Mobile OS – Comparative Study

Jyothy Joseph, Asst. Professor, Computer Science Department, Al-Ameen College Edathala, Ernakulam (Dist.), Kerala, India

Shinto Kurian K, Project Manager, Tech Mahindra, Chennai

Abstract

In the fast growing mobile revolutionary era, many operating systems are playing vital role in present market. This study is intending to identify the apt and secure mobile based on mobile operating systems capability and user requirements.

Keywords: Android, Symbian, iOS, Windows, Blackberry, Mobile OS

1. Introduction

In the recent period, mobile operating systems are getting a tremendous growth. Analysts are upbeat further more potential developments in coming days. Today's markets, a wide variety of mobile phones are available in various brands with different operating systems. So the selection of an optimal and secured one is a confusing task. Present mobile operating systems are equally or more playing vital role than a computer operating system. It is covering most of the activities which were doing in a computer. We can see many of them are highly relay on mobile phones for their office activates like outlook, communicator etc. That indicates mobile operating systems are leveraging the high capability. Security is one of the key features of any mobile operating system. Many studies are keeping progressing in the same area. These studies are trying to provide a glance about the various mobile operating systems and its security measures which were expecting and available.

2. Research Elaborations:-

Many methodologies are available to define the workflow of a research topic. This study followed the analytical methodology as mentioned below(Fig 1). Here in the initial stretch doing a survey of current mobile operating systems in the market. Then review the customer expectations on mobile based on the present features and trends. Then check the security mechanism implemented. Based on these studies and reviews users can finalize the optimal one for their requirements/convenience.
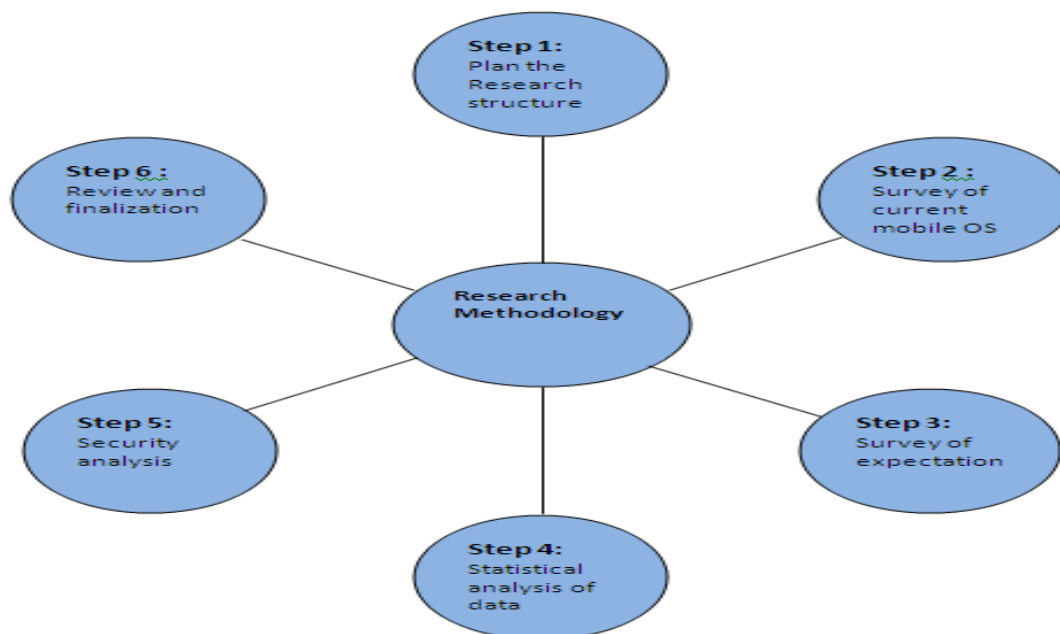

Fig 1. Research Methodology

2.1 Research Structure:

This study is organized based on the statistical analysis and expectations on mobile operating systems and its performance as well as security. Here validating the operating systems growth is recent period, which helps to identify the user/market expectations and present trends. For instance the current growth of Android operating system marks the availability of bunch options in each activity. Another importance target point is, various security mechanisms provided by the operating system; it might be similar in most of the systems but vary on its implementation

2.2 Market strategy of Operating systems:-

User expectations and trends are keeping changing each period of time. Now the era of smart phone, which makes the world in finger tips. Below table (Table 1) give a market trend.

OS Usage	iOS	Android	Symbian OS	Black Berry OS	Series 40	Samsung	Unknown	Sony Ericsson	Other
2009-01	35.56	0.66	39.31	0.95	0	0	14.73	0	8.8
2009-02	36.43	2.06	37.04	5.57	0	0	11.87	0	7.04
2009-03	39.6	2.18	35.12	5.97	0	0	11.29	0	5.82
2009-04	41.91	2.02	34.25	6.39	0	0	10.2	0	5.24
2009-05	37.32	1.86	39.11	6.92	0	0	9.88	0	4.91
2009-06	35.81	0.13	40.61	7.91	0	0	10.61	0	4.94
2009-07	34.2	2.21	24.06	8.55	0	0.45	23.63	1.87	5.04
2009-08	33.91	2.28	34.06	8.86	0	1.76	6.14	6.93	6.06
2009-09	31.13	2.32	36.29	8.92	0	1.94	7.12	6.79	5.49
2009-10	30.5	2.56	38.17	9.16	0	1.88	6.23	6.72	4.79
2009-11	31.56	3.31	36.17	9.73	0	1.85	5.93	7.03	4.42
2009-12	32.05	4.07	35.05	9.69	0	1.81	6.05	7.12	4.15
2010-01	33.13	4.54	34.16	10.28	0	1.69	5.76	6.89	3.54
2010-02	33.92	5.35	32.71	11.13	0	1.69	5.46	6.38	3.35
2010-03	30.13	5.9	34.51	12.73	0	1.69	5.71	6.21	3.1
2010-04	29.38	5.58	33.54	14.06	0	2.02	6.68	6.02	2.73
2010-05	29.01	3.94	32.92	14.15	0	2.86	9.09	5.9	2.13
2010-06	26.66	3.95	33.39	14.98	0	3.34	9.81	5.79	2.09
2010-07	26.05	7.91	32.04	16.45	0	2.93	6.77	5.47	2.38
2010-08	25.71	9.22	31.54	16.95	0	2.85	6.16	5.43	2.13
2010-09	22.85	9.79	32.69	17.9	0	2.96	6.59	5.61	1.62
2010-10	22.45	10.67	32.83	18.19	0	2.83	5.91	5.54	1.59
2010-11	21.94	11.61	31.93	19.25	0	3.49	5.32	4.9	1.56
2010-12	23.57	13.6	29.66	18.04	0	4.05	5.13	4.32	1.62
2011-01	25.02	14.61	30.25	15.03	0	4.33	5.21	3.91	1.66
2011-02	24.56	15.16	30.66	14.52	0	4.51	5.14	3.86	1.6
2011-03	24.38	15.8	30.61	14.1	0	4.73	5.1	3.75	1.52
2011-04	23.34	16.05	31.56	13.54	0	4.99	5.28	3.66	1.57
2011-05	22.09	17.63	31.36	12.94	0	5.08	5.77	3.46	1.67
2011-06	20.04	17.92	33.58	12.15	0	5.64	5.91	3.19	1.57
2011-07	20.03	18.93	32.45	12.48	0	5.76	5.88	2.97	1.51
2011-08	19.41	20.6	32.12	11.84	0	6.04	5.72	2.7	1.56
2011-09	21.21	20.9	31.83	10.72	0	5.6	5.9	2.26	1.58
2011-10	23.48	22.11	29.84	9.49	0	5.22	6.01	2.04	1.82
2011-11	24.21	21.9	30.95	8.44	0	5.43	5.29	1.93	1.85
2011-12	22.71	21.83	33.46	7.78	0	5.61	4.76	2	1.85
2012-01	24.04	23.21	31.89	6.94	0	5.84	4.45	1.75	1.88
2012-02	25.49	24.76	30.19	6.76	0	5.06	4.37	1.55	1.82
2012-03	23.99	23.61	31.48	6.43	0	6.05	4.78	1.62	2.03
2012-04	23.85	23.79	28.45	6.1	2.74	6.81	4.53	1.54	2.19
2012-05	22.95	23.81	20.25	5.66	11.84	7.18	4.59	1.44	2.27
2012-06	24.56	25.07	17.29	5.26	13.7	6.21	4.38	1.29	2.24
2012-07	25.41	26.53	13.47	4.96	14.73	6.71	4.51	1.14	2.54
2012-08	24.48	28.21	12.58	4.65	15	6.56	4.73	1.03	2.75
2012-09	23.63	29.25	12.22	4.54	15.14	6.72	4.83	0.98	2.69
2012-10	23.72	30.19	11.7	4.29	15	6.72	4.82	0.95	2.61
2012-11	23.73	31.67	10.93	3.93	15.07	6.52	4.75	0.89	2.51
2012-12	23.26	33.19	10.72	3.53	14.86	6.57	4.7	0.85	2.32
2013-01	25.85	36.87	8.86	3.39	12.86	5.03	4.31	0.71	2.12
2013-02	27.21	36.9	8.18	3.32	12.61	4.79	4.25	0.65	2.1
2013-03	27.18	37.19	7.98	3.27	12.56	4.7	4.28	0.63	2.2

Table : 1 Market Share of Operating Sytems

3.3 Expecting behaviors:-

At present the usage of mobiles are very high, same way the expectations also. Many of the daily activities got replaced by mobile from personal computer, so the respective user expectations also increased. Below are the highly using functionalities through mobile.

a) Search for information
b) Access social networks
c) Access local information and services
d) Search Videos
e) Accessing webpages
f) Entertainments
g) Shopping
h) Wifi , Bluetooth and GPS connectivity
i) Travel information.
j) Office activities e-mail, communicator etc.

3.4 Statistical Analysis:-

Many operating systems are available in the current market. As per latest statistics Google's Android and Apple's iOS are in front in the utilization. All operating systems are in race to bring new features and getting a leading role in the current market. Below diagram (Fig 2) and table (Table 2) give a better understanding.
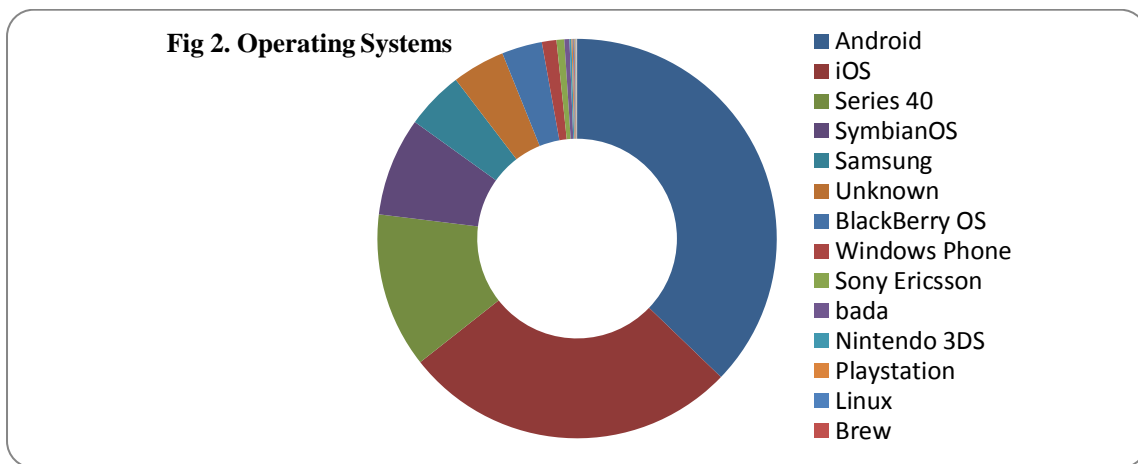

Fig 2. Operating Systems

Legend: Android, iOS, Series 40, SymbianOS, Samsung, Unknown, BlackBerry OS, Windows Phone, Sony Ericsson, bada, Nintendo 3DS, Playstation, Linux, Brew

Table 2. Market coverage of Mobile OS

Operating System	Percent
Android	37.19
iOS	27.18
Series 40	12.56
SymbianOS	7.98
Samsung	4.7
Unknown	4.28
BlackBerry OS	3.27
Windows Phone	1.18
Sony Ericsson	0.63
bada	0.41
Nintendo 3DS	0.16
Playstation	0.1
Linux	0.08
Brew	0.07
Nintendo	0.04
Motorola	0.03
LG	0.03
MeeGo	0.03
Windows	0.02
WAP	0.01
WinXP	0.01
JAVA	0.01
Maemo 5	0.01
webOS	0.01

Current era each and every activity has directly or indirectly relaying the internet features. Recent days 40% of internet usage is going through mobile devices. That is disclosing the importance of mobile operating systems. In 2008 Mary Meeker an analyst was predicted as "*Mobile to overtake fixed Internet access by 2014*". Most of the surveys are confirming that words. Nowadays mobile devices are highly using than personal computers for social network sites, weather reports, location maps, hearing music etc. Below diagram (Fig 3) and table (Table 3) give a better understanding.
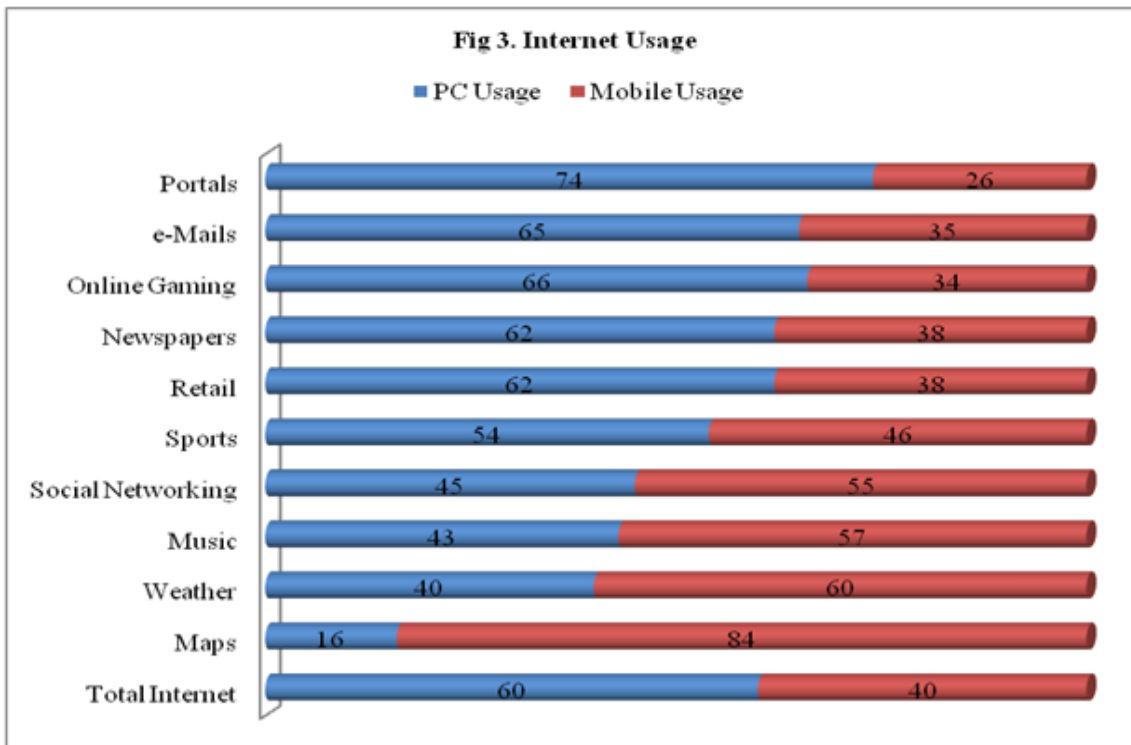
Fig 3. Internet Usage

Table 3. PC Vs Mobile Internet Usage

Items	PC Usage %	Mobile Usage%
Total Internet	60	40
Maps	16	84
Weather	40	60
Music	43	57
Social Networking	45	55
Sports	54	46
Retail	62	38
Newspapers	62	38
Online Gaming	66	34
e-Mails	65	35
Portals	74	26

Mobile browsers are playing major role in mobile operating system. Many of them relay the browsers with same importance as the independent applications. Below diagram (Fig 4) and table (Table 4) give better statistical details.

Table 4. Mobile Browser Usage Percentage

Browser Version	Percentage
Safari 6.0	39.80%
Android Browser 4.0	21.93%
Safari 5.1	5.09%
Safari 536	5.00%
Opera Mini 4.2	3.02%
Chrome 28.0	2.38%
BlackBerry	2.31%
Chrome 18.0	1.97%
Safari 5.0	1.96%
Opera Mini 7.1	1.89%
Safari 8536	1.80%
Opera Mini 4.1	1.08%
Microsoft Internet Explorer 9.0 Mobile	0.96%
Silk	0.85%
Microsoft Internet Explorer 10.0 Mobile	0.82%
Proprietary or Undetectable	0.75%
Chrome 29.0	0.72%
Safari 4.0	0.67%
Opera Mini 4.4	0.58%
Proprietary or Undetectable	0.56%
Opera Mini 4.5	0.55%
Symbian	0.47%

UC Browser	0.46%	Chrome 26.0	0.18%
Opera Mini 7.0	0.32%	Opera Mini 5.0	0.17%
Opera Mini 5.1	0.29%	Opera Mobile 12.1	0.17%
Safari 7.0	0.24%	Opera Mini 6.5	0.17%
Safari 7534	0.22%	Chrome 27.0	0.17%
Android Browser 5.0	0.20%	Safari 420	0.16%
Safari 10.1	0.19%	Safari 7.2	0.15%
Opera Mini 3.1	0.19%	Opera Mini 6.0	0.14%
Opera Mini 4.3	0.18%		
Opera Mini 4.0	0.18%		

Fig 4. Browser Usage

Legend: Safari 6.0, Android Browser 4.0, Safari 5.1, Safari 536, Opera Mini 4.2, Chrome 28.0, BlackBerry, Chrome 18.0, Safari 5.0, Opera Mini 7.1, Safari 8536, Opera Mini 4.1
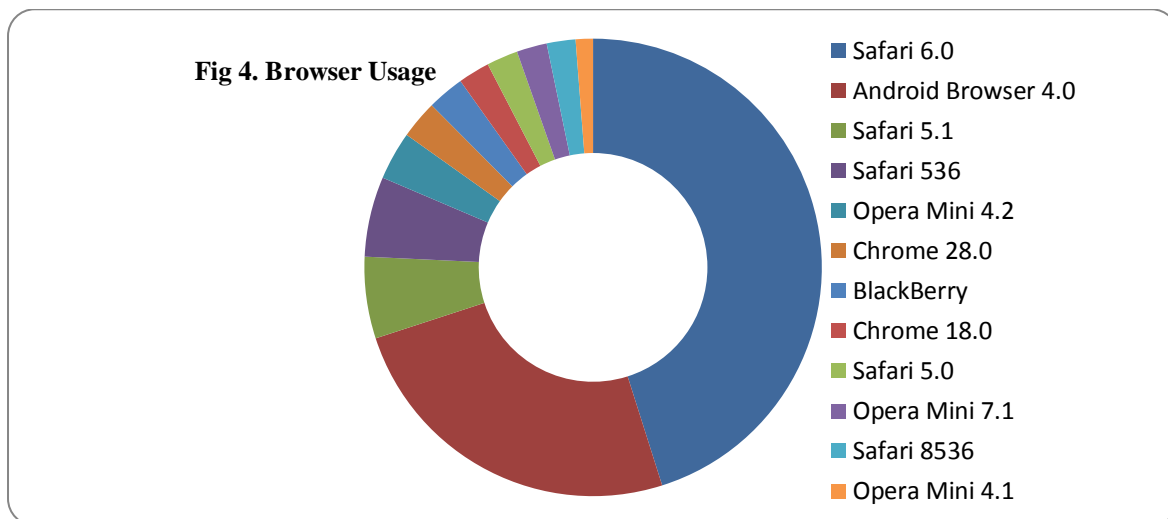
When talks about internet usage the mobile security comes in picture. Now many fo them are doing their personal activites through mobile, like bank transaction, onilne purchase etc. Most of this activities required to use secured information. So definitely the importance of mobile security is high. Most of the operating systems have some kind of common security activies, but the way of securities implemented might be varying from between operating systems.

3.4.1 Quick Glance To Leading Mobile OS

a) Android

Android operating system is the most popular in the current mobile platforms. This is designed by Google using Linux kernel. Every day more than 1 million new Android based devices are activated in worldwide. It is an open source platform, so many of mobile manufactures are customizing this and using as there key operating systems. Android use Linux kernel as its hardware abstraction layer between hardware and other software. This also provides a better memory management, process management, security options and network options. This is written in Java programming language and run in the Dalvik virtual machine. The key advantage of this operating system is anyone can customize this operating system. With the same reason the innovative growth of this OS is in peak. Android applications have common structure, mainly in views, recourse management, notifications, data storage, services etc.
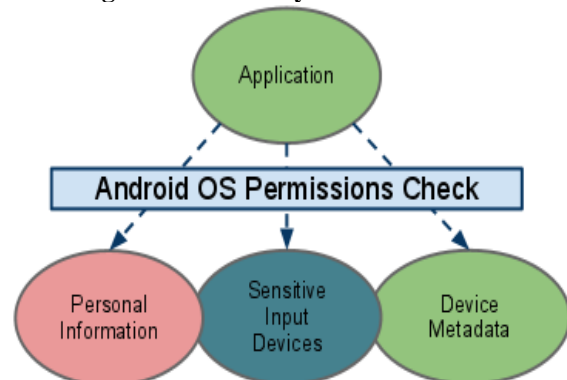
Safety and security: As Android OS is an open platform, the security mechanism is a the key challenge. Here in the base structure (Fig 5) is providing security check in application level.

Fig 5 : Base security structure

Securing an open platform requires robust security architecture and rigorous security programs. Android was designed with multi-layered security that provides the flexibility required for an open platform, while providing protection for all users of the platform. It was designed with device users in mind. Users are provided visibility into how applications work, and control over those applications. This design includes the expectation that attackers would attempt to perform common attacks, such as social engineering attacks to convince device users to install malware, and attacks on third-party applications on Android. Android was designed to both reduce the probability of these attacks and greatly limit the impact of the attack in the event it was successful. It seeks to be the most secure and usable operating system for mobile platforms by re-purposing traditional operating system security controls to:

a) Protect user data
b) Protect system resources (including the network)
c) Provide application isolation
d) Android provides these key security features:
e) Robust security at the OS level through the Linux kernel
f) Mandatory application sandbox for all applications
g) Secure inter process communication
h) Application signing
i) Application-defined and user-granted permissions

b) iOS

iOS is one of the leading mobile operating system, which others trying to catch up. Related to the same many patent related cases are going in many places. This OS is designed by Apple followed by Mac operating system. In first glance the user friendly feature is the key for this operating system. HTML5 technology started raising in mid of 2011, iOS very well using this one. iOS considered the foundation of the iPhone. This is designed for the iPhone but now supports iPod touch, iPad and Apple TV Businesses around the world are choosing iOS devices for their enterprise-ready features and powerful security. iOS works with Microsoft Exchange and standards-based servers to deliver over-the-air push email, calendar, and contacts. It protects your data by encrypting information in three separate areas: in transmission, at rest on the device, and when backed up to iTunes. You can securely access private corporate networks through industry-standard VPN protocols. And companies can easily deploy iPhone across an enterprise using configuration profiles.

Safety and security: iOS provides built-in security from the moment you turn on your device. Low-level hardware and firmware features are designed to protect against malware and viruses, while high-level OS features help to secure access to personal information and corporate data. To guard your privacy, apps requesting location information or data from Calendar, Contacts, Reminders, and Photos must first get your permission. You can set a pass code lock to prevent unauthorized access to your device and configure it to delete all your data after too many unsuccessful pass code attempts. This pass code also automatically encrypts and protects your stored email as well as allows third-party apps to encrypt their stored data. iOS supports encrypted network communication that apps can use to protect your sensitive information during transmission. And, in case your device is lost or stolen, Find My iPhone allows you to locate it on a map and remotely delete all your data. When you get it back, you can restore everything from your last backup.

c) Series 40

Series 40 is Nokia's mid-tier embedded software platform and designed in Java, its like a customised version. This was introduced in 1999, thrid gereration is introduced in 2005 and its fast gtrowth clicked in 2011-12 period. The key features of this operating system are simplicity, responsivenss and speed. Its major disadvantages are not supporting multitasking and donot have native code application interfaces for thrid parties. So this OS not supporting the applications not written in Java.

d) Symbian

Symbian is an open source (from 2008) operating system mainly used in Nokia Mobile Devices. The underlying OS was historically created by Symbian Ltd and licensed by Nokia and other phone manufacturers. Symbian OS is designed to make minimal demands on batteries and to have low memory. It is a multitasking operating system and very less dependence on peripherals. All applications are designed to work seamlessly in parallel. The use of technologies based on agreed-upon standards is a basic principle of Symbian OS, ensuring that applications are robust, portable, and interoperable. Memory management optimized for embedded software environment. Application support for international environment with built-in Unicode character sets. Symbian uses microkernel approach. The kernel manages system resources such as memory and is responsible for time-slicing the applications and system tasks.

Safety and security: The integrity and security of user data is of paramount importance. Symbian OS offers gate keeper type security. The system asks user permission to install any applications. There are three concepts, which are the foundation of Symbian OS platform security architecture.

Tiers of Trust: A mobile phone tends to be used by one person only, this is particularly true of smart phones which hold personal information such as contact details and calendar entries. The design of Symbian OS assumes this

Trusted Computing Base : It controls the lowest level of the security mechanisms and has the responsibility for maintaining the integrity of the system. The trusted computing base includes the operating system kernel, which looks after the details of each process, including the set of privileges assigned to it. Some Symbian OS phones are 'closed', that is they do not support installation of native add-on software; on such a closed phone, the kernel, including the kernel-side device drivers and the file server are the only fully-trusted components.

Trusted Computing Environment: This consists of further trusted software provided in the mobile phone by Symbian. TCE code usually implements a system server process – failure of one server should not threaten the integrity of the operating system itself: the kernel can restart the server and maintain that integrity. Each server has limited privileges to carry out a defind set of services. By not granting all privileges to all servers, Symbian OS limits the threat exposed by any flaw in, or corruption of, a server. By requiring servers to have certain privileges, it is possible to limit access to sensitive low-level operations to selected servers and, thereby, prevent misuse of these operations by other processes.

e) Windows

Windows is the most popular computer operating system. Past five years they are started to give more attention on mobile operating system also. It is offering new user interface with 'Metro' design. They designed Windows CE (Compact Edtion) specifically for handheld devices, based on Windows API. Later introduced Windows 7 version. Recent version Windows 8 mobile OS released at June 2012, its support, many of great fatures like multi core procssor support, hifi screen resolution, higher storage support and near field communications. This mobile OS is almost simulating the personal computer version of Windows 8. Windows 8.1 mobile version is progress and it's targeting the mobile markets in 2014.

Fig 6. Windows Phone 8 Application security model
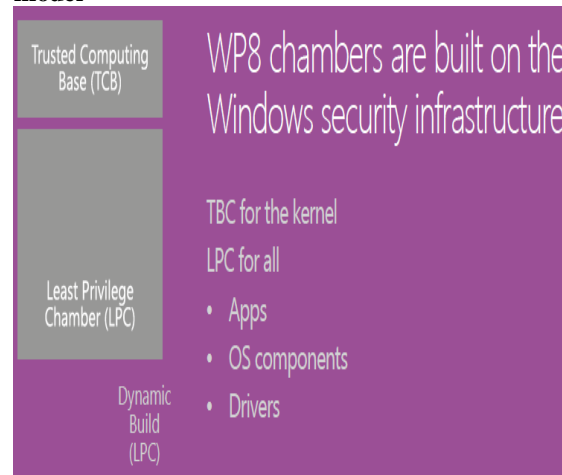
Safety and Security: Windows operating systems are mainly taking care Device encryption, Data Encryption, Data Leak Prevention and Digital Signature.

Device Encryption: Full internal storage encryption to protect information. It is built on Windows BitLocker architecture.

Data Encryption: It helps provide privacy and authentication between two communicating parties who have exchanged a shared secret.

Data Leak Prevention (DLP) : Information Rights Management (IRM) Helps prevent intellectual property from being leaked. It helps to protects emails and documents on the phone from unauthorized distribution. Easy to deploy on Exchange Server and SharePoint Active Directory Rights Management supports all your Mobile Information Management (MIM) needs.

Digital Signature: It helps to authenticate another party, or information sent by that party, without prior exchange of a shared secret.

f) Blackberry

The BlackBerry OS is the proprietary mobile platform developed by RIM (Research in Motion), exclusively for its BlackBerry smart phones and mobile devices. It offers native support for corporate mail via MIDP, which enables effortless wireless sync with Microsoft Exchange, Lotus Domino and email, contacts, calendar, notes and so on, while used along with the BlackBerry Enterprise Server. This OS additionally supports WAP 1.2. Its network architecture is differing than other operating systems.

Fig 7. Blackberry security modal
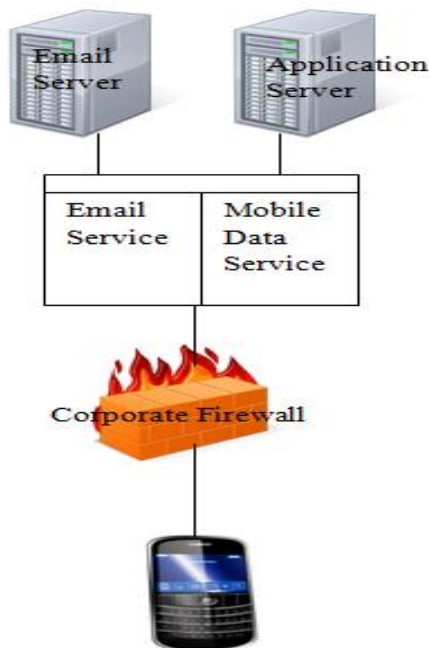
Blackberry provides end to end encryption. It is using two encryption options. Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES). Data sent to the BlackBerry smart phone is encrypted by BlackBerry Enterprise Server using the private key retrieved from the user's mailbox. The encrypted information travels securely across the network to the smart phone where it is decrypted with the key stored there. Its enabled RSA SecurID Two-Factor Authentication. Additional authorization also available when users access application data or corporate intranets

3.5 Security Measures

Importance of mobile security measures are increasing day by day. Now many of personal and professional information is stored in mobiles. Mobile Os are under target to attackers as other operating systems. Recent days mobiles users are highly demanding the internet features. Many of the users are wish to carry single compact device for multiple activities.

As per MSRA(Mobile Security Reference Architecture) provides an architecture pattern that can use to ensure the confidentiality, integrity, and availability of data accessed through a mobile computing solution.

Major mobile security measures require in mobile operating system.
a) Authorization
b) Device Management
c) Identity and Access management.
d) Data management
e) Logging
f) Personnel and Facilities Management
g) Network Access Control
h) Software Validation
i) Patch Management

When choosing a mobile based on operating system, consumers can validate the required security functions are available on their device. Device management includes OS configuration, software patches, data management etc. Based user identity access activities have to enable. The Logging security is includes various policies and infrastructure management. When installing new software it has to validate whether it is provided by genuine software provider. Required periodic patches update to maintain the device as secure.

As per mobile security experts the analysis reveals today's mobile platform have wide difference. Device management, application security and corporate e-mail support are almost fine but still required improvements. Below bar charts are giving a brief idea on various security measures between Android, iOS, Windows and blackberry comparison on built-in security, data protection, authentication, device protection, application security, mobile device management, corporate managed e-mail, device firewall, security certifications, virtualization.
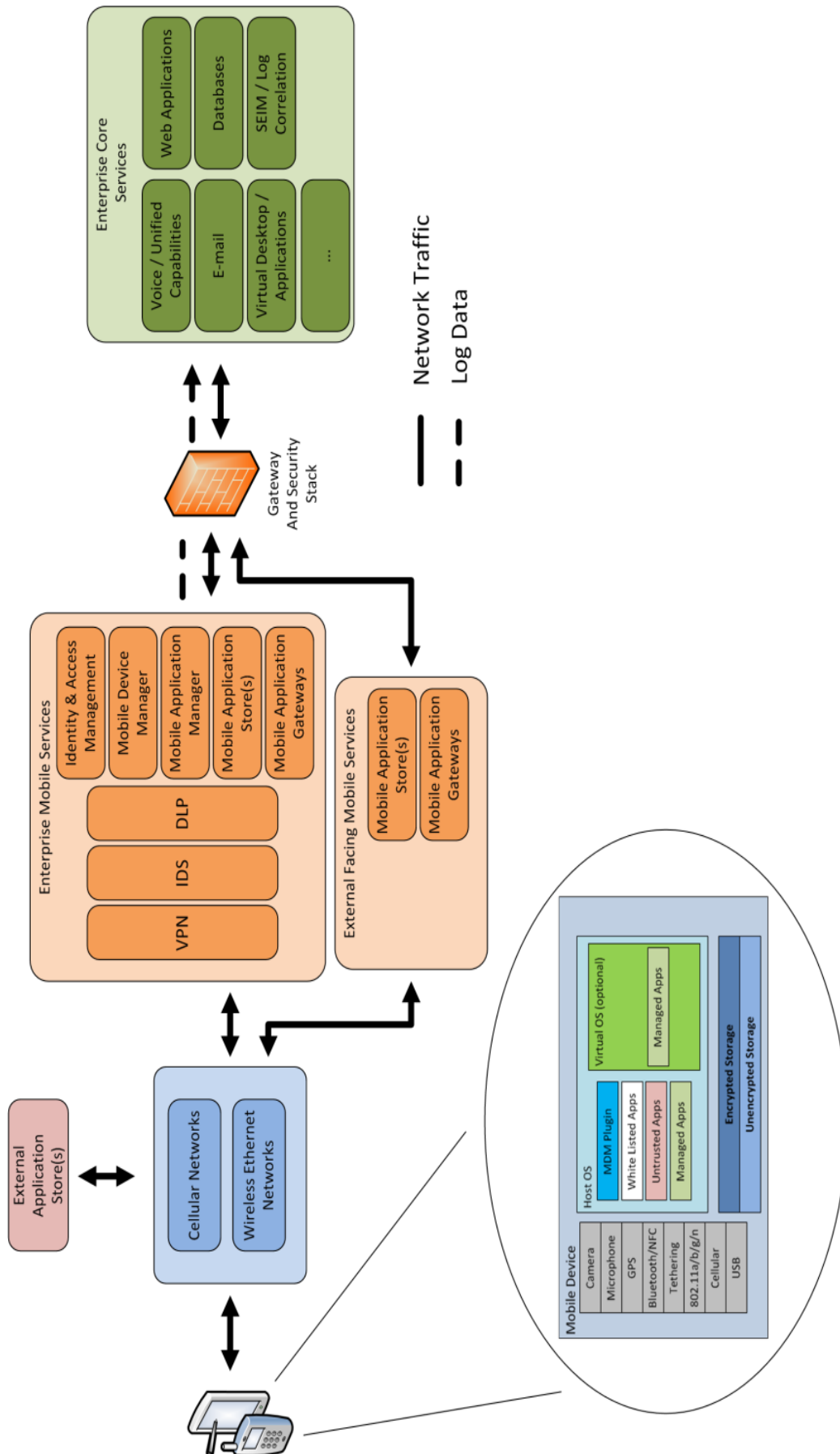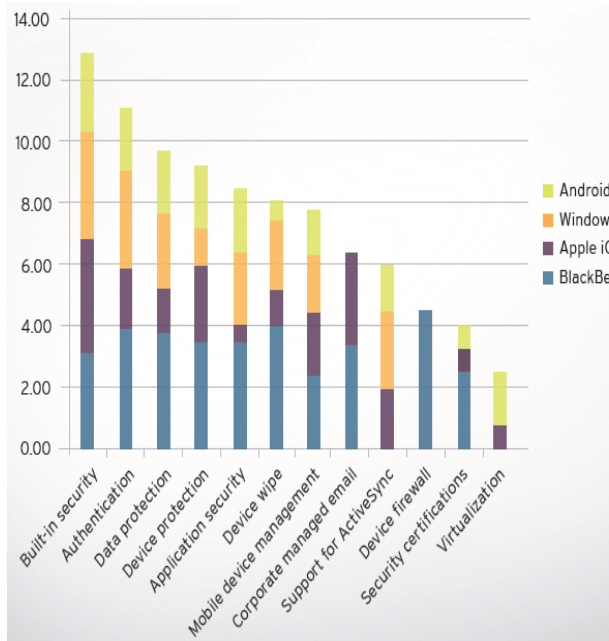
Fig 8. Mobile Security Conceptual Architecture

Fig 9. Security Comparison

4. RESULTS AND FINDINGS

Based on the analysis and data collected, we can finalize best option. The analysis is giving a brief idea about the market trends on mobile operating systems. The present trend leads Android and iOS operating systems in market.

Android is a freeware operating system from internet gaint Google. Its base version itself provides many of the features, which gives lot of popularity. Many of mobile companies did their own research and customization on top of this and making that more popular. As it as wide users and development peoples huge number of software are available in market. This also provides a better memory management, process management, and network options. As Android OS is an open platform many of them doing OS level development, it is security challenge.

Apple derives the iOS operating system, which is popular in mobile software perfection and professionalism. Multiple mobile thoughts they contributed to mobile technology. Many of other operating systems are following their features. Comparatively iOS is giving better security than android.

Few of other operating systems are gives greater security. Blackberry maintains separate security architecture. Many of them in using blackberry OS for professional activities.

5. Conclusions

When filter out the analysis portion, we can bring up few key points which helps to choose the apt and secured mobile OS. Uses have some priority features when choosing the operating system based on their work nature or personal interests. It's like user friendly, high security, professional motions, multiple capabilities, official activities, entertainment, financial activates, search, news etc. Based on user priority ranking they can check which operating system is capable to fulfill user requirements. Based on that they can choose apt and secured one.

6. References

[1] 'Statistical reports reference for various operating systems' http://stats.areppim.com/

[2] 'Statistical reports reference for mobile and personal computer http://www.smartinsights.com/

[3] 'Msec Research Group' https://www.msec.be/

[4] 'Mobile Security Reference Architecture' https://cio.gov/

[5] 'Enterprise Readiness of Consumer Mobile Platforms' http://www.trendmicro.com/