



## Cloud Computing in Mobile Applications

Rahul Srivastav<sup>1</sup>, Akshit Gupta<sup>2</sup>, S.Aravinth Kumar<sup>3</sup>, Dr. Ajay S. Singh<sup>4</sup>

<sup>1,2</sup> 2 Yr-B.Tech (CSE), Galgotias University, India

<sup>3</sup> Assistant Professor, SCSE, Galgotias University, India

<sup>4</sup> Professor, SCSE, Galgotias University, India

**Abstract:** Together with the huge growth of the mobiles application and rising of cloud computing techniques, mobile cloud computing (MCC) has been introduced as a technology with potential for mobile services. MCC convert the cloud computing into the mobile environment and overcomes the obstacles related to the performance (e.g., life of battery, storage capacity, and bandwidth), environment (e.g., heterogeneity, scalability, and opportunity), and security (e.g., reliability and privacy) concerned in mobile computing. This paper provides a survey of MCC, which gives overview of the MCC including the definition, architecture, and applications. The problems, present solutions and approaches are presented.

**Keywords** –Cloud Computing, Cloud Services, Challenges.

### I. INTRODUCTION

Mobile devices like iPhone, Blackberry, Android are becoming popular clients to use any Web resources, mainly Web Services (WS). This research paper discussed cloud computing as a currently exploring way to deliver remote mobiles application to mobile devices through internet providing a remedy to the lack of resources in mobile devices and also a new level of security is achieved by centralizing maintenance of security-critical software. It gives mobile world a new ad hoc infrastructure where storage of data and processing is performed outside the mobile device and cloud computing gets an extended feature of mobility.

DivyaNarain has also favored the concept that “Cloud computing” will soon provide a new ways of developing, acquiring, and using mobile applications. Processing of any mobile application is not going to be dependent on handset with advance configuration any more. From the desk of Senior Analyst Mr. Mark Beccue for Mobile application programmer, today’s major challenge is the presence of such vast range of mobile operating systems. They are mostly left with two options whether they write for only one OS or they can just create many versions of the same application. In any mobile devices for any application execution has two basic important requirements one are of processing power and other is that memory of that device capable of supporting that corresponding application. Scenario of „Cloud Computing” provides us this opportunity to execute our applications on servers instead of processing them locally and support us to overcome the handset’s limitation of finite resources to a great extent. And also there will be no requirement for Mobile application programmers” to developed many versions of duplicate application. It’s just the starting of a new phase of mobile application development; still there is a long way to go to developed a new mobile world infrastructure involving cloud computing in its base

### II. CLOUD COMPUTING

This is published from the University of California, Berkeley state that cloud computing does not have a commonly agreed upon definition. But yes these days its brand new definition is developing according to its offerings, features, characteristics, service models, and deployment models . The National Institute

of Standards and Technology (NIST) has given a definition for „Cloud computing“ which says “Cloud Computing is a model for enabling convenient, on-demand network access to share pool of configurable computing resources (example, networks, servers, storage, applications, and services) that can be frequently provisioned and released with less management effort or service provider interaction. ”

From layman’s language it can be conclude that the ability to achieve sector of heavy resources fastlyand freely as per the demand and user is charged as per demand of resources .It’s a web-based process, where resources,software, and information are shared, provided on demand to computers, smartphones, and other similar devices allowing users to adjust their computing power depending on how much is needed at a given timeintreval or for a given task . Five essential features of cloud computing listed by NIST in are:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

In overall Cloud Computing revolves around two things one is Cloud Platforms (CP) and second is Cloud Services (CS).

### III. CLOUD PLATFORM

Cloud Platforms are mainly the hosts that provide the needed resources (computational power, storage, Web access etc) to the client. It is an arrangement for runing software applications in a logically abstract environment combining of various utility cloud services.

Cloud platform is a platform which helps developers to write or design applications that run on cloud, or enable clients to use the services provided by the cloud, or both. It is the cloud Platform that is responsible for providing an application that specified physical environment for its execution without the need of purchasing and managing its corresponding hardware and software requirements .

It is from the cloud platform, the service provider arranged an operating system and a development environment where client’s required application is grown or run as per user want. Moreover client needed to setup the installation of compulsory applications . Cloud computing are handle by cloud service providers that inlude Amazon cloud drive, Google apps,icloud, egnyte and dropbox including local vendors including Hewlett Packard, IBM, Intel, Microsoft they are opted by various users, ranging across to an individual from large companies including General Electric, L'Oréal, Procter & Gamble and Valeo. Some reknowned cloud platform are:

- I. Citrix cloud platform
- II. Google cloud platform
- III. Fujitsu global cloud platform
- IV. Xen cloud platform

### V. CLOUD SERVICES

Cloud provide the remote services which are hosted over the network from any other places. In cloud system large number of computer working over internet to facilitate internet server . With the advancement of cloud services it is easy to different clients and users to access his data saved on cloud, use the service of cloud and content placed remotely. Using internet one can connect to his cloud account and access the desire information what he wants from server. It can be concluded that cloud is a

service which uses software system for giving interoperable machine interaction on network. some examples are:

1. Identity
2. Integration ( Amazon Queue Service)
3. Mapping ( Google Maps, Yahoo! Maps)
4. Payments ( Amazon Flexible Payments Service, Google Checkout, PayPal)
5. Search ( Alexa, Google Custom Search, Yahoo! BOSS)
6. Others ( Amazon Mechanical Turk)

## VI. CHALLENGES AND SOLUTIONS

For achieving common and regular environment of cloud computing for the cellphone apps we have to work on various mobile infrastructure to get drive of network latency and transmission delay. Efficiency of delivering services/apps is needed to be increased in order to achieve to access anywhere and with whatever device.

Concept of cloud computing in mobile is to deliver mobile services over network using cloud vendors,. Manufacturing of different remote applications which are available for mobile devices contain main component are:

1. Mobile device
1. Network (on which mobiles devices are accessing accessed cloudcloud)
2. Mobiles Application
3. Security

All of these component have some extent of challenges

### A. Challenges regarding mobile devices

**1) Constrained energy sources for mobile devices:** For change the presettings, adjust on templates as describe. Energy scope of cellphone gadgets depended upon their power resources battery. Its power have fixed strength so it is important to increase its life. Number of program running on cloud suppose to conserve more battery but commonly it can not be done to move the whole implementation in the cloud. Some basic example

Are running the app on the cloud and displaying it on the device It may be application function may be partition across various cloud that is to be remove to the cloud and they can be run by themselves. Mobile gadgets mainly consume energy in playing an app or network connectivity.

Supposing that various exhibited element relate to under attention that it can be grouped into two categories, First one display applications and second one non-display application. Display and practical app required huge battery cells because it execute huge displays while non-display app mostly had comparely less display usage. Few non-display program such as threat and malwar examining, etc are most perfect for being removed from cloud.

In deeply engaging applications, running remove flexibility is very powerful constrained, as application functions running on server and device are tightly hold. For this reason, the battery-saving strategy for immersive applications typically comes down to finding the least expensive path to connect to the cloud servers and minimizing inactivity to maintain high interactivity. For smartphones, Wi-Fi represents the less costly path (with 23% less energy consumption) in comparison to GPRS in a web browsing scenario. If we ignore the maintenance of GPRS connection (for example, for non-phone devices like

tablets) then the power consumption of GPRS versus Wi-Fi is even starker, with Wi-Fi using just one third of the energy of GPRS.

**2) Resource poverty of Mobile Devices:** *pc* when we compare *pc* with mobile devices it show at what cost mobility is achieved. In comparison to a fixed device, mobile devices in general have:

2. 3 extent fewer execution potential
3. 8 extent fewer space
4. 5 extent fewer content volume
5. 10 extent fewer network bandwidth

### **B.Challenges with Mobile Applications**

**1) Interoperability:** Institute that follow Bring-your-Own-Mobile (BYOD) norms commonly faces interoperability objection it may be happen that an assorted combined with gadgets as for example iPhone, Android phones, BlackBerry and others been utilized by workers in the institute or delicately distributing a network. At that condition features of cloud program are in service and os of mobile devices have interoperability issue which is a major in take out data in many devices .BYOD norms applicable power maker to have a wide area having latest technology & infrastructure qualities which can be construct into program, facilitating secure reach of companies data

Using technology we can work on maximum optimization of mobile accessibility using its background and location info.

**2) Cloud And its program Flexibility:** A program have cloud supported infrastructure which can not be denied on the type of its requirement vst the cloud infrastructure qualities that a device have, network bandwidth and latency vectors.

various program requires is variant for its considerable cloud infrastructure entities (computation intensity, network bandwidth, and network latency). like, loosely coupled & low-capacity program such as browsing would give maximum output on a 3G bandwidth together with comparatively down compute servers away from data center. If we think in another direction program such as real-time face recognition which ask for a high-bandwidth/low-latency network similar to LTE so that bigger size image can be move fastly as compare to other and seamlessly to the servers running the face recognition algorithm and the user-facing devices. In high-demand applications transfer and its delay can be decrease by taking in view of data centers. And for a powerfully advance program of mobile cloud infrastructure could be used Wi-Fi rip off that minimal passiveness substitute that are in demand

**3) Mobile cloud convergence:** For approach in gain interest of mobile technology from accomodation cloud computing to mobile environment, Data circulation is the major problem. Boundary of mobile gadgets for their computation potential manufacture duty sharing very primary as the computation potential of mobile gadgets is not have efficiency enough for making these gadgets to be in the main computation podium. Concurrence of mobile cloud labourer carry out progress, elongated life for batteries, and a quick fix to the computation potential dilemma. Chief drawing near by mobile cloud concurrence is to divide the function such that place that require large calculation will execute on the cloud and rest sectors which is related with the end user interface can execute on the mobile gadget. Since unique action is being divided here this is the reason why IPC (inter-process communication) is very significant to comprehend this concurrence. An revised and maximal PI computation algorithm can be gain by maximizing mobile cloud concurrence .Cableless tech., early electric technologies and internet has to extend along and combined together for gaining universal and persistent computing.

### C. Security Challenges

**1) Security:** Since cloud technology mainly operate with file storing & execution that's why the most important thing is security. At present several cloud platforms gives the offer of robust prepared safety concerns SSL and certificates which are digital that facilitate a service option to activate security by external techniques .

Since security of data is bothering companies it is essential to merge info lock on and operational security (IA and OPSEC) norms & procedures. Organization-wide training, education, and awareness packages concentrating mainly on IA and OPSEC problems that can also be merge to confident that the norms and procedures are go after fully. Norms related to gain charge, load validation procedures and user authority data declaration, encryption and common security communication (COMSEC) must be generated & assent scale has to be taken for pouring them. This is very compulsory too to set up & manage users belief over the platform of mobile for security and for providing user privacy & application of data confidentiality from oppose.

Mobile gadgets security will always remain a key concern. If mobile gadgets is swiped or mislaid vital data can be adjust. Maltreatment of data from swiped/ mislaid gadgets can be rejected by sweeping the mobile gadgets as side effect. This speciality is mostly facilitated by the most mass producer of mobiles & cableless carriers. Mobile gadgets (cell phones, PDA, smartphones etc) are accessible to variety of threats of security such as malware codes (e.g. ,worm, virus, and Trojan horses). The Global Positioning System (GPS) of mobiles can also increase problems related to privacy. Easiest mode for sensing threats (e.g., virus, worms, and malware codes) in mobile is settling & executing antivirus applications (like Avast, Norton, Quickheal & Avira etc). But gadgets like mobiles has fixed executing capacity & supply of power, securing it of these virus is much difficult than securing innovative gadgets like PC. It is also possible to transfer the threat sense efficiency to the clouds. The given idea widens the present Cloud of AV platform which gives service for malware sense in cloud detection. This will facilitate us to avail maximum anti-virus softwares in coordinate by presenting the softwares in virtualized boxes. The technique power up the capacity of sensing malwares and it also upgrade the lifetime of it's battery to 30%. Also, keeping data/applications of such huge volume on cloud have its own advantages but straight forwardness, provising and the digital rights regarding the applications should also be considered .

**2) Isolation and Confidentiality:**Talking about several plans and norms (like Fair Information Practice law (FIPP)) being presented which needed perfect inside track and norms to prevent the personal details of user. Companies which collect data should have some rules & procedures in order to manage, store & destroy it safely and it must be fulfilled in order to keep the user's privacy. Danger of personal detail exposure, swiped identity & fraud has to be reduced by applying power up prevention scale for sharing data between systems which are interconnected, applying observational skills & protocols & by guiding the people about proper social media safe-surfing. By setting up and applying processes to save their foundation from provisioning social media use & organisations can save themselves from serious legal & problems related to security. Otherwise it will cause their information structure and reputation a lot of damage.

Encryption gives the very advance technique to manage isolation of private details & information confidentiality. It support storing and transferring of data but centrally block processing of data. Hence , startlingly, it was wasteless by sending encrypted data to the providers of cloud for processing. But thiss challenge has met by homomorphic cryptography (HC) which assures that computations

performed by an encrypted column effect in the encrypted interpretation in the computed column .GPS orientating device has well favoured mobiles consumers for using location based services (LBS). However, LBS bump up a security issue when mobile consumers provides personal informations such as their present locations & it turn even worst if an opponent knows some of user's other primary detail. The Location trusted servers (LTS) gives answer to these issues . Digital rights management (DRM) gives another paramount issue of privacy. Digital contents which are unstructured (example, ebook, audio, images & video) are frequently being illegally copied & distributed among consumers. To stop the piracy & unstructured digital contents distribution declare. The cloud unfree mobile based Digital Rights Management (DRM) plot along with the sim cards in smartphones. This enhances malleability & also reduce the exposure to the security at low rate. However this push pass on is mainly based on sim card of mobile phones, so it cannot be used for other kinds of entranceway like a notebook using WiFi to approach the collection of data .

**3) Attacks by Malicious:** Every network is unresistant to attacks by malicious softwares. Number of Websites is getting approached by mallicious product has high possibility to gain the access of the network & active info. of the firm. Applying security management to all Web 2.0 server & cross check those strict privacy management can minimize the harmful threats to internal networks & computational data. Add on, isolation Web 2.0 servers from other inside servers may further lessen the threat of certified access to info. through social media tools and Web sites. Some of the potential vectors attacker criminals may attempt include:

**1.Denial of Service (DoS) attacks** – It has been explained that a cloud is more easily susceptible to a DoS attack; because more than one client can access the cloud at the same time, which makes DoS attacks much more damaging. Twitter has suffered a devastating DoS attack in 2009.

**2.Side Channel attacks** – In this kind of attack a malicious virtual machine is placed in close proximity of a target cloud server to compromise the cloud security and then a side channel attack is launched.

**3.Authentication attacks** – Authentication is one of the weak points in case of hosted and virtual services and is generally been targeted. A consumer can be genuine in variety of ways and these action and methodology which are used to prevent the genuine process are mostly been pointed by the ambushers.

**4.Man-in-the-middle-cryptographic attacks** – These attack is mostly done when an ambusher placed himself in the middle of two users. In this type of strike attacker keep himself in the communication layout and then it is on to him what to do, he can cut out and corrupt the layout for communication .

**4) Network Monitoring:** As extension in access time & bandwidth the difficulty of network operational performance observation is also an essential hot button concern which call for proper treatment & care. This is unfavourable to use a projectile cloud performance system which can re-route the traffic, accessing, replacing & handover. Even with all these key's provoke given mobile computing is still feasible business & is being preferred by more cloud user. Foreign intelligence services (FIS) have widen resources & have continously show their capability to use automated "social engineering" techniques to mime sites of social media. Due to their different quality, sites of social media have abundance of information, which makes them vulnerable to data mining. Their rivals can use their data to analyze aggregated information. Without monitoring the network, a company cannot ensure that whether users are complying or not its policies regarding the release of high-value information. Also, programming languages used in Web 2.0 applications (e.g., Java, Ajax, and the JSON data interchange

format) may also create opportunities for malicious softwares to access an company's back-end network infrastructure and done irreparable damage. Accordingly, an institution using social media may call to apply maximum security management for any isolated delicated information reside on the backend of server.

**5) Enforcement and Compliance:** There are no conventional standard sets that can be come after occurance and policy of cloud computing apply. However there are still number of principle focusing storage & application of data, carry Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, among others. Uniform informing & editing drop back are needed for many of these normss. These norms are needed to be finished and about to corporate data to be moved to the cloud. It may be tough or imaginary to utilize public clouds if data is dominate to authorized restrictions or daily compliance. We can assume suppliers to construct and approved cloud framework to address the requirement of continous markets. Gaining approval may be competative due to the many non-mechanical facts, including the present state of general cloud knowledge. There are huge number of security threats; it is impossible to apply preventive scale to all of them. When user run any program and he is aware of the acerbity and nature of potential threats to security related with its use then he can block process that are more prone to security attacks. This give rise to applicant knowledge and training crucial in preventing networks and data. From the arrival of social media, training programs are also required add to address the additional risks posed by social media. This social media training can be incorporated to the annual security training programs of organizations

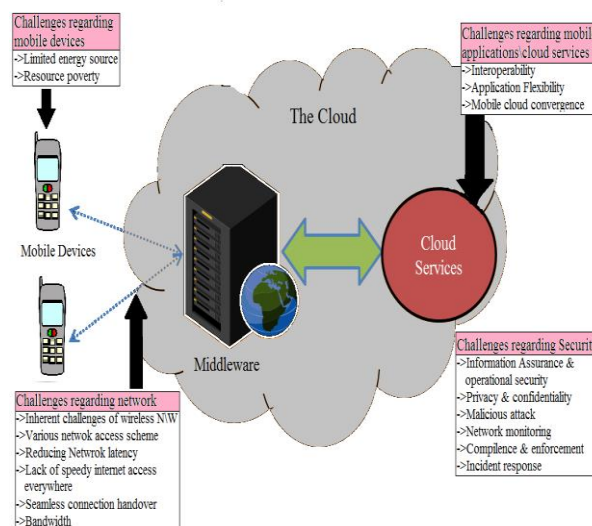


Fig:1

## REFERENCES

1. DivyaNarain. March 2009. "ABI Research: „Mobile Cloud Computing“ the Next Big Thing”, <http://ipcommunications.tmcnet.com/topics/ip-communications/articles/59519-abi-research-mobile-cloud-computing-next-big-thing.htm>
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 10 February 2009, "Above the Clouds: A Berkeley View of Cloud Computing," EECS Department University of California, Berkeley. Technical Report UCB/EECS-2009-28, <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>.
3. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Version 15, 7 October 2009, <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.

4. DoD Directive 3020.40, Defense Critical Infrastructure Program, 19 Aug, 2005, p. 13, <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>.
5. ZTE Communications. March 2011, Vol.9, No.1, „Special Topic:Mobile Cloud Computing and Applications“ <http://ebookbrowse.com/p020110318511856092974-pdf-d100931817>
6. IANewsletterVol 13 No 2 Spring 2010. „Cloud Computing: Silver Lining or Storm Ahead“ <http://iac.dtic.mil/iatac11>
7. Adrian Otto“s Blog. „What is a Cloud Platform?“ <http://adrianotto.com/2011/02/cloud-platform/>  
<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>.
8. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Version 15, 7 October 2009, <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.
9. DoD Directive 3020.40, Defense Critical Infrastructure Program, 19 Aug, 2005, p. 13, <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>.
10. ZTE Communications. March 2011, Vol.9, No.1, „Special Topic:Mobile Cloud Computing and Applications“ <http://ebookbrowse.com/p020110318511856092974-pdf-d100931817>
11. IANewsletterVol 13 No 2 Spring 2010. „Cloud Computing: Silver Lining or Storm Ahead“ <http://iac.dtic.mil/iatac11>
12. Adrian Otto“s Blog. „What is a Cloud Platform?“ <http://adrianotto.com/2011/02/cloud-platform/>
13. Resources: Internet Marketing Glossary. <http://www.digital-marketing-course.co.nz/resources.php?Glossary-8>
14. TavisJ.Hampton. August 11th, 2011. „A Quick Guide to Cloud Terminology“, <http://www.thehostingnews.com/a-quick-guide-to-cloud-terminology.html>
15. “Amazon elastic compute cloud (EC2).” AWS. [Online]. Available: <http://www.amazon.com/ec2/>
16. Google app engine. [Online]. Available: <http://appengine.google.com/>
17. <http://www.force.com/why-force.jsp>
18. Microsoft azure. [Online]. Available: <http://www.microsoft.com/azure/>
19. E. Marinelli, “Hyrax: cloud computing on mobile devices using MapReduce”, Master thesis, Carnegie Mellon University, 2009.
20. Fung Po Tso, Lin Cui, Lizhuo Zhang, and WeijiaJia. March 18th, 2011. “Building a Platform to Bridge Low End Mobile Phones and Cloud Computing Services”  
[http://www.zte.com.cn/endata/magazine/ztecommunications/2011Year/no1/articles/201103/t20110318\\_224547.html](http://www.zte.com.cn/endata/magazine/ztecommunications/2011Year/no1/articles/201103/t20110318_224547.html)
21. Cloud Computing. October 11th 2008, <http://www.reference.com/browse/cloud+computing?s=t>
22. API Dashboard at programmable web. <http://www.programmableweb.com/apis#topa-1>
23. JitendraMaan, „Extending the Principles of Cloud Computing in Mobile Domain“ D.C. Wyld et al. (Eds.): NeCoM/WeST/WiMoN 2011, CCIS 197, pp. 197–203, 2011.© Springer-Verlag Berlin Heidelberg 2011
24. Kyung Mun, *Corporate Technology Strategist*, „Mobile Cloud Computing Challenges“, <http://www2.alcatel-lucent.com/blogs/techzine/2010/mobile-cloud-computing-challenges/>