****

**SYSC5801**

**ADVANCED NETWORK ROUTING TECHNOLOGIES**

**PROJECT REPORT**

**(SECURE MOBILE CLOUD COMPUTING)**

**SUBMITTED TO:-**

**CHUNG-HORNG LUNG**

**(INSTRUCTOR)**

**SUBMITTED BY:-**

**MANDEEP SINGH (100872459)**

**SIDHANT SHARMA (100875655)**

**Contents**

* Security

1. Security for mobile user
2. Security for mobile applications
3. Privacy
4. Securing data on cloud
5. Data integrity
6. Authentication

* Handover

1. Handover latency
2. Fast handover for mobile IPv6

* Cloudlets

1. Introduction
2. Transient cloudlet customization
3. Difference between cloudlet and cloud

* Conclusion

**Abstract**

Mobile cloud computing is simply the integration of cloud computing on mobile devices. By the definition of cloud computing we understand that it is the process of providing services like data storage or processing of data to the clients over the internet. Mobile cloud computing is simply cloud computing in which some of the devices are mobile. This technology can be used to overcome various limitation of mobile computing like battery life, storage, network availability and security issues. This report focuses on the overview of mobile cloud computing, its definition, the architecture, challenges regarding mobile cloud computing and the possible solutions to the issues. The two main areas of research are the bandwidth management and the security. Also the quality of service and quality of experience regarding mobile cloud computing is discussed.

1. **Introduction**

The importance of mobile devices in our daily life is well known to all of us. We are constantly in contact with each other with the help of mobile phones. With the development of multimedia devices by companies such are apple and google more graphic rich devices are being introduced which utilize applications such as mail, chat and other resource intensive applications which are provided to the end user over the wireless network. Thus mobile computing is a hot trend in industries and in the field of IT. However research and development of mobile device is limited due to constraints such as limited battery life, size and weight of the device and the data storage capability. Due to this the end user is not able to receive the best service possible.

With the advent of mobile cloud computing, various issues regarding mobile development can be eliminated by providing storage and bandwidth management over the internet and partitioning the resource intensive applications over the internet or cloud as we may call it and that too at a low cost.According to ABI Research, “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.

Mobile cloud computing will also be beneficial to the developers as the current scenario is that developers have to write separate codes for application for different platforms such as ios and android. But with the help of mobile cloud computing the developers will be able to address a large group of users as application will be made available through browser and all the devices with suitable browser will be able to run the same application.

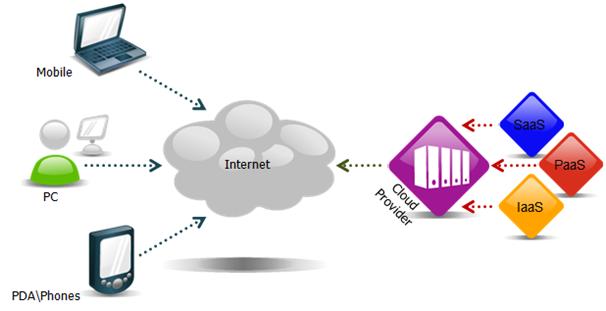
This report provides a survey on mobile cloud computing. Section 2 provides the overview of mobile cloud computing. How it works and the architecture and its various uses in different fields. Section 3 explains the various issues regarding mobile cloud computing and their possible solutions. Section 4 provides the concept of quality of experience and how it is applied to mobile cloud computing. Finally we summarize the report with the conclusion and some future research proposals.

**2. Overview of mobile cloud computing**

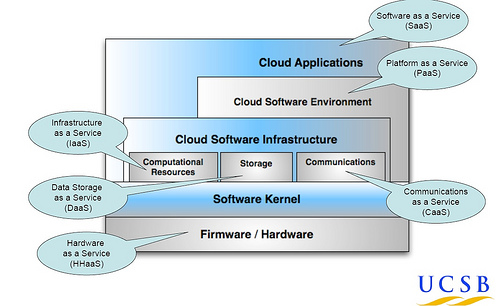
**i. What is mobile cloud computing:**

By the definition Mobile cloud computing is a combination between **mobile network** and **cloud computing**, thereby providing optimal services for mobile users. In mobile cloud computing, mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the clouds. Thus mobile computing and applications are not limited to just high end multimedia devices but is made available to a wide group of users. With the help of mobile cloud computing resource intensive applications such as data processing and storage are moved from mobile devices to servers which are located over the internet and are much more powerful than mobile devices and the results are transferred back to the mobile devices over the wireless network with the help of suitable browsers. Thus mobile cloud computing greatly enhances the research and development of mobile devices.

**ii. a. Architecture**:––



Mobile cloud computing in the simplest form can be explained with the above architecture. The mobile users are connected to the internet over the wireless network and the services are provided to them over the internet by cloud providers. These services include Saas, Paas, Iaas. The architecture based on these services is used to demonstrate the effectiveness of cloud computing in terms of user experience.



The cloud services are generally classified based on a layer concept based on virtualization.Virtualisation allows you to install an operating system on a generic layer overlaying the hardware. The various layers of this model are explained as follows:

**i. Data centre or hardware layer**: this layer provides the infrastructure and the necessary hardware for the cloud. In this layer the servers are linked with high speed networks to provide services to the users.

**ii.Infrastructure** as a service: it offers an alternative to the companies purchasing servers, hardware, data centre space or network equipment. With the help of IaaS these services are outsourced to the companies so that the companies have to spend less money on them. As a result instead of deploying physical machines, the companies get access to virtual servers on which they deploy their own software. This reduces the risk as the companies do not have to look after the maintenance of the machines and the service is based on pay as you go model so that huge investment is not required.

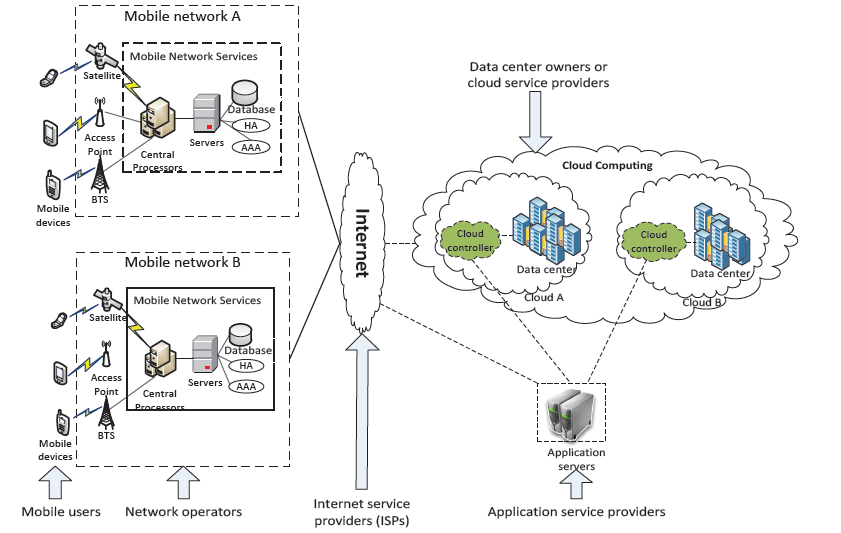
The various subcategories of IaaS are:

1. HaaS: hardware as a service.
2. SaaS: storage as a service.
3. DaaS: desktop as a service.
4. CaaS: communication as a service.

**iii.Platform** as a service: this service provides facilities for construction and delivery of web based applications available through the internet without the need for special installation of a software or infrastructure. PaaS offers advanced integrated environment for building, testing and deploying custom applications. It provides services such as application framework and development tools.

**iv.Software** as a service: this service is concerned with the end users as the application is delivered from the internet to the end user.SaaS continues the cloud paradigm of low-cost, off-premise systems i.e no need for infrastructure and on-demand, pay-per-use models, while further eliminating development costs and lag time.

b. The MCC architecture can also be explained in an alternate way:



This architecture explains how the mobile cloud computing works. The mobile users or the mobile devices are connected to the mobile networks through base transceiver stations or through satellite links. When the user requests the service, the request is sent to the servers through the central processors where the user is granted authentication and other services according to the specific accounts. From the servers the user is connected to the cloud through wireless connection or the internet where the user is provided with the requested service by the content providers or the cloud controllers.

**iii.Advantages of mobile cloud computing**:

With the help of mobile cloud computing the various limitation of mobile development can be eliminated such as limited battery life, limited storage, bandwidth management, processing power and limited availability.

The battery life of the devices can be managed by careful scheduling of tasks and partitioning of resource intensive process to the remote servers so that the very less power of the device is consumed and the results are available quickly. Tasks such as background virus check and video indexing can be performed on remote machines and the results are sent to the device over the internet.

Similarly the storage problem in mobile device can be solved by storing the data over the cloud. There are several companies that offer data storage on their own servers so that the mobile memory is not utilized. This also helps in securing the data as it is backed up on separate computers. Thus cloud computing also helps in improving reliability.

The problem of limited availability can be solved with the help of various techniques like cloud servers and languages such as html5 which can help in offline storage so that the service can be provided to the user even in the case of network failure.

**iv.Uses of mobile cloud computing:**

There are various uses of mobile cloud computing in our daily life. A few common applications of mobile cloud computing are discussed below.

1. Mobile commerce: this is by far the most widely accepted application of mobile cloud computing. It includes mobile banking i.e making transactions, paying bills etc. Mobile shopping which is a new trend which includes buying goods on the internet. The ease of access and less capital investment makes it even more attractive trend.
2. Mobile learning: an example of mobile learning can be taken from the company Educomp solutions. This company provides services to the schools in form of hardware and software. They setup up their equipment and the educational content is delivered through their servers in the form of powerpoint slide show or videos in the classrooms equipped with video projectors. The same can be applied to mobile devices as the content can be delivered through the internet on an on demand basis.
3. Mobile healthcare: the healthcare facilities can be provided to mobile users by uploading each users database over the internet and monitoring their health conditions accordingly. First aid techniques and hospital information can be made available over the internet on an on demand basis.
4. Mobile entertainment: This area is also another fast growing trend in mobile computing. Services such as mobile gaming, video streaming and data storage can be greatly improved with the help of mobile cloud computing. Graphic rich games can be played on any device as the processing is done over the internet. Also social networking is a hot trend and cloud computing helps in improving the user experience even further as video sharing and image tagging is made easy. Also users are able to share real time experience over the cloud with each other.

**3. Issues regarding mobile cloud computing**

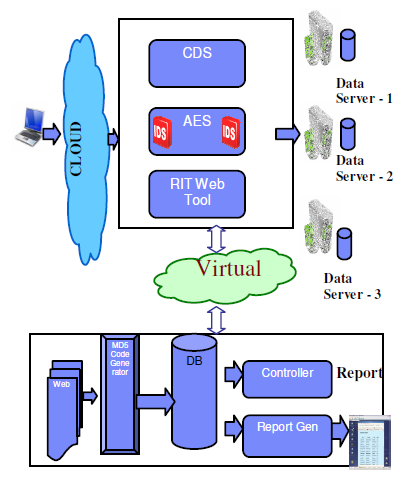
As mobile cloud computing is the integration of cloud computing with mobile computing, so the challenges faced by cloud computing are also faced by mobile cloud computing. We will discuss the issues of bandwidth management and security in this report and the possible solutions to these problems.

1. **Bandwidth management:**

In case of mobile computing, network availability is one of the biggest problems faced by the service providers and the end users. The mobile technology assumes a shared bandwidth capacity i.e. users in a particular cell share the limited amount of bandwidth with each other. The greater number of users will result in even lesser bandwidth availability to each user. Thus to overcome the bandwidth limitation several methods have been proposed. The two main technologies are use of cloud servers for online storage of data and the use the programming language such as html5 for offline storage.

**a) Cloud servers**: The concept of cloud server is based on virtualization. Virtualization allows you to install an operating system on a generic layer overlaying the hardware. Cloud servers are different from physical server in a way that cloud servers are actually software over the internet. These can be launched on an on demand basis and has no physical limitation and can be discarded at any moment. Also cloud servers are dynamic in nature. They can be configured at any time by adding modifications such as memory or processing power.

The advantage of cloud server is that it has very low downtime and in the case of network failure the signal is restored very quickly. As the cloud servers are deployed over the internet so the backed up data can be accessed from anywhere. As there is no investment needed for hardware deployment of these servers hence this technology is widely accepted by small business groups and other small companies to expand their business.With the help of data storage over the cloud, the back and forth movement of data between the end user and the dedicated server is highly reduced and hence the bandwidth is properly utilized. The architecture of cloud server can be explained in the following way.



In the above architecture when a request is generated by the user, the server holds the request and connects to the virtual controller which approves the request according to the agreement protocol and the requested service is provided to the user. The virtual controller is used to monitor the web server and look for any sort of failure. In case of network failure it generates an alarm to the administrator. The controller follows certain protocols such a timely check of each request and monitoring of web servers after particular time. Maintaining log of the number of failure and following remedy procedure.

The hash code generator generates a 32 digit hexadecimal code which is used for authentication of the request. The working can be explained with the following algorithm

1. CDS reads the http request

2. Holds the request and disconnects the cloud.

3. Controller is connected with the CDS.

4. CDS checks the Hash Code, Generated by the controller for sub server 1 along with the already stored hash code in the database.

5. If a Match Occurs, Then the controller is disconnected and http response is sent to the user by connecting to the cloud

6. If Match fails then step 4 is repeated for sub server 2, and the controller starts replacing the affected file with the original file

7. If Match fails then step 4 is repeated for sub server 3, and the controller starts replacing the affected file with the original file

8. If Match fails then System is rebooted

The purpose of AES algorithm is to ensure the security of the hash code. The DBM monitors the activity of the virtual controller and performs the following activities such as monitoring the http request, the date and time of request, the type of content requested and the reliability of the server and alarm generation in case of network failure. The cloud data server is implemented using java and My SQL.

**Sl No Name of the Web page Persistent service Availability (Rank Correlation )**

**Average Delay Time Average Speed**

**1** Cloud Data Server 45 13

**2** Http Web Server 93 27

**3** Java Web Server 102 31

By comparing the cloud server results with other standard servers it is clear that cloud servers takes less time and provides better service than other servers.

**b) HTML5**:

HTML5 can be used for its data caching technique to improve the bandwidth utilization in mobile cloud computing. But let us first understand what HTML5 is. HTML5 is an update to the programming language HTML that is used to add new features to websites and for web application development. HTML5 can be used to add audio and video to the website, drawing stuff on the website and to drag and drop stuff to the website. The most important feature of this language in case of mobile cloud computing is the application caching. With the use of certain technologies such as web worker, webGL and geolocation the application cache allows mobile web application to run even in the case of network failure.

There are primarily two offline capabilities in HTML5: application caching and offline storage (or "client-side storage").Application caching involves saving the application's core logic and user-interface. Offline storage is about capturing specific data generated by the user, or resources the user has expressed interest in. To explain the two types of caching we can take an example of a video game. When we install a game into our computer from a cd it loads all the files directly into the hard disk of the computer like frequently used images, videos, maps, video and audio files so that the next time the user wants to play the game it would, load up quickly. This is purpose of application caching in case of HTML5. The other case is when the user wants to play the game again and start from the point where he left the game the last time. Like the player health, the current map and the state of the surrounding object. This cannot be done on the application cache as it is user specific, hence offline storage is used in this case.

The HTML code for offline application caching can be explained as follows.

The mechanism for ensuring Web applications are available even when the user is not connected to their network is the manifest attribute on the html element.

The attribute takes a URI to a manifest, which specifies which files are to be cached. The manifest has a text/cache-manifest MIME type. A typical file looks like this:

CACHE MANIFEST

index.html

help.html

style/default.css

images/logo.png

images/backgound.png

NETWORK:

server.cgi

This file specifies several files to cache, and then specifies that server.cgi should never be cached, so that any attempt to access that file will bypass the cache.

The manifest can then be linked to by declaring it in the (HTML) application, like this:

<!DOCTYPE HTML>

<html manifest="cache-manifest">

...

The server.cgi file would be white-listed (put in the NETWORK: section) so that it can be contacted to get updates from the server, as in:

<event-source src="server.cgi">

(The event-source element is a new feature in HTML 5 that allows servers to continuously stream updates to a Web page.)

The application cache mechanism also supports a way to opportunistically cache (from the server) a group of files matching a common prefix, with the ability to have a fallback page for rendering those pages when offline. It also provides a way for scripts to add and remove entries from the cache dynamically, and a way for applications to atomically update their cache to new files, optionally presenting custom UI during the update.

Other benefits of HTML5 for mobile cloud computing is that it can be used to develop applications that will run on almost any device that support a suitable browser. Platforms like ios and android can only run applications with codes written specifically for their platform. But with the help of HTML5 developers will be able to write a single code for application that will run on any platform.

**4. Quality of experience**

The concept of quality of experience comes for quality of service. Quality of service can be described as the work done by the service provider to ensure that there is minimum time delay, least data loss and proper data traffic management. But how the end user feels about that service being provided is what really matters these days. Providing the service as the end user demands is known as the concept of quality of experience. There are many companies that measure the quality of experience by real time monitoring of the user’s call experience. Factors such as noise, echo, video distortion, freezing, call dropping etc are measured and steps are taken to ensure that these factors are eliminated. Various factors such as pricing, availability and simplicity need to be considered to please the end user.

The method of measuring the quality of experience can be explained as follows: In general, there are three possible methodologies for measuring QoE:

1. The no-reference model has no knowledge of the original stream or source ﬁle and tries to predict QoE by monitoring several QoS parameters in real-time.

2. The reduced-reference model has some limited knowledge of the original stream and tries to combine this with real-time measurements to reach aprediction on the QoE.

3. The full-reference model assumes full access to the reference video, possibly combined with the measurements conducted in a real-time environment.

The most prominent example of a no-reference model is the E-model. It predicts the quality users experience during a voice conversation based on the end-device characteristics and the transport parameters. These characteristics and parameters are plugged into some functions internal to the E-model of which the coeﬃcients were tuned based on subjective experiments. The E-model determines a rating R: R = R0 − Is − Id − Ie + A where R0 is the basic signal-to-noise ratio, Is takes into account phenomena that occur simultaneously with the speech signal (like the loudness of the speech signal and the side-tone and quantization eﬀects), Id groups impairments associated with delay (such as, impairments due to echo and loss of interactivity), Ie accumulates the eﬀects associated with special equipment (for example, the use of a low bit rate codec or packet loss), and A is an advantage factor (i.e., a decrease in R-rating a user is willing to tolerate because he or she has a certain advantage, e.g., being mobile).

An example of a full-reference model is the Perceptual Evaluation of Speech Quality (PESQ) model. It assesses the listening-only quality of narrow-band speech encoded, packetized and sent over a (possibly packet-lossprone) network. This model compares the original with the received signal and determines which diﬀerences result in annoying artifacts. For this purpose both signals need to be suitably aligned (which forms an integral part of the model). There is ongoing research on extending PESQ to wideband speech in Study Group 12 of the ITU-T.

Ultimately quality of experience is all about how service in accepted by the end user. The end user does not care about the technology that goes behind the service, they are just concerned about the availability of service, low pricing and getting exactly what is requested. So service providers have to keep in mind these factors and decide their company policy to provide the best service possible.

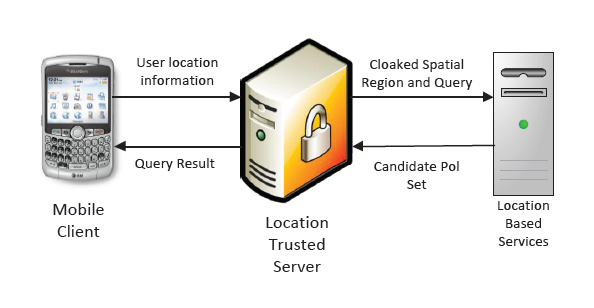
**Security:-**

In Mobile cloud computing, to establish and maintain consumers trust in mobile platform is necessary by protecting user privacy and data secrecy from an enemy. Every mobile user think twice before share or store their private information or data on the cloud. As the number of devices enters the market increases, some security issues will grow as well.  Hopefully, years of experience in the computer industry and cloud computing mean that mobile is not far behind in resolving these security issues. The security related issues in MCC are introduced in two categories: the security for mobile users and the security for data.

**1.Security for mobile users:** Mobile devices like cellular phone, Smartphone are exposed to so many security threats like virus, worm etc.. And also to protect the user’s important information from an enemy. Some solutions to overcome these issues are reviewed.

**a) Security for mobile applications:** The simplest way to detect security threats (like virus, worm and malicious codes) on the mobile device is by installing and running security software’s such as kaspersky, AVG etc..But as we know that mobile devices are resourceless i.e. low battery life time, we can’t keep these software’s running for long time. To overcome this problem, move the threat detecting software to the cloud platform i.e. cloud AV platform, this platform consists the Mobile agent and Network Service components. The Mobile Agent is a lightweight process that runs on the mobile device, it inspects the file activity on a system. If identified file is not available in the cache,then this file will be sent to in-cloud service. When network service in Cloud AV receives a file, it will perform file verification and check whether a file is malicious or not.

**b) Privacy:** As the usage of Location based services (LBS) increases with the advantages of GPS positioning devices. The LBS faces a privacy issue when user provide their private information like their current location. To overcome this issue Location Trusted Server (LTS) is introduced.

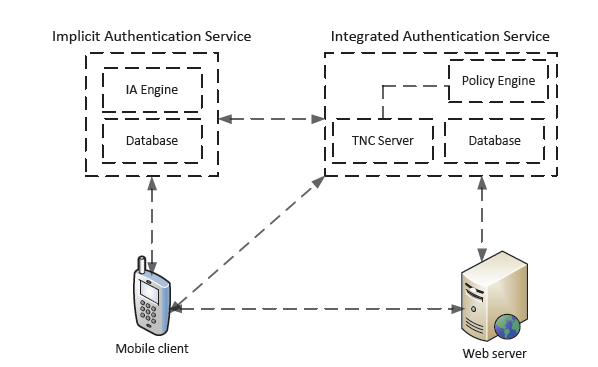


Firstly, the mobile user send request to LTS. After receiving mobile client request, LTS collects their information in certain area and conceals the information called “Cloaked regions” using “K-anonymity” concept. Then the “cloaked region ” is sent to LBS. Therefore by doing this LBS knows only general information about the mobile user but can’t identified them. But still there is a problem if LTS reveals user’s information or if LTS colludes with LBS, in this condition the user’s information is in danger. Now to overcome this problem ,generate the “Cloaked region” on mobile devices by using casper cloaking algorithm. And the cloud will provide information of the surrounding users to program. Then , mobile client generates “cloaked region” by itself and send it to the LTS. Therefore both LTS and LBS cannot know the sender’s information.

**2.Securing data on cloud:-**As we know that, storing data on cloud is beneficial for both mobile users and application developers. But they should be careful in terms of data integrity and authentication on the cloud. There are some data related issues in MCC :-

**a) Data Integrity:** Most of the mobile users are worried about their data integrity on the cloud. Therefore , to provide the data integrity on the cloud ,the new scheme is introduced. This scheme performs three phases: the initialization, the update and the verification. In initialization phase, the files(Fx) that mobile user wants to sent on the cloud will be assigned with a message authentication code (MACFx). These codes will be stored locally on your mobile device,and the file (Fx) will be saved on the cloud. In the update phase, when user is interested to add or modify the existing file(Fx). The cloud sends file (Fx) to the user and parallely cloud send a message to Trusted crypto coprocessor (TCC) to generate MACFx’. Then TCC sends MACFx’ to mobile user to verify the file (Fx) by comparing it with already existing code MACFx i.e. stored in the mobile itself. If both codes match with each other, then user can change or modify the file. Then finally, in the verification phase, client can request the integrity verification of a file. This approach also saves the energy for the devices because checking and verification are processed on TCC on cloud and client only compares a code.

**b) Authentication:** The most fundamental requirement to allowing secure mobile devices within the enterprise is to have a solution in place to authenticate the users of those devices. The new scheme combines Trust cube (policy-based cloud authentication platform using the open standards) and implicit authentication (uses mobile data e.g. calling logs, SMS messages etc. for existing mobile environment) to provide authentication to mobile users. The architecture shown in the figure is used to secure the mobile user access. Let’s see how it works step by step. First mobile client will sent request to web server for the service , after receiving the request web server redirects the request to Integrated Authentication service with the details of the request. The IA service seeks the policy for the access request, then collects the required important information, and send the request to Implicit Authentication server. IA service uses trusted network connect protocol to send the request to IA server. Then IA server generates a report using existing mobile data and send back the report to IA service. Integrated authentication service applies authentication rule in the policy and find out the result. Authentication result is forwarded to web server. Then web server decides according to the result, either provide the service or denies the mobile client request.



**Handover :-**

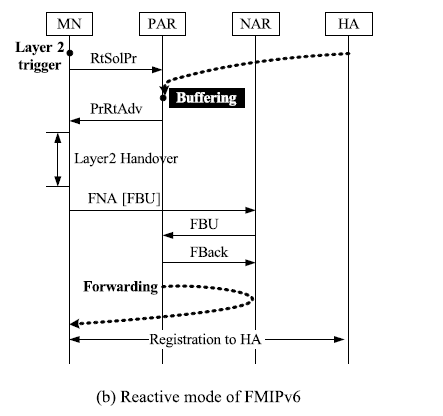
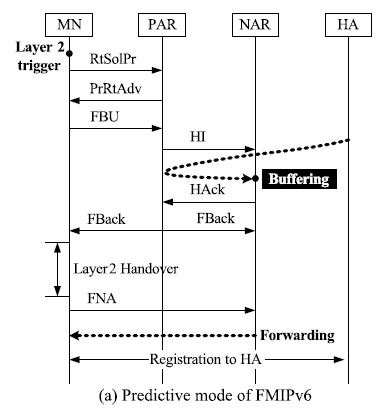
In a very simple words, handover process is a process which maintain connectivity when a mobile node (MN) moves between different subnets.

**Handover Latency:-** During the Handover process, there is a period that the MN is unable to send or receive packets, i.e., the handover latency.

As we know, in the future number of mobile users will be increasing rapidly. Therefore, it is important to provide seamless mobility management to mobile users who are interested in using real time services like audio-video streaming etc. But when mobile users are moving from one network to another another, there are chances of disconnect the signal. Therefore to support seamless mobility management for various wireless technologies in cloud computing, Mobile IPv6 (MIPv6) and fast handovers for MIPv6 (FMIPv6) are introduced. One of the most representative efforts on the IPmobile networks is Mobile IPv6 (MIPv6)(Johnson etal.,2004) proposed by Internet Engineering Task Force (IETF). MIPv6 is proposed as a host-based mobility protocol to support global mobility of MNs in IPv6 networks. Therefore, various enhancements, such as FMIPv6 (Koodli, 2005) and HMIPv6 (Soliman et al., 2005), Proxy Mobile IPv6 (PMIPv6) have been pro- posed directed towards MIPv6 performance improvements. Fast handovers

for Mobile IPv6 (FMIPv6) has been studied to reduce the handover latency and packet loss during the handover. In this report , we are going to tell you about the handover process in FMIPv6 and also how it will help in reducing the handover latency and packet loss as well.

**Fast handovers for Mobile IPv6 (FMIPv6):-** FMIPv6 is proposed to reduce handover latency and minimize data packet loss occur in MIPv6. In order to provide a seamless handover for the MN and route its data packet faster, the mobility updates related signaling must be performed more rapidly whenever the MN moves from older network to newer one. The loss of packets should also be minimized. It provides seamless handover using anticipation based on layer 2 trigger information to reduce the handover latency and packet loss.FMIPv6 consists of two operation modes :**predictive mode**: when layer 3 signaling for FMIPv6 may be processed before the layer 2 handover is completed. **reactive mode**:- when layer 3 signaling processing time is greater than the time between the layer 2 trigger and link down.



In the predictive mode of FMIPv6, MN sends proxy message to previous access router(PAR) to get information of the NAR. After getting information from PAR about the NAR, MN configures a new care of address (NCoA). CoA(care of address is the address associated with the MN while visiting the foreign subnets). After that , mobile node sends a fast binding update (FBU) message to the PAR to bind the PCoA with the NCoA. Then PAR tries to establish a tunnel between itself and NAR by exchanging a Handover Initiate and Handover acknowledge messages. After the verification of NCoA at NAR, tunnel is established. And packets starts forwarding to NAR from PAR through the tunnel during the layer 2 handover. NAR buffers packets until it receives a fast neighbor advertisement (FNA) message from the MN. When the MN attaches to the NAR, it sends the FNA message to the NAR. Then the MN registers the NCoA to the HA.

In the reactive mode of FMIPv6 ,the MN requests information from PAR of the NAR by sending the RtSolPr message. IN this mode, the FBU message encapsulated in the FNA message is sent to the PAR via the NAR after the layer 2 handover. Then the MN registers the NCoA to the HA. In the reactive mode, the PAR may buffer packets to the MN before the layer 2 handover is begun. In

this case, packets will be forwarded to the MN via the NAR when the PAR receives

the FBU message. If the PAR chooses not to buffer packets, packets are

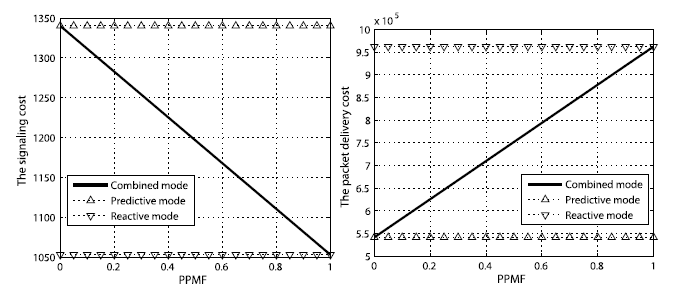
lost during the handover.

For the more accurate performance evaluation, the prediction probability should be obtained as

the function of network parameters such as the radius of a cell, the time required to process additional layer 3 signaling, and the layer 2 triggering time.

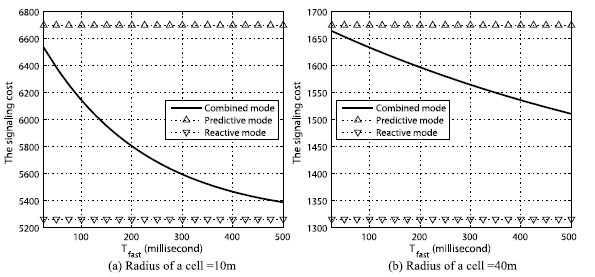
**Analytical results:-**

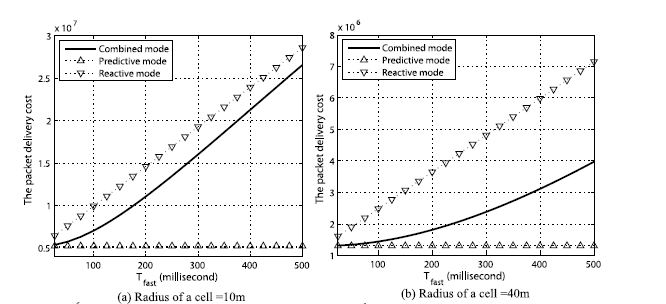
1.Figure shows the effect of the PPMF on the signaling cost and the packet delivery cost. It is clear from these figures that the signaling cost of predictive mode is larger and the packet delivery cost of reactive mode is larger. But PPMF have no affect on signaling cost and packet delivery cost in both modes.



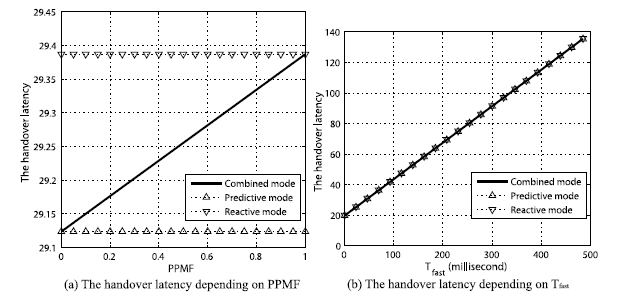
The signaling cost of combined mode decreases linearly as the PPMF increases but the packet delivery cost of the combined mode increases linearly.

2.As the Radius of cell increases the signaling cost of combined mode decreases and the packet delivery cost also decreases.



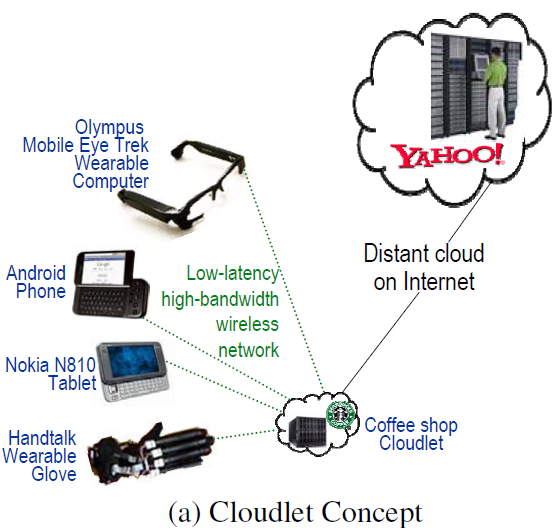


3. The handover latency depends upon the PPMF and Tfast (it is the time taken to establish a tunnel between PAR and NAR). Figure (a) shows that handover latency of combined mode increases linearly with PPMF and Figure (b) shows that the handover latency of combined mode, predictive mode and the reactive mode increases linearly.

.

**Cloudlets in Mobile Cloud computing:-**

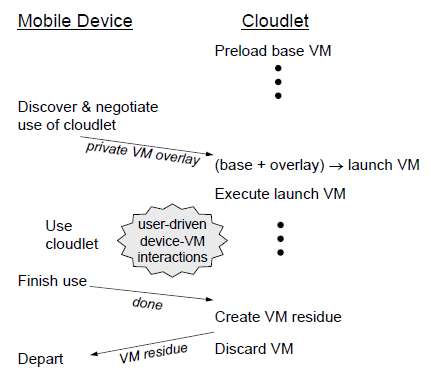
Cloudlets may just be a key to the future of MCC. As we know that mobile devices are resource- less i.e. low battery life, storage capacity is less, which is a main constraint in the way of seamless MCC. This is not just a temporary limitation of current mobile hardware technology, but is intrinsic to mobility. Due to this problem of Long WAN latency occurs.



A cloudlet is a trusted, resource-rich computer or cluster of computers which is well connected to the Internet and available for use by nearby mobile devices. A cloudlet is a “data center in a box”. It is self-managing, requiring little more than power, internet connectivity and setup.  **Rather than relying on a distant cloud, the resource poverty of a mobile device can be addressed by using a nearby resource-rich cloudlet and uses it via a wireless LAN.** Most importantly, acloudlet only contains soft state such as cache copies of data or code that is available elsewhere.

**Transient Cloudlet Customization:-**

Cloudlet infrastructure can bedeployed like Wi-Fi access points. But a key challenge is to simplify cloudlet management. The cloudlet infrastructure will not be deploy widespread unless software management of that infrastructure is ordinary. Therefore, to overcome this transient customization of cloudlet infrastructure using hardware virtual machine (VM) technology can be used.



The VM migration approach in which an already-executing VM is first suspended, its processor, disk and memory state are then transferred. Finally, VM execution is resumed at the destination from the exact point of suspension. The other approach is a small VM overlay is delivered by a mobile device to cloudlet infrastructure that already posseses the base VM from which this overlay was derived. The infrastructure applies the overlay to the base to derive the launch VM, which starts execution in the precise state from which the overlay was derived.

**Difference between Cloudlet and cloud:-**

|  |  |  |
| --- | --- | --- |
|  | **CLOUDLET** | **CLOUD** |
| **State** | Only soft state | Hard and soft state |
| **management** | Self-managed; little to no  professional attention | Professionally administered,  24x7 operator |
| **environment** | “Datacenter in a box” at  business premises | Machine room with power  conditioning and cooling |
| **ownership** | Decentralized ownership  by local business | Centralized ownership by  Amazon, Yahoo!, etc. |
| **network** | LAN latency/bandwidth | Internet latency/bandwidth |
| **sharing** | Few users at a time | 100s-1000s of users at a time |

**Conclusion:-**

Mobile cloud computing is one of mobile technology trends in the future since it combines the advantages of both mobile computing and cloud computing, thereby providing optimal services for mobile users. This report has provided an overview of mobile cloud computing in which its definitions, architecture, advantages, and issues have been presented. We have then analyzed in detail the security issues associated with mobile cloud computing. In MCC, mobile networks should be efficiently managed to support seamless mobility to mobile users who request real-time services. To manage efficient mobile networks, FMIPv6 which is an extension of MIPv6 must be utilized. In this report, FMIPv6 combining two operation modes is analyzed using PPMF, radius of cell and Tfast. And finally FMIPv6 is able to reduce the handover latency and packet loss. The next big problem of mobile device i.e. resource poverty which is a fundamental constraint that severely limits the class of applications that can be run on mobile devices. This constraint is not just a temporary limitation of current technology, but is intrinsic to mobility. By using cloudlets, mobile users seamlessly utilize nearby computers to obtain the resource benefits of cloud computing without incurring WAN delays and jitter. We confirm that a critical untested aspect of this vision, namely rapid customization of cloudlet infrastructure, is achievable through dynamic VM synthesis. While much remains to be done, the concepts and ideas introduced here open the door to a new world of mobile cloud computing. This technology is relatively a new concept and a lot of research has to be carried out to develop a complete system for mobiles computing which is secure and consistent. The use of technologies such as HTML5 is yet to be fully understood for mobile caching and other factors such as cost and execution methods have to be improved so that this technology is fully accepted.

**References:-**

* L. Liu, R. Moulic, and D. Shea, “Cloud Service Portal for Mobile Device Management,” in Proceedings of IEEE 7th International Conference on e-Business Engineering (ICEBE), pp. 474, January 2011.
* M. Satyanarayanan, “Mobile computing: the next decade,” in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), June 2010.
* Cloud Computing for Mobile World ,Chetan S., Gautam Kumar, K. Dinesh, Mathew K. and Abhimanyu M.A. Department of Computer Science & Engineering National Institute of Technology, Calicut.
* Mobility managementforIP-basednextgenerationmobilenetworks: Review, challengeandperspective Ibrahim Al-Surmi a,n, MohamedOthman a, BorhanuddinMohdAli. Available online 17 September 2011
* Mobile cloud computing framework for a pervasive and ubiquitous environment

**Min Choi · Jonghyuk Park · Young-Sik Jeong,** © Springer Science+Business Media, LLC 2011

* White Paper, “Mobile Cloud Computing Solution Brief,” AEPONA, November 2010.
* Z. Leina, P. Tiejun, and Y. Guoqing, “Research of Mobile Security Solution for Fourth Party Logistics,” in Proceedings of the 6th International Conference on Semantics Knowledge and Grid (SKG), pp. 383 - 386, January 2011 .
* Jian Li, “Study on the Development of Mobile Learning Promoted by Cloud Computing,” in Proceedings of the 2nd International Conference on Information Engineering and Computer Science (ICIECS), pp. 1, December 2010.
* S. Wang and X. S. Wang, “In-Device Spatial Cloaking for Mobile User Privacy Assisted by the Cloud,” in Proceedings of the 11th International Conference on Mobile Data Management (MDM), pp. 381, June 2010.
* W. Itani, A. Kayssi, and A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing,” International Conference on Energy Aware Computing (ICEAC), pp. 1, January 2011.
* R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, “Authentication in the clouds: a framework and its application to mobile users,” in Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), pp. 1 - 6,2010.
* A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang