plug computer with cloud services [3].

B. Cloud Computing Service Delivery Models

Following on the cloud formation models, the next security attention relates to the various cloud computing service delivery models[3]. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Infrastructure as a Service (IaaS)
Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as networking devices, processing power and servers. They also allow changing degrees of financial and functional flexibility not found with collocation services or in internal data centers, because computing resources can be added or released much more quickly and cost-effectively than in an internal data centre or with a collocation service.

Platform as a service (PaaS)
Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on beneath the service. PaaS offers developers a service that provides a complete software development life cycle management, from the planning to the design to building applications to deployment to testing and to maintenance [3].

Software as a Service(SaaS)
Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, mostly through the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches have become popular. It is also usually associated with a pay-as-you-go subscription licensing model. Meantime, internet service has become increasingly available to support user access from more areas around the world. It is most usually implemented to cater business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, inwardly operated software without the associated complexity of high initial cost installation, management, support, licensing. The architecture of SaaS-based applications is specifically designed to support many concurrent users at once. SaaS applications are accessed using web browsers over the Internet therefore web browser security is very important. Information security officers will need to examine various methods of securing SaaS applications. WebServices (WS) security, Secure Socket Layer (SSL) , Extensible Markup Language (XML) encryption and available options which are used in enforcing data protection transmitted over the Internet.

C. Security Issues with Cloud models

1.Software-as-a-service (SaaS) security issues:

SaaS provides application services on demand such as conferencing software, business applications such as ERP, CRM, and SCM and email [30]. SaaS users have less control over security among the three fundamental delivery models in the cloud [4]. The adoption of SaaS applications may raise some security concerns as listed below.

Application security
These applications are typically delivered via the Internet through a Web browser. However, bugs in web applications may create vulnerabilities for the SaaS applications. Attackers have

been using the web to compromise user's computers and perform malicious activities such as steal crucial data. Security challenges in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary [4].

Accessibility

Accessing applications over the internet via web browser makes access from any network device easier, including mobile devices and public computers. Nonetheless, it also exposes the service to additional security risks. The Cloud Security Alliance has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (Wi-Fi), vulnerabilities found in the device OS and official applications, proximity-based hacking and insecure market places [4].

2. Platform-as-a-service (PaaS) security issues:

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. As with SaaSand IaaS, PaaS depends on a secure and reliable network and secure web browser [4]. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications [5]. Same as SaaS, PaaS also brings data security issues and other challenges that are described as follows:

Third-party relationships

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups. Mashups combine more than one source element into a single unit. Henceforth, PaaS models also inherit security issues related to mashups such as data and network security [5]. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services.

Development Life Cycle

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security. Developers have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development processes are flexible enough to keep up with changes. However, developers also have to understand that any changes in PaaS components can compromise the security of their applications. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriate locations.

3. Infrastructure-as-a-service (IaaS) security issues:

IaaS provides a pool of resources such as networks, servers, storage and other resources for computing in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor [5]. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial

effort to secure their systems in order to minimize these threats that result from mobility, creation, communication, monitoring and finally modification,. Here are some of the security issues associated to IaaS [5].

4. Security Concerns of Cloud Service Consumers:

Many people are wary of using cloud services because of concerns about loss of data, service outages, hackers compromising their accounts therefore leading to data theft, issues regarding their privacy, and compliance with laws, rules and regulations. Tech savvy enterprises, are likely to have skills and resources to monitor the service level of their service provider, assess the service provider's security detail, or implement their own security safeguards to protect their data. On the other hand, SMEs and other average cloud users, may not consider their own rights and responsibilities, be unsure about how to choose a credible cloud service provider and be hesitant on whether their data is adequately protected when using a cloud service.

5. What Cloud Service Consumers Should Be Aware Of?

Data processed or stored by cloud service users in a cloud service may contain sensitive, important, critical and personal information. Thus, the security measures provided by the cloud service provider is not sufficient enough to protect this data. SMEs need to be aware of what needs to be considered when choosing a cloud service provider and further be aware of the requirements to be considered when using cloud services. All the users of cloud service, both responsible businesses and individuals, are advised to have a deep and clear understanding of the issues and concerns for protecting their data in the cloud environment.

IV. SECURITY RISKS IN CLOUD COMPUTING

A. List of security risks in cloud computing:

Privileged user access -- Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.

Data location and segregation -- Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information.

Data disposal -- Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.

e-investigations and Protective monitoring -- The ability for cloud users to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model being used and the complexity of the cloud architecture. Users cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.

Assuring cloud security -Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

B. Solution of Security threats

1 **Find Key Cloud Provider**

First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

2 **Clear Contracts**

Contract with cloud vendor should be clear. So if cloud vendor closes or ceases to deliver the promised services, enterprise can claim compensation.

3 **Recovery Facilities**

Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

4 **Better Enterprise Infrastructures**

Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber attacks.

5 **Use of Data Encryption for security purpose**

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor. IT leaders must define strategy and key security elements to know where the data encryption is needed.

6 **Prepare chart regarding data flow**

There should be a chart regarding the flow of data. So the IT managers can have idea where the data is for all the times, where it is being stored and where it is being shared. There should be total analysis of data. [8]

V. MCC OPEN RESEARCH ISSUES

A. Research Issues in MCC

Issues regarding Architecture: Reference architecture for disparate MCC environment is a critical requirement for unleashing the advantages of mobile computing towards unrestricted universal computing.

Energy-efficient transmission: MCC requires continuous and incessant transmissions between mobile devices and the cloud platform, due to the stochastic nature of wireless networks, Energy efficient transmission protocols should be designed.

Context-awareness issues: Context-aware and socially-aware computing are inseparable traits of contemporary handheld computing devices. To achieve the goals of mobile computing among heterogeneous converged networks and computing devices, designing environment-aware application and applications that use resources efficiently are needed.

Live Virtual Machine migration issues: Executing resource-rich mobile application via Virtual Machine (VM) and migration-based application offloading involves encapsulation of application in VM instance and migrating it to the cloud, which is a challenging task due to additional overhead of deploying and managing VM on mobile devices.

Mobile communications and bandwidth issues: Mobile data traffic is tremendously hiking by ever increasing mobile user demands for exploiting cloud resources which impact on

mobile network operators and demand future efforts to enable smooth communication between mobile and cloud endpoints.

Credibility and security issues: Credibility is an essential criterion for the success of the burgeoning MCC paradigm.

Cloud computing: relates to the specific design of new technologies and services that allow data to be sent over distributed and scattered networks, using wireless connections, to a undisclosed remote secure location that is usually maintained by a vendor. Cloud service providers usually serve several clients. They set up access between the client's local or internal networks, and their own data repositories and data-backup systems. It implies that the vendor can take in data that is sent to them and store it safely, while delivering services back to a client through these carefully maintained connections.

Mobile computing relates to the emergence of new interfaces and devices. Smartphones and tablets are mobile computing devices that can do a lot of what traditional desktop and laptop computers do. Functions of Mobile computing include accessing the Internet through browsers, supporting different software applications with a core operating system, and sending and receiving data of different types and formats. The mobile operating systems, as an interface, supports users by providing intuitive icons, rich interfaces and familiar search technologies and easy commands or touch-screen actions.

B. Security Issues in Mobile cloud Computing

Cloud computing as opposed to standard computing has several issues which can cause reluctance or fear in the user base. Some of these issues include concerns about privacy and data ownership and security. Some of these concerns are especially relevant to mobile devices. In this section, the paper discusses some of these issues, including both incidents involving them and techniques used to combat them.

- Privacy
- Data Ownership
- Data Access and Security

C. Solution to Security issues in Mobile Cloud computing

Individuals and enterprises take advantage of the benefits for storing large amount of data or applications on the cloud. However, issues in terms of their integrity, authenticity, and digital rights must be taken care of.

1) Integrity:

Every mobile cloud user must ensure the integrity of their information stored on the cloud. Every access made must be authenticated and verified. Different approaches for preserving integrity of one's information stored on the cloud are being proposed.

2) Authenticity:

Different authentication mechanisms have been presented and proposed for using cloud computing to secure the data access suitable for mobile environments. Some use the open standards available and even support the integration of various authentication methods. For example, the use of log- in IDs, passwords or PINS, authentication requests approval etc.

3) Digital rights management:

Illegal distribution and piracy of digital contents such as video, image, audio and e-book programs are becoming more and more wide-spread. Some solutions to protect these contents from illegal access are implemented such as Provision of encryption and decryption keys to access these contents. A coding or decoding platform must be done before any mobile user can have access to such digital contents.[15]

D. Advantages of MCC

Extending battery lifetime:

- Computation offloading migrates large computations and complex processing from resource-limited devices (i.e., mobile devices) to resourceful machines (i.e., servers in clouds).
- Remote application execution which can save energy significantly.
- Many of the mobile applications take the advantages from task migration and remote processing.

Improving data storage capacity and power of processing:

- MCC enables mobile users to store or access large data on the cloud.
- MCC helps in reducing the running cost for the computation intensive applications.
- Mobile applications are not constrained or limited by storage capacity on the devices because their data now is stored on the cloud.

Improving reliability and availability:

- Keeping data, application and data in the clouds minimizes the chance of lost on the mobile devices.
- MCC can be designed as a comprehensive data security model for both service providers and users:
  - ✓ Protect copyrighted digital contents in clouds.
  - ✓ Provide security services such as virus detection, malicious/dangerous code detection, authentication for mobile users.
- With data and some services in the clouds, then are always (almost) available even when the users are moving.

Dynamic provisioning:

- Dynamic on-demand provisioning of resources on a fine grained, self service basis
- No need for advanced reservation

Scalability:

- Mobile applications can be performed and scaled to meet the unpredictable user demands
- Service providers can easily add and expand a service

Multi-tenancy:

- Service providers can share the resources and costs to support a variety of applications and large number of users.

Ease of Integration:

- Multiple services which are from different providers can be integrated easily through the cloud and the Internet to meet the users' demands.

VI. CONCLUSIONS

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, there will be some security problems which may slow down issues. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Mobile cloud computing is a technique or model in which mobile applications are built, hosted and powered using cloud computing technology.

Since Cloud Computing leverages many technologies, it also inherits/takes their security issues. Traditional or the old web applications, virtualization data hosting have been looked over, but some solutions offered are immature or inexistent. We have presented security issues for cloud models: PaaS, IaaS and IaaS, which changes depending on the model.

ACKNOWLEDGEMENT

I thank Dr. T. V. Suresh Kumar, Prof. and Head, Dept. of MCA, MSRIT, Bangalore-54. for his continuous support and encouragement for completing this research paper and also thanks to MSRIT management.

I thank Dr. Jagannatha, Associate Professor. of Dept. of MCA, MSRIT, Bangalore-54, for his valuable guidance and support for completing this paper.

REFERENCES

[1]. F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges",*IDC* Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[2]. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

[3]. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[4]. S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[5]. A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.

[6]. Florin OGIGAU-NEAMTIU - "CLOUD COMPUTING SECURITY ISSUES" The Regional Department of Defense Resources Management Studies,
Brasov, Romania - 2013.

[7] Jaydip Sen - "Security and Privacy Issues in Cloud Computing" -Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[8] Kuyoro S. O. Ibikunle F. "Cloud Computing Security Issues and Challenges" - International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[9] Kevin Hamlen, Murat Kantarcioglu - "Security Issues for Cloud Computing" - International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[10] Wayne A. Jansen, NIST - "Cloud Hooks: Security and Privacy Issues in Cloud Computing" -Proceedings of the 44th Hawaii International Conference on System Sciences - 2011

[11] Mohammad Sajid, Zahid Raza - "Cloud Computing: Issues & Challenges" - International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV

[12] Keiko Hashizume, David G Rosado, "An analysis of security issues for cloud computing" SPRINGER - Hashizume et al. Journal of Internet Services and Applications 2013

[13] Pradeep Kumar Tiwari, Dr. Bharat Mishra - "Cloud Computing Security Issues, Challenges and Solution" - International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[14] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" -2012, IJARCSSE, Volume 2, Issue 9, September 2012 ISSN: 2277 128X

[15] Monica B. Harjani, Dr Samir M. Gopalan - "Comparative study between Green Cloud Computing and Mobile Cloud Computing" International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013

