IOSR Journal of Mechanical and Civil Engineering (IOSR-JMCE)
e-ISSN: 2278-1684, p-ISSN: 2320-334X
PP 68-80
www.iosrjournals.org

Mobile cloud computing and security measures

Nasrudeen Sha.M, 1ST yr ME(CSE), Karthik.U, 1ST yr ME(CSE)
VELS University,Chennai. *VELS University,Chennai.*

ABSTRACT:- The Cloud computing for mobile also called as Mobile Cloud Computing (MCC) combines mobile computing and cloud computing, has become one of the industry buzz words and a major discussion thread in the IT world since 2009. As MCC is still at the early stage of development, it is necessary to grasp a thorough understanding of the technology in order to point out the direction of future research. With the latter aim, this paper presents a review on the background of MCC those portraits the essential characteristics, service models and also the deployment models of MCC. It also pictures the architecture and also on how MCC works in terms of client and cloud. This paper outlines the benefits and novel applications of MCC and the issues of MCC are briefly explained in. This paper zeros on the security measures for the MCC too as the main aim and concept of this paper and the limitations of the security designs are also enlightened thereby through this paper.

I. INTRODUCTION

The market of mobile phones has expanded rapidly. The growth of mobility has changed our lives fundamentally in an unprecedented way. According to Cisco IBSG [2], close to 80 percent of the world‟s population has access to the mobile phone and new devices like the iPhone, Android smartphones, palmtops and tablets have brought a host of applications at the palms of people‟s hands. At the same time, Cloud Computing has emerged as a phenomenon that represents the way by which IT services and functionality are charged for and delivered.

Cloud computing for mobile world or, rather, Mobile Cloud Computing (MCC) is a well accepted concept that aims at using cloud computing techniques for storage and processing of data on mobile devices, thereby reducing their limitations.

The end mobile device user will eventually be the benefactor of the Mobile Cloud Computing. Nature of cloud applications also is advantageous for users since they do not need to have very technical hardware to run applications as these computing operations are run within the cloud. This reduces the price of mobile computing to the end users. They could see a huge number of new features enhancing their phones due to Mobile Cloud Computing. At the same time the developers also have real advantages from Mobile Cloud Computing. The largest benefit of cloud computing for developers is access to a broader audience of a wide range of mobile subscribers. Since cloud computing applications go through a browser, the end user‟s mobile operating system does not have any impact on the application.

Along with the plethora of benefits, there are a large number of issues to be addressed and unsolved problems to be solved. Several challenges such as the dependency on continuous network connections, data sharing applications and collaboration, and security Another key challenge for Mobile Cloud Computing is network availability and intermittency. Also Mobile Cloud Computing concepts rely on an always-on connectivity and will need to provide a scalable and high quality mobile access.

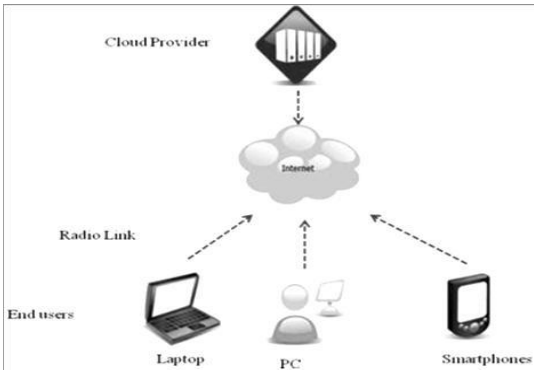

Fig 1 Mobile Cloud Computing Mobile cloud computing and security measures

II. BACKGROUND OF MOBILE CLOUD COMPUTING

The term “mobile cloud computing” was introduced in a short span within the concept “cloud computing” got launched in mid-2007. It has been attracting the attentions of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, of mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost, and of researchers as a promising solution for green IT [3]. This section provides an overview of MCC including definition, architecture, and advantages of MCC.

II. A. Cloud Computing:

In the era of PC, many users found that the PCs they bought 2 years ago cannot keep pace with the development of software nowadays; they need a higher speed CPU, a larger capacity hard disk, and a higher performance Operation System (OS).
That is the magic of ‟Moore‟s Law‟ which urges user upgrading their PCs constantly, but never ever overtaken the development of techniques. Thus, a term called ‟Cloud Computing‟ burst upon our lives.
Cloud Computing has become a popular phrase since 2007. However, there is no consensual definition on what a Cloud Computing or Cloud Computing System is, due to dozens of developers and organizations described it from different perspectives. C. Hewitt [3] introduces that the major function of a cloud computing system is storing data on the cloud servers, and uses of cache memory technology in the client to fetch the data. Those clients can be PCs, laptops, smartphones and so on. R. Buyya [4] gives a definition from the perspective of marking that cloud computing is a parallel and distributed computing system, which is combined by a group of virtual machines with internal links. Such systems dynamically offer computing resources from service providers to customers according to their Service level Agreement (SLA). However, some authors mentioned that cloud computing was not a completely new concept. L. Youseff [5] from UCSB argue that cloud computing is just combined by many existent and few new concepts in many research fields, such as distributed and grid computing, Service-Oriented Architectures (SOA) and in virtualization.

II. B. What is Mobile Cloud Computing?

The Mobile Cloud Computing Forum defines MCC as follows [4]:
“The term Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers”.
Alpena [5] describes MCC as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices.
Alternatively, MCC can be defined as a combination of mobile web and cloud computing [6], [7], which is the most popular tool for mobile users to access applications and services on the Internet. Briefly, MCC provides mobile users with the data processing and storage services in clouds. The mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the complicated computing modules can be processed in the clouds.

II. C. Essential characteristics: The essential characteristics of mobile cloud computing are:

- **On-demand self service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms like mobile phones, laptops, PDAs etc.
- **Resource pooling**: The provider‟s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer does not have control or knowledge over the exact location of the provided

resources. Examples of resources include storage, processing, memory, network bandwidth and virtual machines.

 Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

 Measured Service: Cloud systems automatically control and optimize resources used by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts).

II. D. Service Models: The service models of the mobile cloud computing compromises of

 Software as a Service (SaaS): The capability provided to the consumer is to use the provider‟s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings.

 Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

 Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

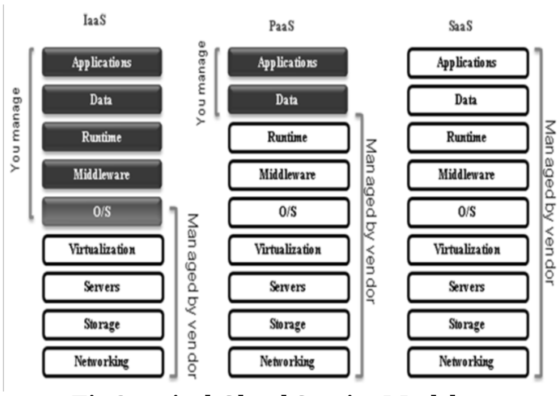

Fig 2 typical Cloud Service Model.

II. D. Deployment Models: The deployment models are the following in mobile cloud computing

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

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

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

 Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Fig 3 below illustrates Public, Private and Hybrid cloud deployment example.

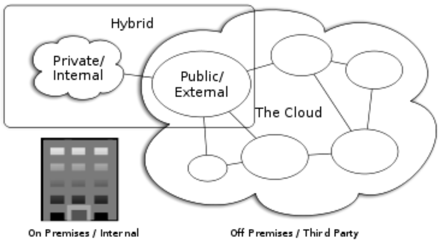

Fig 3 Public, Private and Hybrid Cloud deployment

III. ARCHITECTURES OF MOBILE CLOUD COMPUTING:

From the concept of MCC, the general architecture of MCC can be shown in Fig. 1. In Fig 5, mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Mobile users‟ requests and information (e.g., ID and location) are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers‟ data stored in databases.

After that, the subscribers‟ requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and service-oriented architecture (e.g., web, application, and database servers).

The details of cloud architecture could be different in different contexts. For example, four- layer architecture is explained in [8] to compare cloud computing with grid computing. Alternatively, service oriented architecture, called Aneka, and is introduced to enable developers to build .NET applications with the supports of application programming interfaces (APIs) and multiple programming models [9]. [10] Presents architecture for creating market-oriented clouds, and [11] proposes an architecture for web delivered business services. In this paper, we focus on a layered architecture of cloud computing (Fig. 4).

This architecture is commonly used to demonstrate the effectiveness of the cloud computing model in terms of meeting the user‟s requirements [12].

Software as a Service (Microsoft‟s Live Mesh)
Platform as a Service (e.g., Google App engine, Microsoft Azure)
Infrastructure as a Service (e.g., EC2,S3)
Data centers

Fig. 4 Service-oriented cloud computing architecture.

Generally, a cloud computing is a large- scale distributed network system implemented based on a number of servers in data centers. The cloud services are generally classified based on a layer concept (Fig. 4). In the upper layers of this paradigm, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are stacked.

 Data centers layer: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high-speed networks to provide services for customers. Typically, data centers are built in less populated places, with high power supply stability and a low risk of disaster.

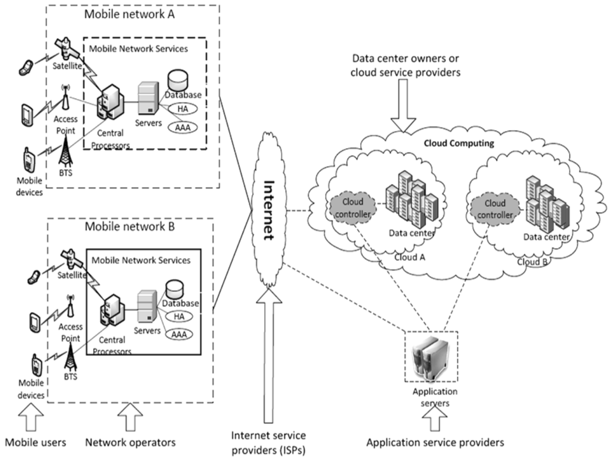

Fig. 5 Mobile Cloud Computing (MCC) architecture

IV. HOW MOBILE CLOUD COMPUTING WORKS

IV. A. Concept and principle: Similar with Cloud Computing, there are a lot but no consensual definitions on what mobile cloud computing is. In this paper, we consider it is a novel computing mode consisting of mobile computing and cloud computing, which provide cloud based services to users through the Internet and mobile devices.

On one hand, the mobile cloud computing is a development of mobile computing, and an extension to cloud computing. In mobile cloud computing, the previous mobile device-based intensive computing, data storage and mass information processing have been transferred to

‟cloud‟ and thus the requirements of mobile devices in computing capability and resources have been reduced, so the developing, running, deploying and using mode of mobile applications have been totally changed. On the other hand, the terminals which people used to access and acquire cloud services are suitable for mobile devices like smartphone, PDA, Tablet, and iPad but not restricted to fixed devices (such as PC), which reflects the advantages and original intention of cloud computing.

Therefore, from both aspects of mobile computing and cloud computing, the mobile cloud computing is a combination of the two technologies, a development of distributed, grid and centralized algorithms, and have broad prospects for application.

As shown is the Fig. 6, mobile cloud computing can be simply divided into cloud computing and mobile computing. Those mobile devices can be laptops, PDA, smartphones, and so on, which connects with a hotspot or base station by 3G, WIFI, or GPRS. As the computing and major data processing phases have been migrated to

‟cloud‟, the capability requirement of mobile devices is limited, some low-cost mobile devices or even non-smartphones can also achieve mobile cloud computing by using a cross-platform mid- ware. Although the client in mobile cloud computing is changed from PCs or fixed machines to mobile devices, the main concept is still cloud computing. Mobile users send service requests to the cloud through a web browser or desktop application, then the management component of cloud allocates resources to the request to establish connection, while the monitoring and calculating functions of mobile cloud computing will be implemented to ensure the QoS until the connection is completed.

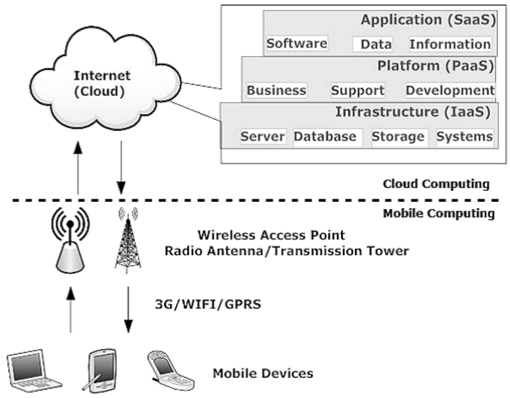

Fig. 6 Mobile Cloud Computing

IV. B. Typical services needed by a mobile cloud client: The most essential services include

 Sync: This service synchronizes all state changes made to the mobile or its applications back with the Cloud Server.

 Push: It manages any state updates being sent as a notification from the cloud server. This improves the user‟s experience as it does not require the user to proactively check for new information.

 Offline App: It is a service which carries the management capabilities to create smart coordination between low level services like Sync and Push. It frees the programmer from the burden of writing code to actually perform synchronization as it is this service which decides synchronization management and mechanism which is best for the current state. The moment the data channel for any mobile application is established, all synchronizations and push notifications are automatically handled by Offline App service.

 Network: It manages the communication channel needed to receive Push notifications from the server. It carries the ability to establish proper connections automatically. It is a very low-level service and it shields any low level connection establishment, security protocol details by providing a high level interfacing framework.

 Database: It manages the local data storage for the mobile applications. Depending on the platform it uses the corresponding storage facilities. It must support storage among the various mobile applications and must ensure thread safe concurrent access. Just like Network service it is also a low- level service.

 Inter App Bus: This service provides low- level coordination/ communication between the suites of applications installed on the device.

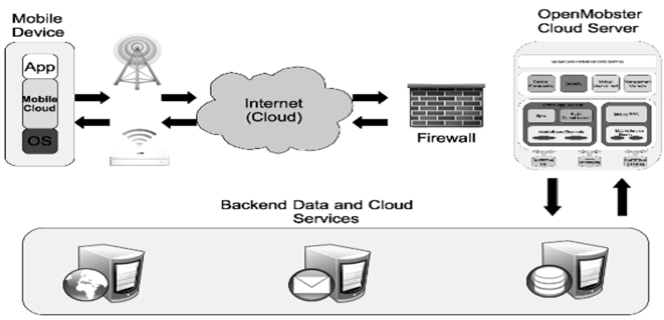

Fig. 7[5] the open mobster architecture for MCC

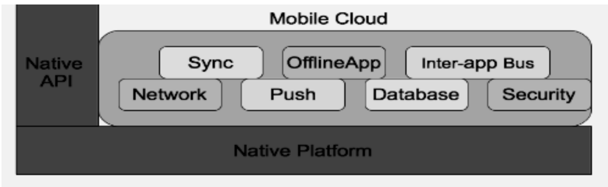

Fig. 8 [5] Client cloud stack

IV. A. Typical services needed by a mobile cloud server: These are the essential services that must be provided to the mobile apps by the server.

- **Sync:** Server Sync service synchronizes device side App state changes with the backend services where the data actually originates. It also must provide a plug-in framework to mobilize the backend data.
- **Push:** Server Push service monitors data channels (from backend) for updates. The moment updates are detected, corresponding notifications are sent back to the device.

If the device is out of coverage or disconnected for some reason, it waits in a queue, and delivers the push the moment the device connects back to the network.

- **Secure Socket-Based Data Service:** Depending on the security requirements of the Apps this server side service must provide plain socket server or a SSL-based socket server or both.
- **Security:** Security component provides authentication and authorization services to make sure mobile devices connecting to the Cloud Server are in fact allowed to access the system. Every device must be first securely provisioned with the system before it can be used. After the device is registered, it is challenged for proper credentials when the device itself needs to be activated. Once the device is activated, all Cloud requests are properly authenticated/authorized going
- **Management Console:** Every instance of a Cloud Server must have a Command Line application such as the

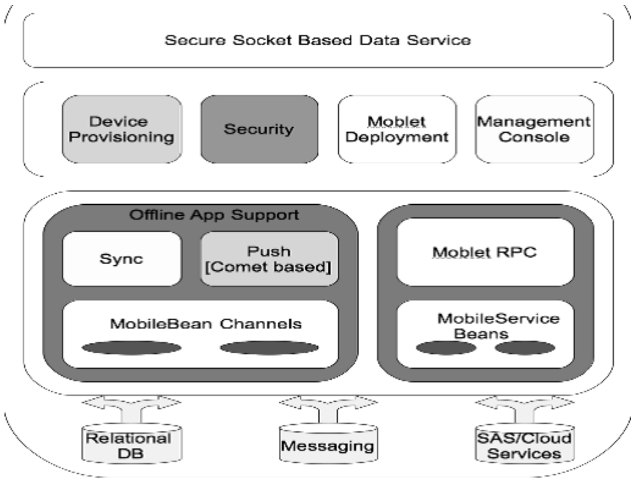

Fig. 9 [5] Mobile server cloud stack

Management Console as it provides user and device provisioning functionalities. In the future, this same component will have more device management features like remote data wipe, remote locking, remote tracking, etc.

V. Benefits of mobile cloud computing:

Mobile cloud applications move the
computing power and data storage away from mobile phones and into the cloud, bringing apps and mobile computing to not just smartphone users but a much broader range of mobile subscribers. In this section, we enlist the possible benefits of Mobile Cloud Computing.

- Mobile Cloud Computing will help to overcome limitations of mobile devices in particular of the processing power and data storage.

 It also might help to extend the battery life by moving the execution of commutation-intensive application „to the cloud‟.
 Mobile Cloud Computing is also seen as a potential solution for the fragmented market of mobile operating systems with currently eight major operating systems.
 Mobile Cloud Computing can increase security level for mobile devices achieved by a centralized monitoring and maintenance of software.
 It can also become a one-stop shopping option for users of mobile devices since Mobile Cloud Operators can simultaneously act as virtual network operators, provide e-payment services, and provide software, data storage, etc. as a service.
 A number of new technical functionalities might be provided by mobile clouds. In particular, provisioning of context- and location-awareness enables personalization of services is an attractive functionality.
 Mobile Cloud Computing might open the cloud computing business that is currently almost exclusively addressing businesses to consumers since they will significantly benefit from the above described options.

VI. Novel application models for MCC:
 Augmented Execution: Augmented execution refers to a technique used to overcome
the limitations of smartphones in terms of computation, memory and battery. Chun and Maniatis [14] propose an architecture that addresses these challenges via seamlessly
offloading execution from the phone to computational infrastructure (cloud) where cloned replica of the smart phone‟s software is running.
The mobile phone hosts its computation and memory demanding applications.

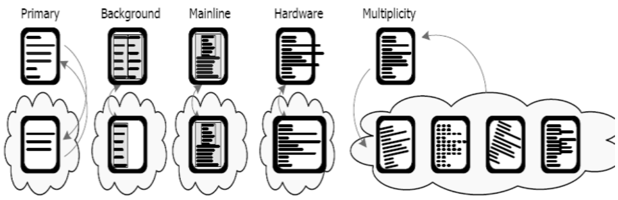

Fig 10 Clone Cloud categories for augmented execution

 Elastic Partitioned / Modularized Applications: Running applications in heterogeneous changing environments like mobile clouds requires dynamic partitioning of applications and remote execution of some components. Applications can improve their performance by delegating part of the application to remote execution on a resource-rich cloud infrastructure.
 Application Mobility: The mobile cloud is accessed through heterogeneous devices. In order to provide seamless user experience same applications need to run on different devices. The application mobility plays a crucial role in enabling the next generation mobile applications.
 Ad-hoc Mobile Clouds: An ad-hoc computing cloud represents a group of mobile devices that serve as a cloud computing provider by exposing their computing resources to other mobile devices. This type of mobile cloud computing becomes more interesting in situations with no or weak connections to the Internet and large cloud providers. Offloading to nearby mobile devices

save monetary cost, because data charging is avoided, especially favored in roaming situations. Moreover, it allows creating computing communities in which users can collaboratively execute shared tasks.

VII. ISSUES AND APPROACHES OF MCC:

As discussed in the previous section, MCC has many advantages for mobile users and service providers. However, because of the integration of two different fields, i.e., cloud computing and mobile networks, MCC has to face many technical challenges. This section lists several research issues in MCC, which are related to the mobile communication and cloud computing. Then, the available solutions to address these issues are reviewed.

VII. A. ISSUES IN MOBILE COMMUNICATION SIDE

 Low Bandwidth: Bandwidth is one of the big issues in MCC since the radio resource for wireless networks is much scarce as compared with the traditional wired networks proposes a solution to share the limited bandwidth among mobile users who are located in the same area (e.g., a workplace, a station, and a stadium) and involved in the same content (e.g., a video file). The authors model the interaction among the users as a coalitional game.

For example, the users form a coalition where each member is responsible for a part of video files (e.g., sounds, images, and captions) and transmits/exchanges it to other coalition members.

This results in the improvement of the video quality. However, the proposed solution is only applied in the case when the users in a certain area are interested in the same contents. Also, it does not consider a distribution policy (e.g., who receives how much and which part of contents) which leads to a lack of fairness about each user‟s contribution to a coalition considers the data distribution policy

which determines when and how much portions of available bandwidth are shared among users from which networks (e.g., Wi Fi and Wi MAX). It collects user profiles (e.g., calling profile, signal strength profile, and power profile) periodically and creates decision tables by using Markov Decision Process (MDP) algorithm. Based on the tables, the users decide whether or not to help other users download some contents that they cannot receive by themselves due to the bandwidth limitation, and how much it should help (e.g., 10% of contents). The authors build a framework, named RACE (Resource-Aware Collaborative Execution), on the cloud to take advantages of the computing resources for maintaining the user profiles. This approach is suitable for users who share the limited bandwidth, to balance the trade-off between benefits of the assistance and energy costs.

 Availability: Service availability becomes more important issue in MCC than that in the cloud computing with wired networks. Mobile users may not be able to connect to the cloud to obtain service due to traffic congestion, network failures, and the out-of-signal. After detecting nearby nodes that are in a stable mode, the target provider for the application is changed. In this way, instead of having a link directly to the cloud, mobile user can connect to the cloud through neighboring nodes in an ad hoc manner. However, it does not consider the mobility, capability of devices, and privacy of neighboring nodes.

According to the messages, each node maintains a neighboring node list and a content list and estimates role levels of other nodes based on the disk space, bandwidth, and power supply. Then, the nodes with the shortest hop length path and the highest role level are selected as the intermediate nodes to receive contents. Besides, the authors also consider security issues for mobile clients when they share information by using account key (to authenticate and encrypt the private content), friend key (to secure channel between two friends), and content key (to protect an access control). Two applications are introduced, i.e., Wi Face and Wi Market that are two co-located social networking.

This approach is much more efficient than the current social networking systems, especially in the event of disconnection.

 Heterogeneity: MCC will be used in the highly heterogeneous networks in terms of wireless network interfaces. Different mobile nodes access to the cloud through different radio access technologies such as WCDMA, GPRS, Wi MAX, CDMA2000, and WLAN.

As a result, an issue of how to handle the wireless connectivity by satisfying MCC‟s requirements arises. (e.g., always-on connectivity, on-demand scalability of wireless connectivity, and the energy efficiency of mobile devices)

This architecture is built based on a concept of Intelligent Radio Network Access (IRNA [68]). IRNA is an effective model to deal with the dynamics and heterogeneity of available access networks. As shown in Fig. 10, this architecture consists of three main components: context provider, context broker, and context consumer. In this architecture, when a context consumer wants to communicate with a context provider, the context consumer will request the URI (Uniform Resource Identifier) of context providers at the context broker. Using this URI, the context consumer can communicate directly to the context provider and request the context data. Hence, this process increases the speed of context data delivery.
Therefore, this architecture enables controlling context quality according to the demands of the context consumers.

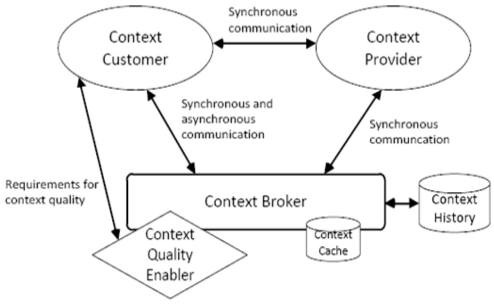

Fig 11 Context management architecture

VII. B. Issues in Computing Side

 Computing Offloading: As explained in the previous section, offloading is one of the main features of MCC to improve the batteries lifetime for the mobile devices and to increase the performance of applications. However, there are many related issues including efficient and dynamic offloading under environment changes.

a) **Offloading in the static environment**: Experiments in show that offloading is not always the effective way to save energy. For a code compilation, offloading might consume more energy than that of local processing when the size of codes is small. For example, when the size of altered codes after compilation is 500KB, offloading consumes about 5% of a device‟s battery for its communication while the local processing consumes about 10% of the battery for its computation. In this case, the offloading can save the battery up to 50%. However, when the size of altered codes is 250KB, the efficiency reduces to 30%. When the size of altered codes is small, the offloading consumes more battery than that of local processing.

b) **Offloading in the Dynamic Environment**: This subsection introduces a few approaches to deal with offloading in a dynamic network environment (e.g., changing connection status and bandwidth). The environment changes can cause additional problems. For example, the transmitted data may not reach the destination, or the data executed on the server will be lost when it has to be returned to the sender.

VIII. LEVERAGING PEER MOBILE DEVICES

It has been demonstrated [12, 16] that one can leverage peer mobile devices to perform cloud computing functions. A system called Misco [16], a version of Map Reduce, can be handled by a "server farm" comprised of 20-odd Nokia N95 smartphones. The choice of using peer mobile devices for the cloud computing technique causes many other hurdles. The security, trust, privacy issue is even greater. There is also the incentive issue.

IX. SECURITY

Protecting user privacy and data/application secrecy from adversary is a key to establish and maintain consumers‟ trust in the mobile platform, especially in MCC. In the following, the security related issues in MCC are introduced in two categories: the security for mobile users and the security for data. Also, some solutions to address these issues are reviewed.

A) Security for Mobile Users: Mobile devices such as cellular phone, PDA, and smartphone are exposed to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses) and their vulnerability. In addition, with mobile phones integrated global positioning system (GPS) device, they can cause privacy issues for subscribers. Two main issues are as follows.

 Security for mobile applications: Installing and running security software‟s such as Kaspersky, McAfee, and AVG antivirus programs on mobile devices are the simplest ways to detect security threats (e.g., virus, worms, and malicious codes) on the devices. However, mobile devices are constrained in their processing and power, protecting them from the threats is more difficult than that for resourceful device (e.g., PC). For example, it is impossible to keep running the virus detection software on mobile devices.

 Privacy: With the advantages of GPS positioning devices, the number of mobile users using the location based services (LBS) increases. However, the LBS face a privacy issue when mobile users provide private information such as their current location. This problem becomes even worse if an adversary knows user‟s important information. Location trusted server (LTS) [86] is presented to address this issue.

 Most of the mobile devices (especially the smartphones) have almost all the functionalities of a standard desktop computer which poses the same security threats to mobile devices. To combat the security threats, current mobile devices run the threat detection services on the mobile device itself. A possible solution is to come with a new model of security where detection services can be moved to cloud. It significantly saves the device CPU and memory requirements. Such an approach has several benefits:

 Better detection of malicious software
 Reduce on-device Resources consumption
 Reduce on-device Software complexity

They propose an architecture containing three components:

 Host agent: It is a light weight process that runs on each device and inspects the file activity on the system. It has a cache where it stores the unique identifier (such as hash) for files received. Whenever a new file whose file identifier is not available in the cache, it will be send to the Network Service.

 Network Service: This service analyses the files send to it by the host agent. There can be multiple instance of Network Service running on the cloud using virtualization; hence supports parallel detection of multiple files send by
many Host agents.

 Caching: There are two types of cache:
 Local private cache is on the device where the host agent can put the identifier of inspected files.
 Global shared cache resides on the Network Service which contains the identifiers of all inspected files received so far.

Apart from the anti-virus service provided, Mobile Cloud Computing platform must also address other mobile specific issues like:

- SMS Spam filtering
- Phishing Detection
- Centralized Blacklisted

B) Securing Data on Clouds: Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication, and digital rights. The data-related issues in MCC are as follows.

- **Integrity:** Mobile users often concern about their data integrity on the cloud. Several solutions are proposed to address this issue. However, such solutions do not take the energy consumption of mobile users into account. The scheme performs three phases: the initialization, the update, and the verification.
- **Digital rights management:** The unstructured digital contents (e.g., video, image, audio, and e-book) have often been pirated and illegally distributed. Protecting these contents from illegal access is of crucial importance to the content providers in MCC like traditional cloud computing and peer-to-peer networks.
- **Enhancing the Efficiency of Data Access:** With an increasing number of cloud services, the demand of accessing data resources (e.g., image, files, and documents) on the cloud increases. As a result, a method to deal with (i.e., store, manage, and access) data resources on clouds becomes a significant challenge. However, handling the data resources on clouds is not an easy problem due to the low bandwidth, mobility, and the limitation of resource capacity of mobile devices.
- **Context-aware mobile cloud services:** It is important for the service provider to fulfill mobile users‟ satisfaction by monitoring their preferences and providing appropriate services to each of the users. A lot of research work try to utilize the local contexts (e.g., data types, network status, device environments, and user preferences) to improve the quality of service (QoS).

Mobile Service Clouds (MSCs), which is extended from Service Clouds Paradigm, is a model when a customer uses a service on the cloud, the user‟s request firstly goes to a service gateway. The gateway will choose an appropriate primary proxy to meet the requirements (e.g., the shortest way and minimum round-trip time) and then sends the result to the user. The advantages of this model are that the model addresses the disconnection issue and can maintain the QoS at an acceptable level.

X. LIMITATIONS OF SECURITY DESIGN

Following are the limitations of this securitydesign.

- Disconnected operation Due to network situations a mobile agent may not be able to effectively utilize network Fig. 6. [10] Mobile Agent Based Open Cloud Computing Federation mechanism based security services. This causes the mobile devices to be disconnected.
- Privacy Sensitive user files are collected by organizations which host such services.

XII. CONCLUSION

With the high increasing of data computation in commerce and science, the capacity of data processing has been considered as a strategic resource in many countries. Mobile cloud computing (MCC), as a development and extension of mobile computing (MC) and cloud computing (CC), has inherited the high mobility and scalability, and become a hot research topic in recent years.

According to ABI Research [7], “By 2015, more than 240 million business customers will be leveraging cloud computing services through mobile devices, driving revenues of $5.2 billion”, While it must be noted that there were only 42.8 million Mobile Cloud Computing subscribers in 2008. This underlines the importance of cloud computing for mobile. With this importance, with the future further techniques all the incorporated security issues are to be eliminated and thereby providing a secured, reliable and much efficient mobile cloud computing technique.

REFERENCES

[1]. http://www.idc.com
[2]. IBSG Cisco, “Mobile Consumers reach for the Cloud”
[3]. Peter Mell, Tim Grance, “The NIST definition of Cloud Computing”, v15.
[4]. Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi, “Cloud Computing – The business

perspective", Decision Support Systems [5]R. Buyya, C. Yeo and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," in10th IEEE International Conference
[5]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,"
[6]. G.H Forman and J.Zahorjan, "The Challenges of Mobile Computing," IEEE Computer Society Magazine, vol. 27, Issue 4, Pages: 38-47, 1994
[7]. X. Gu, K. Nahrstedt, A. Messer, I. Greenberg, and D. Milojicic, "Adaptive Offloading Inference for Delivering Applications in Pervasive Computing Environments," in Proceedings of the First IEEE International Conference
[8]. B.-G. Chun and P. Maniatis, "Augmented Smartphone
[9]. Applications Through Clone Cloud Execution," in Proceedings of the 12th Workshop on Hot Topics in Operating Systems (Hot OS XII).
[10]. A. Wright, "Get Smart," Communications of the ACM,
[11]. vol. 52, no. 1, pp. 15–16, 2009.
[12]. On Live Inc., "On LIve." http://www.onlive.com
[13]. Amazon.com, Inc., "Amazon Web Services." http://aws.amazon.com OpnMobstr,http://code.google.com/p/openmobster/.
[14]. ABI Research. http://www.abiresearch.com/. 2010.
[15]. R. Kakerow, "Low power design methodologies for mobile communication," in Proceedings of IEEE International Conference on Computer Design: VLSI in Computers and Processors, pp. 8, January 2003.
[16]. L. D. Paulson, "Low-Power Chips for High-Powered
[17]. Handhelds," IEEE Computer Society Magazine, vol. 36, no.
[18]. 1, pp. 21, January 2003.
[19]. J. W. Davis, "Power benchmark strategy for systems employing power management," in Proceedings of the IEEE International Symposium on Electronics and the Environment, pp. 117, August 2002.