ISSN 2250-3153

Cloud Computing in Mobile Applications

Deepti Sahu, Shipra Sharma, Vandana Dubey, Alpika Tripathi

Department of Computer Science, Amity University, Lucknow, India

Abstract- Cloud computing is emerging as one of the most important branch for providing seamless applications on mobile devices. In this paper, cloud computing is introduced as a new and speedily growing and accepted way of providing better and efficient applications for mobile devices. It provides mobile users with data storage and processing services on a cloud computing platform.

We are going to discuss two major questions which are basically raised on implementation of any technique. One is "how we are going to implement it?" and second "what is going to be affected by it?" OR "what challenges have to be resolved for its successful implementation. While considering about cloud computing in mobile devices first question about its implementation is further distributed in two aspects, one is how to build cloud for mobile devices and second how mobile devices will access this cloud for data and application processing. While considering about challenges we have identified/discussed various issues regarding mobile devices, mobile network, mobile applications and some major security concerns. So in a whole main objective of this paper is:

1. To discuss how to implement cloud computing for mobile devices providing data storage and processing outside the device:
   - How to build cloud for mobile devices.
   - How mobile devices are going to access applications being offered by these clouds.
2. What are the major challenges in its seamless implementation and what are their possible solutions?

Index Terms- Cloud Computing, Cloud Platform, Cloud Services, Mobile Applications

I. INTRODUCTION

Mobile devices like iPhone, Blackberry, Android are becoming popular clients to consume any Web resources, especially Web Services (WS). This paper discusses cloud computing as a currently exploring way to deliver remote mobile applications 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 provides mobile world a new ad hoc infrastructure where data storage and processing is performed outside the mobile device and cloud computing gets an extended feature of mobility.

Divya Narain has also favored the fact that 'Cloud computing' will soon provide a new way of developing, acquiring, and using mobile applications [1]. Execution of any mobile application is not going to be dependent on handset with advance configuration any more. According to Senior Analyst Mark Beccue for Mobile application developers, today's major challenge is the existence of such a wide range of mobile operating systems. They are generally left with two options either they write for just one OS or they just create many versions of the same application. In any mobile device for any application execution two basic significant requirements are of processing power and 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 running them locally and favors us to overcome the handset's limitation of limited resources to a great extent. And also there will be no need for Mobile application developers' to create many versions of same application. It's just the starting of a new phase of mobile application development; there is still a long way to go to achieve a new mobile world infrastructure involving cloud computing in its base.

II. CLOUD COMPUTING

It is published by the University of California, Berkeley report that cloud computing does not have a commonly agreed upon definition [2]. But yes now days its new definition is evolving according to its offerings, characteristics, service models, and deployment models [3]. National Institute of Standards and Technology (NIST) has given a definition for 'Cloud computing' which says that:

"Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [4]

In layman's language we can say that it is the ability to acquire parts of bulk resources quickly and easily according to the requirement and the client is charged for those resources on usage basis. It's a web-based processing, whereby shared resources,

software, and information are provided on demand to computers, smartphones, and other similar devices allowing users to adjust their computing capacity depending on how much is needed at a given time or for a given task [5]. Five essential characteristics of cloud computing listed by NIST in [6] are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

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

A. Cloud Platform

Cloud Platforms are basically the hosts that provide the required resources (computational power, storage, Web access etc) to the client. It is an arrangement for executing software applications in a logically abstract environment comprising of various utility cloud services [7].

Cloud platform is a platform which enables developers to write or design applications that run on cloud, or enable clients to utilize the services provided by the cloud, or both. It is the cloud Platform that is responsible for providing an application its specified environment for its execution without the need of buying and managing its corresponding hardware and software requirements [8].

It is through the cloud platform, the service provider arranges an operating system and a development environment where client's required application is developed or executed on demand. Further customer is required only to develop or install the necessary applications [9]. Cloud computing is being driven by cloud providers including Amazon, Google, Salesforce and Yahoo as well as traditional vendors including Hewlett Packard, IBM, Intel, Microsoft and are adopted by different users, ranging from an individual to large enterprises including General Electric, L'Oréal, Procter & Gamble and Valeo. Few well-known cloud platforms are:

- Amazon Elastic Cloud Computing (EC2) [10]
- Google App Engine (GAE) [11]
- Force.com [12]
- Microsoft Azure [13]
- Hyrax [14]
- Tumb_in_cloud [15]

Table I: COMPARISON OF EC2 AND GAE CLOUD PLATFORMS

Properties	EC2	GAE
Administration	Need to keep track of traffic (now automated through scripts) and spin-off new instances on the basis of your configuration.	Virtually nil administration, required once when your application is deployed.
Portability	More portable	Less portable than EC2
Auto Scale Option	Elastic MapReduce	Billable option
Charging Model	Time and Resource	Resource
Focus	Infrastructure	Platform
Basic Technology used	Virtualization	Existing Google infrastructure
Languages supported	Any language as long as you can install it on OS and the hardware that they provide.	Python, Java, and any language which get converted to bytecode and can execute on JVM
Service Access Interface	Command line Web Services	Commandline
Service model	Virtual Machine with OS image	Web Application Container
Best suited for	Appl. requiring heavy processing power for short interval	Startups wanting it free
Services being offered	Provide tools to build failure resilient applications and isolate themselves from common failure senerios.	Provide ready to use services which help in rapid application development.
Other bundled Services	AmazonS3 Amazon SimpleDB Amazon RDS AmazonSQS	Data store Memcache URL fetch Mail Task Queue

B.Cloud Services

Cloud services are hosted services. Here a computer a group of computers working as internet server offers a part of or its whole required resources for use in exchange of certain rental fee. These are the cloud services which make it possible for different clients to access information, services and content located on any remote location or on to this server. Client uses internet to connect with the server and displays the desired content to the client. So we can say that *cloud service* [16] (eg Web Service) is software system(s) which is responsible for providing interoperable machine-to-machine interaction over a network or internet which is further accessed by other cloud computing components, clients, software (eg Software plus services) or end users directly. For example:

- Identity (OAuth, OpenID)
- Integration (Amazon Simple Queue Service)
- Mapping (Google Maps, Yahoo! Maps)
- Payments (Amazon Flexible Payments Service, Google Checkout, PayPal)
- Search (Alexa, Google Custom Search, Yahoo! BOSS)
- Others (Amazon Mechanical Turk)

III. CHALLENGES AND THEIR POSSIBLE SOLUTIONS

In order to get pervasive and ubiquitous environment for cloud computing in mobile applications we need to get across various stages of mobile infrastructure, which are responsible for added network latency and transmission delay. Efficiency of delivering services/apps is needed to be increased in order to achieve goal of access anywhere and with whatever device.

Using cloud computing concept in mobile world is all about supplying mobile applications and services in the cloud, enabled through cloud service providers and then deliver it to end-users' mobile handsets over the Internet when required. So in making remote applications available to mobile devices by the use of cloud computing, main entities of this arrangement are:

- Mobile device
- Network (through which mobile devices are accessing cloud)
- Mobile Applications
- Security

All of these elements have some extent of challenges or we can say that expectations attached to themselves which are discussed here.

A. Challenges regarding mobile devices

1) *Limited energy source of mobile devices:* To change the default, adjust the template as follows. Power capacity of mobile devices is based on their batteries whose capacity is limited so it is very important to maximize the battery life. More and more application execution in the cloud means more battery saving but in general it is not possible to completely transfer the whole application execution to the cloud. For example basic functions like opening of an application, inputting data and displaying result of processing obviously need to run on device. We can just partition application function which is to be offloaded to the cloud and which is to be carried out on device itself. In case of mobile devices energy is basically used for displaying different element and for internet connectivity [18].

If display element is taken under consideration then we can divide mobile application into two major categories, one is display applications and second is non-display application. Display and sophisticated applications need larger battery packs as they have to run larger displays while non-display applications generally have very little display usages. Some non-display applications like virus scanning, etc are most suited for being offloaded to cloud.

For immersive applications, execution offload flexibility is even more constrained, as application functions running on server and device are tightly coupled. For this reason, the battery-saving strategy for immersive applications typically comes down to finding the least costly path for connecting to the cloud servers and minimizing latency 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:* Comparison of desktop pc with any mobile device shows that on what cost this feature of mobility is being achieved. As compared to a fixed device, mobile devices in general have:

- 3 times less processing power
- 8 times less memory
- 5 times less storage capacity
- 10 times less network bandwidth

So in general we can say that this resource deficiency is one of the major reason for the adoption of mobile cloud computing. In order to overcome this limitation of mobile devices, resources are added to the cloud infrastructure and can be used anytime on requirement, providing a seamless user experience for advanced applications. Even after continuous improvements in mobile device performances', the disparity between the resource constraints of mobile and fixed devices will remain and must be accounted for in the types of application selected for mobile cloud computing [19].

B. Challenges regarding network

1) *Inherent Challenges of Wireless Network:* Wireless network is base for carrying out cloud computing and it has its own intrinsic nature and constraints. These challenges complicate its design for mobile devices even more in comparison to the fixed cloud computing.

Fixed broadband is supported by consistent network bandwidth while wireless connectivity is characterized by variable data rates, less throughput, longer latency and intermittent connectivity due to gaps in coverage. Subscriber mobility and uncontrollable factors like weather are also responsible for varying bandwidth capacity and coverage [19].

2) *Various Network Access Schemes:* For implementing cloud computing to mobile devices basic requirement is to have an access to network. In mobile world there are heterogeneous access scenario with different access technologies like WiMAX, WLAN, 3G, GPRS and so on, each one with their own schemes, policies, offerings and restrictions. Due to the existence of different access schemes we need seamless connection handover schemes (to avoid connection failure and connection reestablishment) when we move from one network access point to another network access point [20].

3) *Reducing Network Latency:* Factor responsible for overall delay response of applications are:

- Processing time at the data center
- Processing time on the device
- Network latency
- Data transport time

Processing time involved is based on application and we can't do so much for it. But yes measures can be taken to improve the network latency. Keeping the applications as close to the users can reduce latency delay as latency is significantly affected by distance. Heavy data like video and podcasts if kept closer to the device then it will save bandwidth and cuts transmission delay. Similar is the case with highly immersive apps, such as real-time translation. Latency can be positively improved by allowing service providers to re-route internet traffic logically based on the location and cache capabilities, and can save bandwidth effectively.

4) *Lack of Speedy Mobile Internet Access Everywhere:* In order to get speedy mobile internet access new technologies like HTML5 are being developed. They provide facility of local caching. Researchers are working to get a better way of accessing mobile web other than browser. Technologies like OMA's Smartcard Web Server and TokTok are being introduced just to provide a better access to mobile web. OMA's Smartcard Web Server, which is basically a souped-up SIM card that connects directly with the carrier to provide applications to mobile phones. TokTok allows voice enabled access to web services like Gmail and Google Calendar. Through these voice-enabled searches, mobile apps talk directly to the service itself sitting on the edge of the network, avoiding the requirement to launch a web browser and navigate through the mobile web.

In order to resolve this connectivity problem existing with mobile devices, most of the providers are offering 4G/Long Term Evolution (LTE) services. These services provide advantages of data storage capacity, plug and play features, low latency, and they also supports both FDD and TDD using the same platform. According to the requirement, sometime LTE is also loaded on speed as it is capable of providing download peak rates of 100 Mbps and upload of 50 Mbps [21].

5) *Seamless Connection Handover:* In order to provide data communication using cellular network mobile operators are trying to set up Wi-Fi Aps on street so that offload traffic of Wi-Fi systems can be reduced, resulting in reduced cellular traffic congestion. But in this arrangement basic requirement is to provide seamless connection handover between access networks. Currently executing application is terminated or returns error when we move from one access point of network to another access point of network or we move from Wi-Fi network to 3G-based cellular network due to occurrence of communication failure and connection reestablishment situation.

Problem of Communication failure is described as broken-pipe problem and it can be resolved by having communication channel with flushing zero window notification. And problem of connection reestablishment is defined by bind error, and can be resolved by implementing TCP port inheritance during socket reconstruction. No additional messages for channel clearing are introduced and no modifications are imposed on TCP protocol stack during TCP port inheritance. Approach of TCP inheritance is independent of the internal architecture of current 3G cellular networks as it is purely based on end-to-end architecture. By imposing Zero window advertising and TCP port inheritance our open network connections can be preserved and even server sockets also [22].

6) Bandwidth: Now a day accessing social media sites (e.g., YouTube, Facebook, etc) through mobile is becoming very popular. But these sites generally require more bandwidth in comparison to the traditional sites. If number of clients using social media of any

organization increases then demand for modified network infrastructure capable of supporting wide-scale use of external and resource-intensive Web sites also increases. Overall mission capabilities will get impair over time if the social media functions starts to compete with the organization's other functions for use of the network. Then it becomes organizations' responsibility to plan for it and ensure that adequate bandwidth is available for widespread Internet use. Additional bandwidth can be achieved from hosting environments to cover surges in Internet or network activity. Memorandums of understanding (MOU) are developed between organizations and their respective hosting companies just to ensure that sufficient bandwidth is made available during surges of activity that may occur at an emergency event, time of heightened network activity, and with increasing popularity in social media [6].

In case of rich internet and immersive mobile applications, e.g. online gaming, that require high-processing capacity and minimum network latency cloud computing faces challenges due to low bandwidth of mobile network. So an improved network bandwidth is required so that data transfer within the cloud and other devices can be improved.

C. Challenges related to Mobile Applications

1) *Interoperability:* Organizations that follow Bring-your-Own-Mobile (BYOD) policy generally faces interoperability challenges [23]. It's possible that there is an assorted mix of mobile devices including iPhone, Android phones, BlackBerry and others being used by employees in an organization or a group of people sharing a network. And in such situation according to the nature of cloud applications being used and operating system of mobile device interoperability issue can prove to be a major challenge in pulling/ pushing data across multiple devices [24].BYOD policy acceptance forces developers to think of a wide range of new security and management features that have to be build into application, providing safe access to company data [25].

By using context and location information we can work for optimizing mobile access. Context aware services exploit data collected from terminal sensors or network sensors measuring network statues and load. Network services and consumer application both uses these information.

2) *Cloud Application Flexibility:* An application is going to be supported by certain mobile cloud infrastructure or not, can easily be judged on the basis of its requirements against the cloud infrastructure characteristics along the device, network bandwidth and latency vectors.

Different applications' needs are different for its respective cloud infrastructure attributes (computation intensity, network bandwidth, and network latency). For example, a loosely coupled and low-content application like web search will provide optimal result on a 3G network with relatively low compute servers at a 'distant' data center. But if we talk about a hugely immersive and content-rich application like real-time face recognition it will require a high-bandwidth/low-latency network like LTE so that large image content can be transferred quickly and seamlessly to the servers running the face recognition algorithm and the user-facing devices. In high-demand applications transmission and latency delay can be minimize by considering 'nearby' data centers. And for a highly immersive application mobile cloud infrastructure can go for Wi-Fi offload that reduced latency further which is generally required by such applications [19].

3) *Mobile Cloud Convergence:* In order to achieve advantage of mobility by integrating cloud computing to mobile world, Data distribution is the key issue. Limitation of mobile devices for their computing power makes task distribution very important as the computing power of mobile devices is not powerful enough for making these devices to be the main computing platform. Mobile cloud convergence provides performance improvement, longer battery life, and a solution to the computation power problem. Basic approach of mobile cloud convergence is to partition application such that parts that need more computation run on the cloud and remaining parts which is associated with the user interface run on the mobile device. As a single process is being partitioned here so IPC (inter-process communication) is very important to realize this convergence. An improved and optimal PI calculation algorithm can be achieved by optimizing mobile cloud convergence. Wireless technologies, advanced electronics and internet are overlapped and integrated to achieve pervasive and ubiquitous computing [22].

D. Challenges regarding Security

1) *Information Security:* Since cloud computing basically deals with data storage and its processing so security is of paramount importance. Now a day's various cloud platforms offer robust built-in security measures. SSL and digital certificates provides an option to enable external security [26].

As far as data security is concerned organizations are needed to incorporate information assurance and operational security (IA and OPSEC) policies and procedures. Organization-wide training, education, and awareness package focusing on IA and OPSEC issues can also be included to ensure that the policies and procedures are followed completely. Policies regarding access control, authentication procedures, account and user management, encryption, content assurance, and general communications security (COMSEC) should be developed and compliance measures should be taken for enforcing them [6]. It is very important to establish and maintain consumers' trust on to the mobile platform protection for providing user privacy and data/application secrecy from adversary.

As far as mobile devices are concerned security remains a key concern. As if a device gets stolen or misplaced, crucial data may be compromised. Data misuse from stolen/ misplaced devices can be avoided by wiping of mobile device remotely. This feature is generally provided by most of the mobile manufacturers and wireless carriers [27]. Mobile devices (cellular phone, PDA, smartphone etc) are vulnerable to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses). Global Positioning System (GPS) of mobile devices could also raise privacy issues. Simplest way to detect security threats (e.g., virus, worms, and malicious codes) of any mobile device is by installing and running security softwares (like Kaspersky, McAfee, and AVG antivirus programs etc). However, mobile devices have limited processing power and energy supply, protecting them from the threats is more difficult than that for resourceful device (e.g., PC). We can move the threat detection capabilities to clouds. This paradigm is an extension of the existing Cloud AV platform that provides an in-cloud service for malware detection. It also enables us to use multiple antivirus engines in parallel by hosting them in virtualized containers. This approach enhances the efficiency of detecting malware and also improves battery lifetime up to 30%. Although storing a large amount of data/applications on a cloud has its own benefits but integrity, authentication and digital rights of data/applications should also be taken into consideration [28].

2) *Privacy and Confidentiality:* There are various policies and schemes (such as Fair Information Practice Principles (FIPP)) being proposed which require rigorous controls and procedures to protect the privacy of individuals. Organizations that collect data\information must have some policies and procedures in order to handle, store, and dispose them securely and must be implemented to maintain the privacy. Risk of privacy exposure, identity theft and fraud can be reduced by implementing enhanced protection measures for sharing data in interconnected systems, implementing monitoring capabilities and protocols, and by educating users about proper social media safe-surfing. By establishing policies regarding use of social media and implementing processes to protect their infrastructures from unauthorized use of social media an organization can protect themselves from serious legal and security-related problems. Otherwise their information infrastructure and reputation both will be irreparably damaged [6].

Encryption provides most effective way to maintain integrity and confidentiality of information. Encryption favors data storage and transport but it fundamentally prevents data processing. Therefore, initially it was quite useless to send encrypted data to cloud providers for processing. But this challenge has been met by homomorphic cryptography (HC) which ensures that operations performed on an encrypted text results in an encrypted version of the processed text [29].

GPS positioning devices has favored mobile users for using location based services (LBS). However, LBS raise a privacy issue when mobile users provide private information such as their current location and it becomes even worse if an adversary knows user's some other important information. Location trusted server (LTS) provides solution to this issue [30]. Digital rights management (DRM) provides another issue of privacy. Unstructured digital contents (e.g., video, image, audio, and e-book) have often been pirated and illegally distributed. In order to stop the piracy and illegal distribution of these unstructured digital contents [31] proposed Phosphor, a cloud based mobile digital rights management (DRM) scheme with a sim card in mobile phone. It improves flexibility and reduces the vulnerability of its security at a very low cost. But this approach is basically based on sim card of mobile phone, so it cannot be applied for other kinds of accesses like a laptop using WiFi to access these contents [28].

3) *Malicious Attacks:* All networks are susceptible to one or more malicious attacks. As more as external Web sites are being accessed malicious actors will have more opportunities to access the network and operational data of that organization. Implementing security controls across all Web 2.0 servers and verifying these rigorous security controls can reduce the threats to internal networks and operational data. Additionally, separating Web 2.0 servers from other internal servers may further mitigate the threat of unauthorized access to information through social media tools and Web sites [6]. Some of the potential attack vectors criminals may attempt include:

- Denial of Service (DoS) attacks – It has been argued that a cloud is more susceptible to a DoS attack; because more than one client can access cloud at the same time, which makes DoS attacks much more damaging. Twitter has suffered a devastating DoS attack in 2009.
- 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.
- Authentication attacks – Authentication is one of the weak points in case of hosted and virtual services and is generally been targeted. A user can be authenticated in number of ways and these mechanisms and methods which are used to secure the authentication process are frequently been targeted by the attackers.
- Man-in-the-middle cryptographic attacks – This attack is carried out when an attacker places himself between two users. In this kind of attack attacker places himself in the communication path and after that it is up to him what to do, he can intercept and modify communication [32].

4) *Network Monitoring:* In addition to latency and bandwidth problems network performance monitoring is also an important issue which need proper concern and care. It is critical to have a dynamic cloud performance system that can allow traffic re-routing, access swapping and handover. With all these key challenges given mobile computing is still viable business and is being preferred by more cloud users.

Foreign intelligence services (FIS) have extensive resources and have repeatedly demonstrated their capability to use automated 'social engineering' techniques to mine social media sites. By their very nature, social media sites have an abundance of information, which makes them susceptible to data mining. Our adversaries can use this data to analyze aggregated information. Without adequate network monitoring, an organization cannot ensure that whether users are complying or not its policies regarding the release of high-value information. Additionally, programming languages used in Web 2.0 applications (e.g., Java, Ajax, and the JSON data interchange format) may create other opportunities for malicious actors to access an organization's back-end network infrastructure and do irreparable damage (e.g., access or corrupt data or applications). Consequently, an organization using social media may need to implement increased security controls for any separate sensitive information residing on the server's backend [6].

5) *Compliance and Enforcement:* For now there is no formal set of standards that should be followed for events and policies of cloud computing implementation. But still there are numerous regulations concerning storage and usages of data, including Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, among others. Regular reporting and audit trails are required for many of these regulations. These regulations are needed to be followed completely and appropriately for corporate data to be moved to the cloud. It may be difficult or unrealistic to use public clouds if our data is subjected to legal restrictions or regulatory compliance. We can expect providers to build and certify cloud infrastructures to address the needs of regulated markets.

Achieving certification may be challenging due to the many non-technical factors, including the current state of general cloud knowledge. There are a large number of security threats; it is not possible to implement preventive measures to all of them. When user executes any application and he is aware of the asperity and nature of potential threats to security associated with its use then he can avoid steps that are more susceptible to security attacks. This makes user education and training crucial in safeguarding networks and data. With the advent of social media, training programs are also need to be augmented to address the additional risks posed by social media. This social media training can be incorporated to the annual security training programs of organizations.

Social media tools and sites can be addressed during existing certification and accreditation procedures, thereby helping to ensure that security standards of organization are upheld. Additionally, on the side of organizations they can develop a mentoring program; take advantage of skills of those employees who have more advanced social media skills in training those for whom this technology is unfamiliar [6]. What type of training does the provider offers to their employees is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important item to review.

6) *Incident Response:* Even after implementing best measures for safeguarding data and information and having users trained with best 'safe-surfing' techniques, incidents will inescapably occur. Every cloud provider organization must plan and develop some measures that can be implemented as a quick response and recovery from data spill, misinformation and rumor, or from any malicious attack. Many providers promote their services as being unhackable. But we know it very well that cloud based services are an attractive target to hackers so it's better to anticipate such incidents previously rather than developing and implementing a plan for managing and responding to them after their occurrence. Or we can say that for security concern events prevention is better than cure [6].

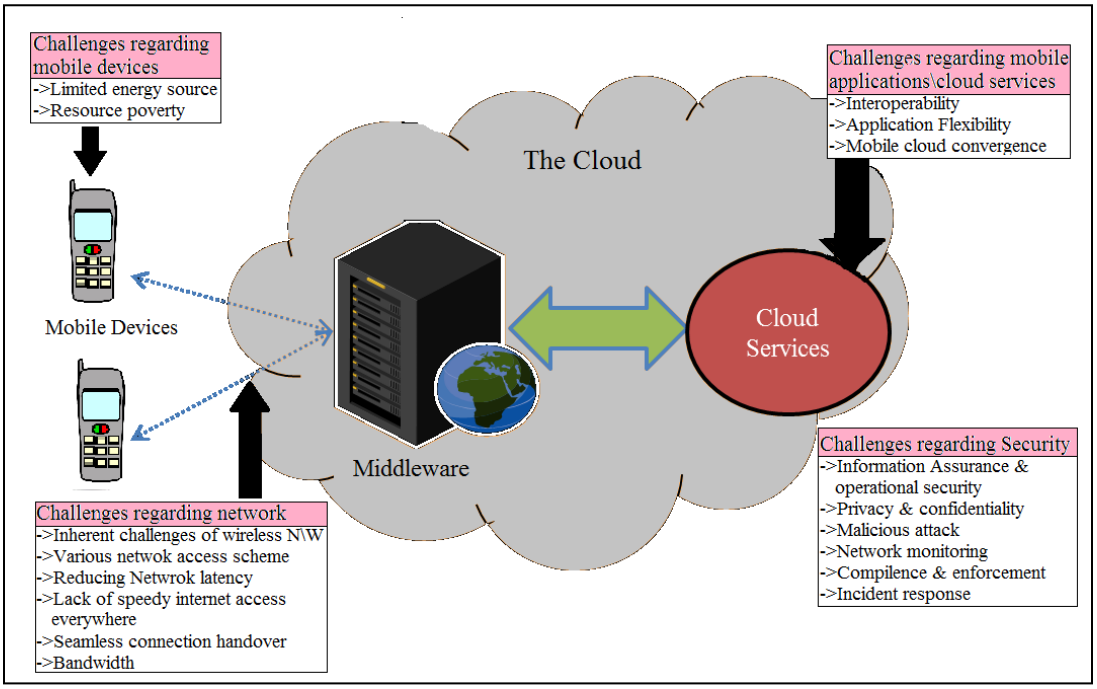

Figure 1. Challenges regarding Implementation of Cloud Computing in Mobile Applications

In case of cloud computing user generally don't have the knowledge of location where our cloud services are physically located. But like all physical locations' they also faces threats such as fire, storms, natural disasters, and loss of power. So it is also an important aspect to take care about these events. How will the cloud provider is going to respond them, and what guarantee of continued services are they promising? [33]

IV. CONCLUSION

Implementation of cloud computing in mobile applications is going to be a trend in the future since it combines the advantages of both mobile computing and cloud computing, thereby providing optimal services for mobile users. According to Recent researches, by the end of 2013 there will be more than 10 thousand mobile applications that will be executed through cloud computing. That traction will push the revenue of mobile cloud computing to $5.2 billion. Here in this paper we have provided an overview of cloud computing its definitions, constituting elements (that are cloud platform and cloud applications) and finally we have discussed about the challenges of implementing cloud computing in mobile applications and their possible solutions.

ACKNOWLEDGMENT

The authors are very thankful to their respected Mr. Aseem Chauhan, Additional President, Amity University, Lucknow, Maj. Gen. K.K. Ohri, AVSM (Retd.), Director General, Amity University, Lucknow, India, for providing excellent computation facilities in the University campus. Authors also pay their regards to Prof. S.T.H. Abidi, Director and Brig. U.K. Chopra, Deputy Director, Amity School of Engineering, Amity University, Lucknow for giving their moral support and help to carry out this research work.

REFERENCES

[1] Divya Narain. 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] IAnewsletter Vol 13 No 2 Spring 2010. 'Cloud Computing: Silver Lining or Storm Ahead' http://iac.dtic.mil/iatac 11

[7] Adrian Otto's Blog. 'What is a Cloud Platform?' http://adrianotto.com/2011/02/cloud-platform/

[8] Resources: Internet Marketing Glossary. http://www.digital-marketing-course.co.nz/resources.php?Glossary-8

[9] Tavis J.Hampton. August 11th, 2011. 'A Quick Guide to Cloud Terminology', http://www.thehostingnews.com/a-quick-guide-to-cloud-terminology.html

[10] "Amazon elastic compute cloud (EC2)." AWS. [Online]. Available: http://www.amazon.com/ec2/

[11] Google app engine. [Online]. Available: http://appengine.google.com/

[12] http://www.force.com/why-force.jsp

[13] Microsoft azure. [Online]. Available: http://www.microsoft.com/azure/

[14] E. Marinelli, "Hyrax: cloud computing on mobile devices using MapReduce", Master thesis, Carnegie Mellon University, 2009.

[15] Fung Po Tso, Lin Cui, Lizhuo Zhang, and Weijia Jia. March 18th, 2011. "Building a Platform to Bridge Low End Mobile Phones and Cloud Computing Services" http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2011Year/no1/articles/201103/t20110318_224547.html

[16] Cloud Computing. October 11th 2008, http://www.reference.com/browse/cloud+computing?s=t

[17] API Dashboard at programmable web. http://www.programmableweb.com/apis#topa-1

[18] Jitendra Maan, '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

[19] *Kyung Mun, Corporate Technology Strategist,* 'Mobile Cloud Computing Challenges', http://www2.alcatel-lucent.com/blogs/techzine/2010/mobile-cloud-computing-challenges/

[20] 10th IEEE/ACIS International conference on computer and information science http://wenku.baidu.com/view/caf74ab9c77da26925c5b033.html

[21] *Irmee Layo. July 11th ,2011, 'Overcoming Challenges in Mobile Cloud Computing',* http://cloudtimes.org/2011/07/11/overcoming-challenges-in-mobile-cloud-computing/

[22] Min Choi · Jonghyuk Park · Young-Sik Jeong © Springer Science+Business Media, LLC 2011, 'Mobile cloud computing framework for a pervasive and ubiquitous environment'

[23] *Colin Steele. October 2011, "BYOD policy",* http://searchconsumerization.techtarget.com/definition/BYOD-policy

[24] *Roger Collings. April 16th , 2011. "*Mobile Cloud Adoption Challenges in the Enterprise"; http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise/

[25] http://www.eweek.com/c/a/Mobile-and-Wireless/BYOD-Policies-Creating-Mobile-Application-Development-Challenges-314028/

[26] *Le Guan, Xu Ke, Meina Song, Junde Song. 2011. 10th IEEE/ACIS International Conference on Computer and Information Science. "A Survey of Research on mobile cloud computing".*

[27] *Roger Collings,* 'Mobile Cloud Adoption Challenges in the Enterprise'; http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise/

[28] "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches". Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/abstract

[29] Peter Schoo, et.al. 'Challenges for Cloud Networking Security', http://www.hpl.hp.com/techreports/2010/HPL-2010-137.pdf

[30] H. Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010.

[31] P. Zou, C. Wang, Z. Liu, and D. Bao, "Phosphor: A Cloud Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, June 2010.

[32] Michael Gregg, 'Security Concerns for Cloud Computing', http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf

[33] Michael Gregg, '10 Security Concerns for Cloud Computing', online available at: http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf

AUTHORS

First Author – Deepti Sahu has completed her M.Tech in Computer Science Engineering from Amity University, Lucknow in 2012 and B.Tech degree from Integral University, Lucknow in 2009. Her area of interest includes Software engineering and Networking. Email ID- md19ip_sahu@yahoo.com

Second Author – Shipra Sharma received M.Tech. in Computer Science Engineering from Amity University Lucknow in 2010. She is a Lecturer in Department of Computer Science Engineering, Amity University, Lucknow. She has guided number projects and thesis in graduate and post-graduate level program. She has produced several national and international publications. Her research interests include Wireless Sensor Network, Software Engineering and Artificial Intelligence.
Email ID- shipra.sharma1510@gmail.com

Third Author – Vandana Dubey received M.Tech. in Computer Science from Amity University, Lucknow in 2010. She is currently working as a Lecturer in Department of Computer Science Engineering, Amity University, Lucknow. Her research interests include Advanced Computer architecture and Computer Organization. Email ID- vandanashuklaec05@gmail.com

Forth Author – Alpika Tripathi received M.Tech. in Computer Science from Amity University Lucknow in 2010. She is currently working as a Lecturer in Department of Computer Science Engineering, Amity University, Lucknow. She has guided number projects and thesis in graduate and post-graduate level program. She has produced several national and international publications. Her research interests include Software Engineering and Data Mining. Email ID- alpika2k@gmail.com

Correspondence Author – Deepti Sahu has completed her M.Tech in Computer Science Engineering from Amity University, Lucknow in 2012 and B.Tech degree from Integral University, Lucknow in 2009. Her area of interest includes Software engineering and Networking. Email ID- md19ip_sahu@yahoo.com