Volume 3, Issue 2
April2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Mobile Applications Architecture &Usage in Cutting-Edge Technologies

[1]*Rabia Shaheen,*[2]**Faheem Babar**[3]*Dr. Shahbaz Pervez Chattha,*[4]*Dr. Nasser Abosaq*

[1]Information and Computer Technology Department, King Khalid University, [2]Alfutaim Technologies, Islamabad Pakistan

[3,4]Information and Computer Technology Department, Yanbu Industrial College,

Kingdom of Saudi Arabia

E-mail: [1]rshahin@kku.edu.sa, [2]greatfaheem@gmail.com,[3]rasools@rcyci.edu.sa, [4]abosaqn@rcyci.edu.sa

ABSTRACT

Revolution of IT has changed the life style of people and their working habits. Also, it has totally changed the traffic patrons on the internet, due to excellent features of mobiles applications. The trend of using mobile devices has gone beyond limits and with every passing day the users are thinking to get solutions of their daily lives. That includes computing needs, liberty of communication and information sharing via Mobiles applications. This paper discusses the architecture of mobile applications, its major components and the role of mobile application in cutting edge technologies. Also, a comprehensive comparison of the performance of different platforms with respect to performance of mobile applications is presented.

Keywords: Mobile *OS architecture, IOS APPs,SDK,Appification, Multi-touch , Multi-Window, SDK Manager, Mobile API, SMS*

1. INTRODUCTION

Due to the rapid development in the field of mobile computing and its popularity among end users, mobile application development becomes a challenging job with every passing day. The diversity of platforms for different mobile devices makes ads more challenge to the development process. Keeping the cost of development as minimum as possible to reach to the end users of different platforms is the most concern factor. Another factor is to be considered is the apps should not be resource hungry and their performance is monitored in terms of memory usage and CPU(Central Processing Unit). In this paper, section 1 describes general architecture of mobile OS, its history and different available features of common OS platforms. Section 2 describes Internal architecture and different sensor types. Section 3 shows the performance comparison of mobile apps. Section 4 discusses the related work on mobile devices with different aspects. In section 4 the future traffic trends of mobiles devices is explained. Section 5 describes the future of traffic trends by the use of Mobile Applications. Finally the paper concludes with some security issues and some future directions.

1.1 General Architecture of Mobile OS.

Following figure shows the major tiers that are mostly considered while developing a mobile application for variety of platforms.

Figure 1: Mobile Apps Architecture

All the Android based applications are developed by the process of Android Software Development, in which new applications are created for the Android operating system. Java Programming language is mainly used for developing these Android applications using the Android Software Development Kit (SDK), but other development tools are also available. This Android SDK includes sample projects with source code, development tools, an emulator, and other libraries required to build an Android application. There are two categories of tools that are used in SDK: SDK tools and Platform tools. SDK tool is a downloadable

component for the Android SDK, which includes the complete set of development and debugging tools. The Platform tools are customized to support the features of the latest Android platform.

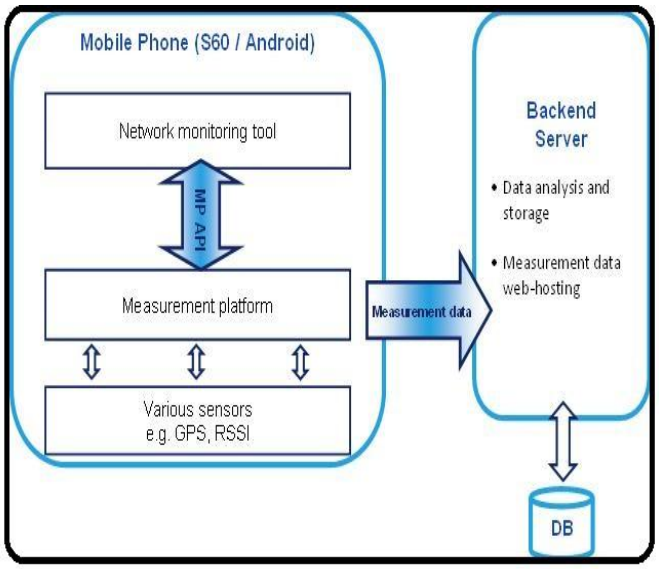

Figure 2: Mobile Phone Communication Block Diagram

1.2 Communication of Mobile with internal DB

Here is a brief detail of internal communication of mobile device which shows after initiating request from device which procedures it has to follow to complete the cycle of this query. A user send request to local Cache Database there are two scenarios for this request

I. If he don't get cached content from there then it will issue a request with no date appended and request is forwarded to Sitecore API, Once Sitecore API receives GET Request+ returns a response and this response in two forms.
   a) If it is content then use response content, store it in cache and goes to render view.
   b) If its 304 then use the cache and modify date and then it will forward it to render view.

II. If cached contents are there then it will compare date in cache to see if its older than the threshold then it will further go to stale and here again conformity test will be done
   a) If stale is yes then it will issue request date appendedand forwarded it to Sitecore API, Sitecore API receives GET Request+ returns a response and this response will again in above two forms and process will use the same path as described above in (I).
   b) If No Stale from here then it will go further to use cache and it will signal to the systems there is no need to modify the date and it will forward it to render view.

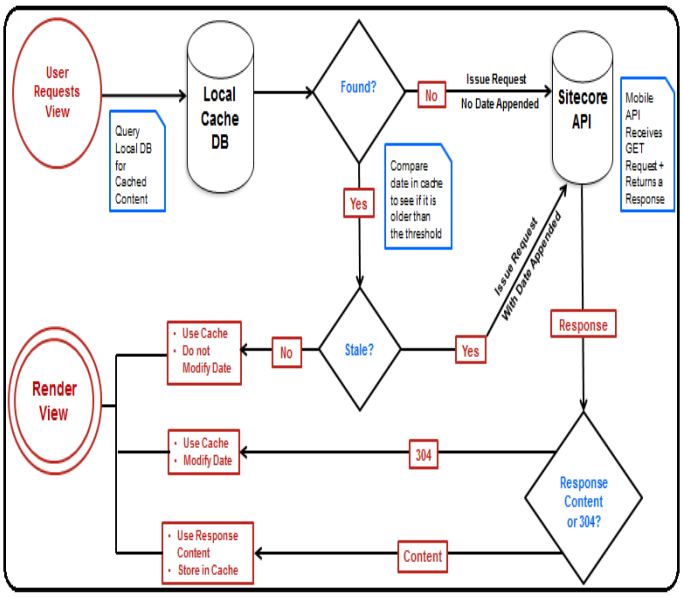

Figure 3: Internal Block Diagram of query request

2. SENSORS USED IN SMARTPHONES

A sensor is a converter that measures a physical quantity and converts it into a signal. The signal can be read by an observer or by an instrument. There is large number of sensors available in market today. Most android powered phones, windows phones, iPhone and other OS based smartphones have built-in sensors. These sensors are built to measure and provide a high precision and accurate data to the reader. In addition to handling the calls, smart phones can do video recording, GPS navigation, MP3, Wi-Fi, etc. These sensors can be hardware-based or software-based. The hardware-based sensors are physically present in the device and they directly measure the environmental properties. The software-based sensors are virtual sensors that take their inputs from one or more hardware sensors for calculation. The hardware-based sensors play big role in developing an application for that particular mobile devices. These sensors are used in a very creative way to produce very interactive and interesting applications and games. Smartphones are set to become even more smarter with the change in technology that will help the devices play greater

role in people's lives. Improved sensors will allow phones to act and react in a similar manner to Microsoft's Kinect games console which can understand hand gestures and recognize faces. Different types of sensors used in most of the Smartphones are:

Type_Accelerometer: It measures the acceleration force in m/s2 that is applied to a device on all three physical axes (x, y, and z), including the force of gravity. Its common use is Motion detection (shake, tilt, etc.).

Type_Ambient_Temperature: It measures the ambient room temperature in degrees Celsius (°C). Its common use is monitoring air temperatures.

Type_Gravity: It measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Its common use is Motion detection (shake, tilt, etc.).

Type_Gyroscope: It measures a device's rate of rotation in rad/s around each of the three physical axes (x, y, & z). Its common use is Rotation detection (spin, turn, etc.).

By looking at the current market of mobile applications and its major platforms, there are two major participants who are providing platform to host these mobile applications (Android and iOS).

2.1 ANDROID OS:

Android Operating system is based on Linux and it is designed to be used for touch screen mobile devices (e.g. tablets and smart phones). It was initially developed by Android Inc.. Due to financial issues, Google Inc. helped Android financially in developing and modifying it to be aligned with latest market trends. The first version of Android was unveiled in 2007, and the first Smartphone running Android OS (HTC Dream) was in market by 2008. Source code of Android is released by Google under the Apache License. This licensing allows the Android software to be freely modified and distributed by the device manufacturers. This made it the most favorite to consumers and developers. Android gives a world class platform for creating apps and games for Android users and developers. The first commercial version of Android was *Android Alpha 1.1*, it was released in September 2008. The improvement continues by introducing newer versions since then.

2.2 APPLE iOS

A new era of mobile computing started after the Introduction of iPhone by Apple's in 2007. The launching of iPhone, iPOD touch, iPAD has literally redefined the entire world of mobile computing and introduces the new trends in the field of mobile computing. Since iOS is amongst the older mobile operating systems in active development, but that certainly still addressing the processing or communication needs with new fashion of mobile end users. Through what can only be described as persistent and consistent improvement over the years, Apple has made iOS one of the most feature-rich and well-supported platforms on the market by introducing iOS6. [15].

Next version of apple which is iOS 7 was launched in 2013 as the biggest change Apple has made to its iOS platform. iOS 7 provides the user interface, with a complete refresh of the app icons, and a totally new look and feel. The new OS is designed by Apple to be unobtrusive and minimalistic, stripping away any unnecessary features. The design is a flatter one than on previous versions, with less texture on app icons, pared-down fonts and minimalistic menus.

3.PERFORMANCE COMPARISON OF MOBILE APPLICATIONS ON DIFFERENT PLATFORM

The Android and iOS are the leading platforms by offering more than 83% mobile applications on their platforms step by step we are comparing all basic features of these platforms.

3.1 ARCHITECTURE OF ANDROID OS:-

The Android OS can be referred to as software stack of different layers, and each layer of this architecture is a group of several program components. This architecture includes Android OS, middleware and other important application programs.

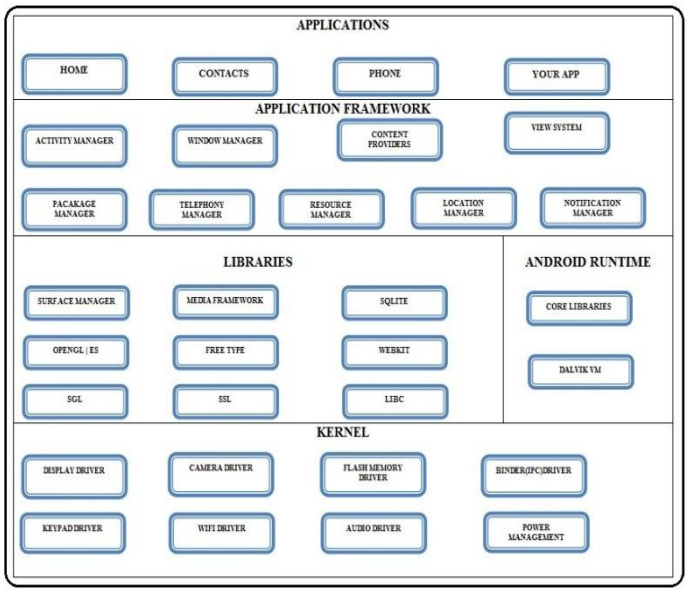

Figure 4: Android OS Architecture [14]

Following are different layers in Android OS :-

- **Linux Kernel :-** Android OS is built on top of the Linux 2.6 kernel which is the basic layer of the Android OS. This layer is further differentiated due to some architectural changes made by Google. This layer provides basic system functionality like process management, memory management, device management like camera , keyboard , display ,etc. This Linux Kernel also acts as a layer of abstraction between the hardware and software layers.
- **Libraries** :- Android native libraries are next to the Linux kernel. This layer enables the device to handle different types of data. An open source web browser engine Web Kit , well known library "libc" , SQLite database , libraries to play and record audio and video , SSL libraries , etc. are also included in this layer of libraries.
- **Android Runtime** :- The third layer of the architecture is the Android Runtime which consists of Dalvik Virtual Machine and Core Java Libraries.The Dalvik is the process Virtual Machine (VM) in Google's android operating system. It is the managed runtime used by applications and some system services on Android. Dalvik was originally created specifically for the Android Project.On the other hand, Core Java Libraries consists of classes which are used by many portions of the JDK. The actual set of files has evolved over time,but mostly they include functionality which is close to the VM . Also included are commonly used tools which are either built on top of the core libraries (such as jar) or are used by developers working with them (such as mic). This set of core libraries enables the Android application developers to write Android applications using standard Java Programming language.
- **Application Framework** :- This layer provides many higher level services to applications in the form of Java classes . These programs manage the basic functions of phone like resource management , voice call management etc . These are some basic tools that are used for building the applications.
- **Applications** :- All the Android applications are found at the top layer of the architecture . The written applications will be installed on this layer only . Several standard applications comes pre-installed with every device.

3.2 ARCHITCTURE OF iOS

Following figures elaborate the architecture of iOS and its different layers

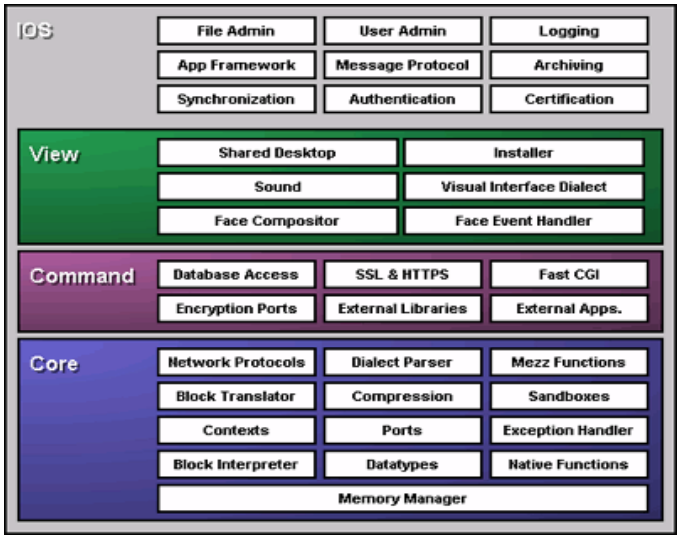

Figure 5: iOS internal Architecture [12]

3.3 MOBILE APPS AVAILABILITY FOR IOS& ANDROID

Android gets apps from Google Play, which currently has 600,000+ apps available, which run on tablets and smart phones. On the other hand some Android devices, such as the Kindle Fire, use separate app stores that have a smaller

selection of apps available. Many originally iOS-only apps are now available for Android, including Instagram and Pinterest, Android includesaccess to Google-based applicationswhich include google doc and youtube.

As for now if we talk about available apps for both platforms, The Apple app store currently have 700,000+ apps, and almost 250,000 of which are available for the iPad. Its general trend that developers prefer to develop apps for iOS and then later on the move develop the same kind of apps for Android.

In net shell if we start comparing Mobile Apps for iOS & Android apps we can say that most popular apps are easily available for both platforms. But in case of apps for tablets we can say that apple is taking lead in this area. If we look at the development trends for developing Mobile Apps we can easily say that apple is taking lead as Developers at startups often focus on one platform (usually iOS) when they first launch their smartphone app because they do not have resources to serve multiple platforms. Many popularapps like Instagram first started with iOS and then later on they developed this app for iOS.

3.4 MOBILE APPLICATIONS STABILITY ON DIFFERENT PLATFORMS

Mobile apps always need some platform to run on any mobile device which also known as operation system, here we are presenting the findings of The Criticism Mobile Experience Report published in March 2014 ranked Android KitKat as more stable than iOS 7.1. there are some other findings from the report which shows

- Android 2.3 Gingerbread has the highest total crash rate, at 1.7%. Other versions of Android — Ice Cream Sandwich, Jelly Bean, and KitKat — have a crash rate of 0.7%.
- iOs 7.1 has a crash rate of 1.6%., and the rates for iOS 7.0 and iOS 5 are 2.1% and 2.5% respectively.
- Tablet versions of iOS & Android are less stable as compared to phone versions for both platforms.
- The ratio for apps Crash is more in games related apps (4.4% crash rate) and on the other hand the lowest ratio of crash is for e-commerce apps (0.4%).

Following figure depicts the users experience in terms of satisfaction.

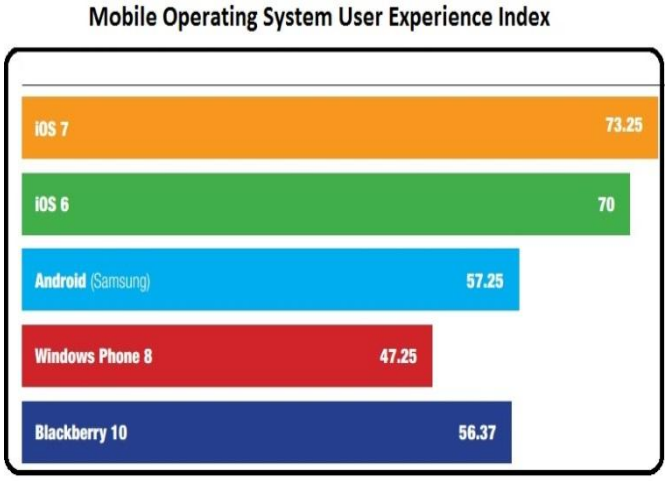

Figure 6: Mobile OS User Experience (Higher is the Better)[8]

Following table draw a comparison of features available in different OS of mobile computing devices.

iOS-7 7/10	Android(Samsung) 7/10
Notification area	Notification area
Notification on lock Screen	Notification on lock Screen
Multitasking	Multitasking
-	Multi-window mode
Control area	Control area
Multi-touch controls	-
Direct Camera Access from lock Screen	-

Table 1: Mobile OS ratings with respect to features

4. RELATED WORK

Here is the list of related work done by other researcher in the field of cloud computing security. Kumar et al described that the propagation of smart phones in business has been increasing tremendously due to its various enterprise applications and this scenario is expected to continue in both business as well as personal fields. However , enterprises require very strict security mechanisms on these smart phone platforms to make their sensitive data available on them , as enterprises cannot compromise on the sensitive data due to the reasons such as employees losing phones to some of the malicious applications which are running on the phones . But most of the existing solutions for such issues are providing security at either device level or through some external monitoring agent , which is the reasons for its limitations. In this paper , the author has proposed such a security solution that can be managed at run time rather than at device level and thus providing more security. This solution can be less intrusive to the end user but provide strong security solution to the enterprise. He has described several scenarios wherein this security at runtime can be more effective and efficient with minimal overhead as compared to solutions that are already present[1]. Tanveer et al has described the implementation of cloud computing using Amazon Web Service interface compatible framework known as Eucalyptus that fully supports virtualization. A cloud has been designed privately using this (Eucalyptus) framework for developing an application store for smart phones. Its architecture, physical and network implementation has been discussed in detail. Two sample applications have been developed that can be downloaded using Amazon Web Services platform (PaaS). These sample applications use this private cloud as their computing platform and its performance has also been found better even on the smart phones that process very slowly [2]. Chit et al described that A platform based on cloud computing known as Mobile Computing Applications Platform (MCAP) is introduced. Its core responsibility is to enhance the situational awareness and control for the first responders. This platform is solely based on cloud computing and is used for defining, developing and deploying applications for smartphones , tablets and different in-vehicle computers like GPS devices . This developmental approach has exclusive differentiators that include the use of COTS (Commercial Off-The-Shelf) technologies for creating low cost and sustainable programs for mobile computing and wireless networking. Such an architectural platform is discussed that reveals some re-usable mobile core services that stimulate an eco-system of partners to develop such applications that have got rich features are highly innovative in nature. Use profile, authentication, content management , location , notification and device management are the basic and significant services provided by this platform . This paper has outlined a public-private collaboration and governance model which is declared as an essential element for a healthy eco-system . Using the experiences from the user trails with several Michigan National Guard units , the present status of the MCAP platform is presented[3]. Ugus et al has presented a runtime security solution to Linux-based smartphones . This dimension is based on a trusted mechanism named as Mobile Trusted Module (MTM) and its sole objective being inhibition of arbitrary third party applications running on smartphones. Using this architecture , only those applications that are signed by Mobile Trusted Module (MTM) are being allowed to run and those applications that are infected are inhibited e.g. a mobile virus after their installation. This approach is mostly useful to administrators in different companies as they mostly want to control all the applications running on employees smartphones and the applications that are installed without the permission of the company should never execute [4].Sodhi et al described that there has been an increasing growth in the use of smartphones. This increase in growth has got great effects on the development of appification of web applications. The advanced smartphones run those applications on them which will solve more complex problems and should be rich in their content. This is in comparison to the smartphones that were used earlier . But the development of these appifying applications does not provide architectural clarity which has become the major issue for the success of these systems . There has been great differences in the architecture of regular web applications and its corresponding appifiedavatars . The appified avatars are designed as such so as to utilize the capabilities of smartphones and tablets . In this paper ,appifying

web applications have been investigated by considering the layered architecture of browser accessed web applications . The author has determined some non-functional quality attributes (QA) which are affected by appifying different layers. It has been found that from quantitative point of viewappifying a particular public web application shows the possibility of saving as much energy daily as is yearly required by 45 households [5]. With the advent of cloud computing and the access of mobile applications both in the number and diversity, there has raised a need to get the clear concept of their architecture, composition and quality. As such, certainly it has become very difficult to understand different applications and their usage that are being used for different mobile application patterns. This issue has directly affected several aspects like user experience, development cost and sale revenues of mobile applications. The author has pinpointed four main mobile application patterns and this identification is based on the evaluation and points of view of developer , user and service provider . The evaluation was carried out by starting from defining high – level criteria towards low – level criteria in order to establish and safeguard the objectivity of these applications. The practical verification was implemented by the after finalizing the theoretical evaluation. The application used for object recognition was selected for development that includes excitement as well as a great challenge for the developer [6]. The authors of the paper has elaborated cloud computing as a very wide area of information technology. It helps to solve problems very conveniently and efficiently. But the greatest challenge in the field of cloud computing is the security of data and protection of our privacy. This security issue is acting as a great barrier for the development of cloud computing and thus hinders its progress. The author has given the detailed description of the security issue of cloud computing by providing a cloud computing security model. This model has been distinguished into four parts as virtualization platform, infrastructure services, fundamental services and application services that analyses the key technologies to be achieved but this model including virtualization security , identity authentication[7]. Kandayet all has discussed the concept of cloud computing as such a technology that uses both the internet and the remote servers located centrally in order to maintain the data and applications. By the help of cloud computing, it is easily possible to accesses our data at anytime anywhere and that too without any installation of applications provided internet is available. This feature of cloud computing makes it much more familiar to consumers and businesses .Since it is available publically, due to that reason security is of high concern. In this paper , survey of different security and application aspects of cloud computing has been reported which include confidentiality , integrity , transparency , availability , assurance , etc. [8]. Cloud computing is an Internet-based computing. Computing services, such as data, storage, software, computing, and application, are delivered to local devices through Internet. The major security issue of cloud computing is that the cloud provider must ensure that their infrastructure is secure, and that prevent illegal data accesses from outsiders, other clients, or even the unauthorized cloud employees. In this paper, we deal with cloud security services including key agreement and authentication. By using Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing, we design the secure cloud computing (SCC). Two types of SCC are proposed. One requires a trusted third party (TTP), and the other does not need a TTP. Also, our SCC can be extended to multi-server SCC (MSCC) to fit an environment, where each multi-server system contains multiple servers to collaborate for serving applications. Due to the strong security and operation efficiency, the proposed SCC and MSCC are extremely suitable for use in cloud computing [10].Ni Zhang et al ,has discussed the concept of cloud computing as one of the new models of other emerging computer technologies that include grid computing, parallel computing, virtualization technology, utility computing ,etc. and has got many other advantages in addition to the basic benefits of these technologies which include large scale computation and data storage , visualization , high expansibility and reliability , low price service. According to him , the fast development of cloud computing can get affected because of its security issues . This paper analyses some of the main cloud computing security issues such as data privacy and service availability and their strategic planning for the formulation of their solution as single security methods alone are not enough for the protection of these cloud computing systems[11]

Volume 3, Issue 1April2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

According to the author cloud computing is a non-traditional prototype that is used presently being used by most of the organizations as it offers Information Technology and other technology related functions to these organizations and that too without spending much over it by providing them with facilities like elastic computing, dynamic storage in addition to the fulfillment of other computing requirements. But, in spite of having such potential gains achieved from cloud computing, the adoption of the cloud computing is broadly affected by the security issues related to it . These security issues are a major concern and can be related to architecture, multi-tenancy , elasticity , and layer dependency . This paper has given the detailed description of these security issues of cloud computing by investigating the problem from different perspectives which include cloud architecture perspective ,cloud characteristics perspective , cloud delivery model perspective ,etc. The author has also carried out a detailed investigation of some of the key research challenges which can be very much helpful to overcome the major issues of cloud computing[13].

5. FUTURE TRAFFIC TRENDS:

Due to popularity of mobile apps in near future the traffic patron will take the following shape and mobile users will be enjoying the liberty of using all these service right from their mobile device. Figure 7 shows communication blocks.

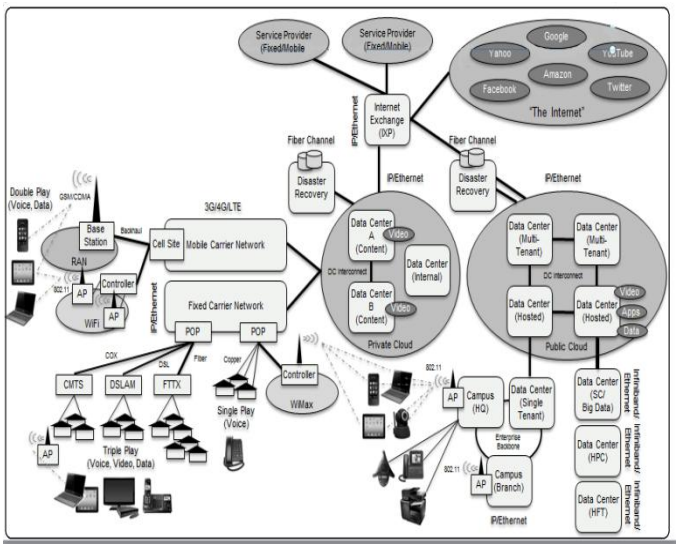

Figure 7: Future Traffic Trends due to Mobile Apps Devices

The following figure 8 shows the traffic routes that would be more popular during the facilitation process of these mobiles users while accessing difference services from their mobile devices .

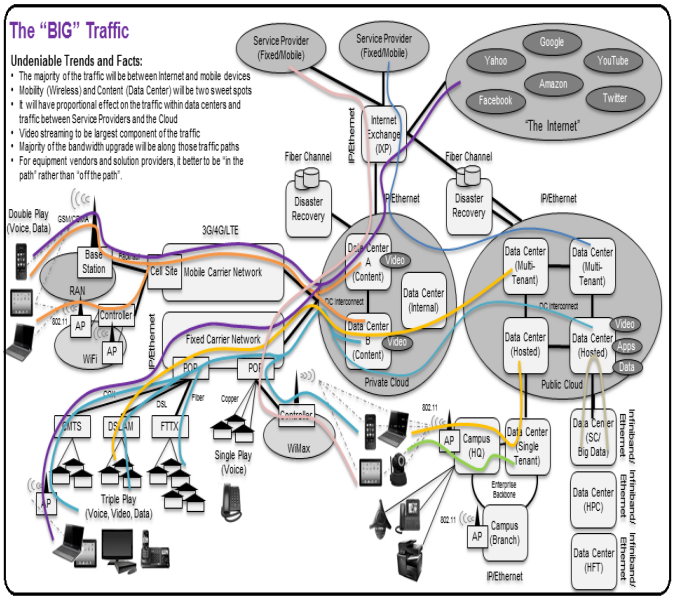

Figure 8: Future Traffic Routs of Mobiles Devices

Here are some findings while keeping in mind the network usage for mobile apps to provide services to mobiles users which are undeniable Trends and Facts for the Next Decade:

- Explosive growth in mobile devices
- Explosive growth in apps for consumer and business
- Explosive growth in storage for date/content
- Video streaming to be largest component of the traffic
- Growth in unified communication and collaboration
- Growth in virtualized services and service delivery/assurance
- TCP/IP stack on everything or a goal
- The majority of the traffic will be between Internet and mobile devices
- Mobility (Wireless) and Content (Data Center) will be two sweet spots
- It will have proportional effect on the traffic within data centers and traffic between Service Providers and the Cloud
- Video streaming to be largest component of the traffic Majority of the band

6. SECURITY AND PRIVACY ISSUES IN MOBILE APPS

With the increased of popularity of mobile devices end users started shifting their personal information (like bank accounts details ,login/password for their personal emails and accounts) from their computers to mobile devices and due to popularity of these mobile devices almost all the major banks are offering mobile apps to use their services right from the mobiles of end users. The intruders on the other hands are very smart and they are trying to intervene by offer some free apps having some kind of Trojan horse to steel the information of end users. It is therefore for important for the user of mobile devices to verify all the applications before going to install on their mobile device to avoid these kind of security breaches.

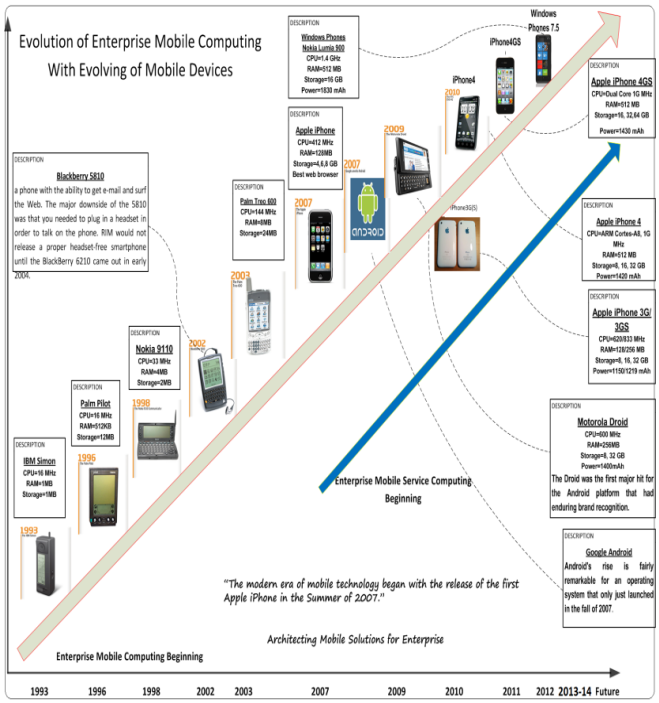

Figure 9: Mobile Technology Evolution

7. CONCLUSION

Here we conclude our work on the basis of performance of mobile apps for different platforms which indeed is a great revolution in the field of computing and this revolution has changed the way of thinking for the computing devices. With the inclusion of these Apps we witnessed a great change in business marketing. These mobile applications also have totally changed the entire trends of traditional communications. Popularity of these apps also changed the concept of social media which was only bound to big computer screens or laptops. Since all these apps have gained this much popularity on the other hand there is significant change at manufacturer side, Now manufacturers of mobile devices are focusing on more memory , storage and processing capability for mobile devices. Eventually we can say that in this era processing devices have completed its one cycle from desktop to laptop and from laptop to palmtop with is a good sign in case of availability of information in timely fashion.

8. REFERENCES

[1]. Kumar, U.; Kodeswaran, P.; Nandakumar, V.; Kapoor, S., "Polite: A policy framework for building managed mobile apps," MILITARY COMMUNICATIONS CONFERENCE, 2012 - MILCOM 2012 , vol., no., pp.1,6, Oct. 29 2012-Nov. 1 2012.

[2]. Tanwer, A.; Tayal, A.; Hussain, M.; Reel, Parminder Singh, "Thin apps store for smart phones based on private cloud infrastructure," Kaleidoscope: Beyond the Internet? - Innovations for Future Networks and Services, 2010 ITU-T , vol., no., pp.1,6, 13-15 Dec. 2010.

[3]. Chit Chung; Egan, D.; Jain, A.; Caruso, N.; Misner, C.; Wallace, R., "A Cloud-Based Mobile Computing Applications Platform for First Responders," Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on , vol., no., pp.503,508, 25-28 March 2013.

[4]. Ugus, O.; Landsmann, M.; Gessner, D.; Westhoff, D., "A Smartphone Security Architecture for App Verification and Process Authentication," Computer Communications and Networks (ICCCN), 2012 21st International Conference on , vol., no., pp.1,9, July 30 2012-Aug. 2 2012.

[5]. Sodhi, B.; Agrawal, A.; Prabhakar, T. V., "Appification of web applications: Architectural aspects," Communications in China Workshops (ICCC), 2012 1st IEEE International Conference on , vol., no., pp.1,7, 15-17 Aug. 2012.

[6]. NguPhucHuy; Do van Thanh, "Selecting the right mobile app paradigms," Service-Oriented

Computing and Applications (SOCA), 2012 5th IEEE International Conference on , vol., no., pp.1,6, 17-19 Dec. 2012

[7]. Su Qinggang; Wang Fu; Hang Qiangwei, "Study of Cloud Computing Security Service Model," Engineering and Technology (S-CET), 2012 Spring Congress on , vol., no., pp.1,4, 27-30 May 2012.

[8]. Kanday, R., "A Survey on Cloud Computing Security," Computing Sciences (ICCS), 2012 International Conference on , vol., no., pp.302,311, 14-15 Sept.2012.

[9]. http://www.diffen.com/difference/Android_vs_iOS

[10]. http://www.pfeifferreport.com/v2/wp-content/uploads/2013/09/iOS7-User-Experience-Shootout.pdf

[11]. Ni Zhang; Di Liu; Yunyong Zhang, "A Research on Cloud Computing Security," Information Technology and Applications (ITA), 2013 International Conference on , vol., no., pp.370,373, 16-17 Nov. 2013.

[12]. http://www.rebol.com/rebol-intro.html

[13]. Gonzalez, N.; Miers, C.; Redigolo, F.; Carvalho, T.; Simplicio, M.; de Sousa, G.T.; Pourzandi, M., "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing," Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on , vol., no., pp.231,238, Nov. 29 2011-Dec. 1 2011.

[14]. www.android.com/apps-and-entertainment

[15]. www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad

[16]. www.thinkybits.com/blog/iOS-versions/

9. AUTHOR PROFILES

Miss RabiaShaheen received her Master (MCA) from University of Kashmir in 2010. with more than four years of research & teaching experience at graduate level. Her area of specialization is high-level Programming, Mobile Application Development, Cloud computing and virtualization. Currently she is working as Lecturer at King Khalid University, Kingdom of Saudi Arabia.

Engr. Faheem BabarHas done his BE in Electrical Engineering (specialization in telecom) and MSc in Information Security from University of Engineering and Technology Taxila Pakistan. His area of specialization is Security systems & Secure Communication both voice and data, QoS by using different services over network. Currently he is working at Islamabad with a UAE Based Multi-National company Al-Futtaim as Sr. System Engineer.

Dr. Shahbaz Pervez Chattha received his PhD Computer Engineering degree from University of Engineering & Technology Taxila Pakistan , with more than fifteen years of research and teaching experience at graduate and post graduate level. His area of specialization is communication and Networks, Network Security, Cloud computing and virtualization. Currently, he is Lecturer at Yanbu Industrial College Royal Commission Yanbu, Kingdom of Saudi Arabia.

Dr. Nasser Abosaqreceived his PhD Computer Science degree from Florida Institute of Technology USA, with more than thirteen years of research and teaching experience at graduate and post graduate level. His area of specialization is Reliability, Software Engineering and cutting-edge technologies. Currently, he is Assistant Professor at Yanbu Industrial College Royal Commission Yanbu, Kingdom of Saudi Arabia