IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

A Study on Mobile Cloud Computing: Security and Services

Lekha Ashok Sevalia
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *The paradigm of conventional Internet computing is changing thanks to a young and promising technology called cloud computing, which is also likely revolutionising the entire IT sector. Taking advantage of the quick development of wireless access technologies, cloud computing is anticipated to grow in the mobile environment. These mobile applications are based on models and techniques from mobile cloud computing. Users can access high-quality on-demand cloud apps and distant data storage in the Mobile Cloud environment without being constrained by the need to buy and maintain their own local gear and software. The key barrier stopping cloud computing from becoming more extensively used is data security, which is still a major worry. This worry stems from the fact that personal information kept in public clouds is handled by for-profit service providers who might not be completely reliable. As a result, there are a number of security and privacy concerns that must be resolved. This paper will first give you an overview of Mobile Cloud Computing, Security Threats, Security Issues and Challenges.*

Keywords: Mobile Cloud Computing, Security Threats, Services Issues and Challenges.

I. INTRODUCTION

Mobile Cloud Computing (MCC) is a latest technology used by people in their day to day lives. Mobile Cloud Computing is the combination of Mobile Computing, Cloud Computing and wireless network. All these three components act together for creating an application which provides a large computation for the users. The users get the benefits of high storage and easy access. MCC has in much demand nowadays as it's an option for app developers. MCC has made possible ways where users can use unlimited online storage.

In addition, with wireless network like WIFI, Ad hoc Network may be browsing the web easily. Thus, people use such mobile phones for their working and entertainment purpose as their main choice.

So, what do you mean by Mobile Computing? As per Wikipedia it is stated that Mobile computing is human–computer interaction in which a computer is expected to be transported during normal usage, which allows for the transmission of data, voice, and video.

Mobile Computing includes communication, hardware and software where communication issues include ad hoc network, protocols, date format etc. Software deals with mobile applications. Hardware includes device components. Mobile Computing is used many Web Browsers like, Internet, Firefox, Google etc.

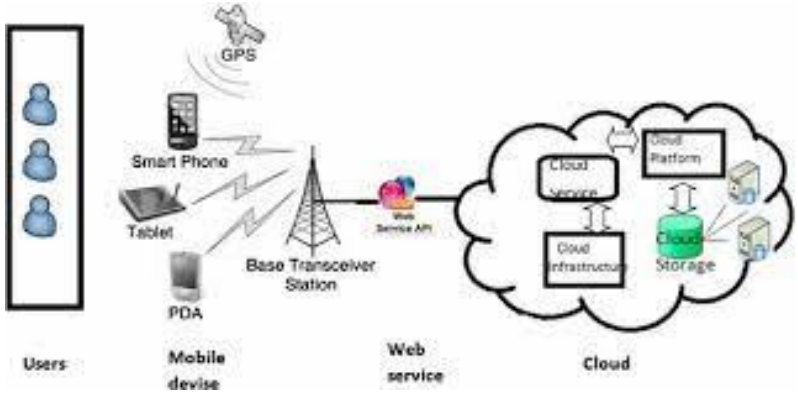

Fig: Mobile Cloud Computing Architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

II. SERVICES PROVIDED BY CLOUD

2.1 Platform as a Service

Stage as a Service (PaaS) extends the advantages of SaaS for applications to the world of package development. Additionally, PaaS is printed as a processing phase that permits the creation of the web applications efficiently, quickly, and without regard to the nature of purchasing and maintaining the package and base at a place it lower. With that exception, fairly speaking, PaaS and SaaS are basically comparable.

It's a step for rather than being packaged and sent over the internet the creation of a bundle that is sent over the internet.

2.2 Infrastructure as a Service (IaaS)

Might be a style of conveying Cloud Computing framework - servers, capacity, network partner degrees usable frameworks - as partner degree on-request administration. as opposed to looking for servers, programming, server farm space or organization instrumentation, customers rather buy those assets as an exceptionally re-appropriated administration on request.

2.3 Software as a Service (SaaS)

Has turned into all the style lately in light of multiple factors. for instance, SaaS is drawing in to the client because of it moves the in cumbrance and worth of equipment and programming bundle planning and upkeep from the client to the merchant. SaaS conjointly gives a few benefits to the dealer, WHO will right now create and keep up with the applying on one stage and see quickly anyway clients use choices of their application.

III. MOBILE CLOUD COMPUTING SECURITY

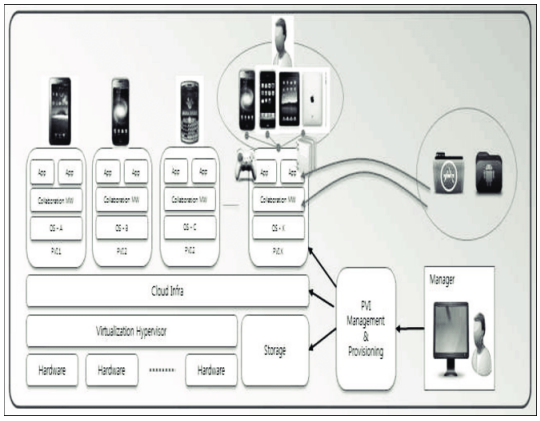

Fig: Mobile Cloud Computing Security

Risks to smartphone and tablet platforms are the main focus when talking about mobile cloud security threats. Additionally, these dangers are separated into five groups.

1. Physical Threats.
2. Application based Threats.
3. Network base Mobile Security Threats.
4. Web based Threats.
5. Other active attacks.

- **Physical Threats:** We feature mobile devices, which are valuable and compact, all throughout India. We have a tendency to use it for all personal and/or professional purposes. The physical security of our phones is also crucial because they may hold vital data.
- **Device Possession:** When it comes to information continuing mobile devices, every business and employee is tightly held, and questions about information possession and liability have still not been resolved. As employees utilise company devices for personal activities and personal devices for business purposes, necessary information privacy issues may arise between employees and businesses.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

- **Lost or taken devices:** One of the most common mobile hazards is having your device lost or stolen. We have a propensity to consider the cost of our mobile device, not just its value but also the delicate personal or structural data that it should hold. Theft or loss of it has immediate repercussions because an entirely undesired person can access all the data you have on the device (bank accounts, social network passwords, contact lists, etc.) and use it for bad purposes.

Application Based Threats

- **Malware:** is a software that acts maliciously when installed on your phone. Malware can add charges to your account without your awareness, send unwanted messages to your contact list, or give a malicious user control over your device.
- **Spyware:** is intended to collect or exploit personal information without your knowledge or consent. Decision histories, text messages, user locations, internet histories, contact lists, emails, and private images are among the information that spyware may occasionally target. For fraud or money laundering, this stolen data is used.
- **Vulnerable Applications:** Applications that have security holes that could be used for nefarious purposes are referred to as vulnerable apps. Such flaws allow a malicious party to gain access to confidential information, carry out undesired deeds, prevent a service from operating as intended, or install programmes on your device without your knowledge.
- **Unlicensed and unmanaged applications**: Applications that are not permitted or licenced could cost your business money in legal fees. Applications must be regularly updated to fix any vulnerabilities that could be used to gain unauthorised access or steal data, regardless of whether or not they are licenced. There is no assurance that end users' mobile devices are being updated, notwithstanding the lack of sight into them.

Network base Mobile Security Threats

Mobile devices typically enable native wireless networks in addition to cellular networks (Wi-Fi, Bluetooth). Each of these network types is capable of hosting a wide variety of threats:

- The main weakness in any mobile app or any app that uses cellular or native networks is caused by network exploitation. Once linked, they will secretly install spyware on your phone.
- Wi-Fi Sniffing intercepts data as it is transmitted between the device and the LAN access point over the air. Many web pages and programmes have inadequate security protections, sending unencrypted data across the network that can be easily scanned by someone capturing data as it travels.
- Address Impersonation: Address impersonation attacks take place when the malicious party has access to some editing tools and can insert any chosen scientific discipline address into the packet. Each host on the network is identified by a unique scientific discipline address. The provision and destination scientific discipline addresses are two pieces of knowledge that must be in clear text and are included in the data science packet. As a result, the data science address is the identification in the network layer for which no authentication is offered.

Web based Threats

- Phishing scams: Phishing scams: These involve sending links to websites that ask for personal information such passwords or account numbers via email, text messages, Facebook, and Twitter.
- Drive-by downloads: Are programmes that are installed on a device without the user's knowledge or consent. The key transmission can also be started by sending an email message with machine-readable text nomenclature or by visiting an internet website.
- Browser exploits: Designed to start from the Delaware browser or from third-party extensions, such as Flash player, PDF reader, picture viewer, etc., in order to take advantage of browser flaws. You can start a browser exploit that will install malware or carry out other harmful actions on your device just by visiting an unsafe website.
- Jail broken devices: Apple's iOS operating system is under danger due to jailbroken smartphones. iPhones and iPads, which are generally safer than other operating systems, lose a lot of their protection through jail breaking, which lifts restrictions imposed by Apple and enables users to get root access to the software. Users will start to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

associate their iOS devices with the ability to transfer extra apps, extensions, and themes that don't seem to be available through the iTunes App Store or with the ability to use them with a different cell carrier than the one for which they were originally intended. However, a 552 4 breakout on a mobile device at the International Conference on Electronics and Communication Systems (ICECS'14) poses a serious threat to the company network by jeopardising internal security.

Facet address space layout organisation (ASLR) and native OS execution space organisation are two measures taken by Apple and Golem to thwart the havoc that jailbreaks can create. Enterprise IT departments, however, can't rely only on such safeguards to keep an eye on devices that have experienced the breakout technique and restrict them access to their networks.

Other Active Attacks

Once the malicious host has established a network connection and understands the data science address to use, it will attempt to disrupt other computers on the network. The network prefix that has been assigned to the connection on which the network jack is attached can be inferred by the user. Additionally, a stranger can guess a variety of passwords to use, which when combined with the network prefix gives him a scientific discipline address to use on this connection or else earn money by attempting to get into the hosts on the network by guessing user-name/password pairings. In order to stop such assaults, worn-out public network jacks should be connected to a spy that requires all nodes on the link to be registered.

IV. SECURITY ISSUES IN MOBILE CLOUD COMPUTING

4.1 Mobile Terminal

It is an open working framework which permits remote access of web whenever anyplace. It additionally upholds third party programming and personalization. So, security issues in portable terminals are vital and as such beneath we talk about them as for malware, programming weaknesses and other perspective.

1. Malware: Malware gains admittance to individual data of clients as they naturally downloaded and conveyed which stays obscure to the clients. So many enemies of malware programming have been grown however because of restricted assets and limit of versatile terminals huge computational assets are hard to accomplish. Thus, answers for malware identification and counteraction in versatile terminals are required.
2. Software Vulnerabilities: If there should be an occurrence of use programming, client name and secret word are moved to organize by utilizing FTP and these are put away in clear text design. This permits unlawful access of cell phones from PCs on a similar organization thus private data not remains got. While there are code errors in the functioning framework, and in certain cases, they lead to attackers destroying cell phones.

4.2 Mobile Network Security

There are many ways for the cell phones to reach the company, including using telephone services, sending Short Messaging Service (SMS), and other internet providers. Organization can also be accessed by modern mobile devices via Wi-Fi and Bluetooth. These access techniques thus create security risks and harmful assaults.

4.3. Mobile Cloud

Stage dependability and information and security insurance are two concerns that are addressed in relation to the security in flexible clouds. The following discusses these two:

a. Dependable platforms: Because the cloud provides a large amount of valuable data assets, there is always a risk of being targeted. These attacks could come from insiders, external viruses, or cloud users. The attackers want to completely destroy the cloud administrations. For instance, a DOS (Denial of Service) attack can shut down cloud administrations by obliterating the available stage.
b. Protection of information and privacy: The owners and managers of the customers' information reside in segregated locations, and in addition, the clients have no awareness whatsoever of the precise location of the building where their information is kept. Thus, information assurance and protection are of extraordinary worry in portable distributed computing climate.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

4.4 Confidentiality

Since information from mobile clients is handled by open organisations and stored on open servers, privacy is a fundamental demand. Therefore, there is a considerable risk of unauthorised access to portable clients' information, which implies that the confidentiality issue is a significant challenge for portable cloud specialist co-ops.

4.5 Availability

Accessibility means that customers can always get help from cloud administration whenever they need it, 24 hours a day. Different attacks that affect accessibility exist, but flexible distributed computing specialist co-ops must thwart them and constantly ensure that the assistance is available for mobile clients.

4.6 Authentication and Access Control

This entails identifying the genuine user of the system using certain login procedures or another tool known as confirmation. Admittance control refers to granting access to limited assets to confirmed framework clients who believe they need to complete a task. Access control entirely controls client actions including reading, writing, refreshing, deleting information, and so forth.

4.7 Integrity

Integrity is the avoidance of data loss or change while it is being transmitted across a public network. Integrity is concerned with the accuracy and consistency of user data.

4.8 Privacy

Through confidentiality, integrity, and authentication, privacy refers to the protection of a mobile user's personal data when communicating in the cloud.

V. CHALLENGES IN MOBILE CLOUD COMPUTING

Smartphones employ the cloud computing service known as "mobile cloud computing. "Tablets, or both. In order to provide cloud services to mobile computing users, mobile computing and cloud computing combine to develop mobile cloud computing. flexibility, resource pooling, measurable services, on-demand self-service, and broad network [7][8] access. Wireless connection technology is used in mobile cloud computing to mobile and cloud communication [9]. Because to the integration of mobile. We encounter numerous challenges with computing, cloud computing, and wireless connectivity. Problems in mobile cloud computing, include the dearth of mobile device resources, stability issue brought on by cellular network restrictions and network costs elasticity difficulty, access increasing at different periods in mobile cloud computing challenges with security and privacy, channel bandwidth, energy efficiency, and quality of service, among others [10].

VI. ADVANTAGES OF CLOUD COMPUTING

MCC still has a lot of benefits and advantages over a standard IT environment, despite the fact that it faces a sizable number of problems and difficulties. This section focuses on a few benefits that still make MCC a promising technology for the future [7].

- Extended Battery Life: In advanced mobile devices like smart phones and tablet computers, battery output longevity has always been a challenge, especially when they run demanding apps. By employing cloud resources to run complex and time-consuming applications in the cloud, MCC helps the user. The battery life of mobile devices is greatly extended by cloud-based application execution.
- Enhanced computing capacity and data storage: The MCC gives mobile users a platform for cloud storage of substantial amounts of data. For mobile users, storage capacity is usually a major concern, which MCC solves. By establishing a wireless network connection with the cloud, mobile users can access storage. Amazon Simple Storage Service is the first example of a cloud storage provider (Amazon S3).
- Scalability: With less work and infrastructure adjustment, cloud service providers can increase the scope of their cloud services. Without worrying about resource usage, they may easily add applications and services.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

- Multi-tenancy: The same cloud resources are shared by cloud service providers and data centre owners in order to offer users various applications and services. Additionally, the two split the expense.

VII. APPLICATIONS OF MOBILE CLOUD COMPUTING

1. **Mobile commerce:** By offering mobile commerce (m-commerce) via portable electronic devices, MCC makes life simple for business. Due to limited bandwidth, complicated mobile architecture, and significant security threats, applications like financial, shopping, tickets, etc., are facing some significant difficulties. But by integrating m-commerce applications into the cloud environment, the MCC offers a solution to these problems.
2. **Mobile Education**: Mobile learning was created as a mix of electronic learning and mobility (m-learning). However, problems including high mobile device and bandwidth costs, slow network speeds, and a shortage of electronic educational resources are proving to be the main barriers to m-learning. However, the cloud's huge storage and powerful processing capabilities introduce the concept of cloud-based mobile learning and remove its obstacles.
3. **Healthcare**: The mobile medical applications have a lot of restrictions, such as limited storage space, lack of data confidentiality and privacy, etc. MCC, on the other hand, does away with the drawbacks of conventional medicinal uses. Due to the availability of on-demand services in the cloud, m-healthcare enables mobile users to efficiently access medical resources.

VIII. CONCLUSION

Due to the numerous benefits and uses it provides to mobile users, mobile cloud computing (MCC) is a new and futuristic technology. MCC provides data processing and storage capabilities to mobile users with minimal resources, making it a highly promising technology in the near future. By outlining its design, benefits, and applications, I have provided a thorough knowledge of MCC in this work. I have mostly concentrated on drawing attention to the problems and difficulties associated with MCC, such as data security. The major goal of this study is to pinpoint the problems and obstacles that impede mobile consumers from utilising cloud services.

In order to reduce user security worries, mobile service providers can benefit greatly from this research by enhancing the security technologies and methods utilised for cloud security.

IX. ACKNOWLEDGEMENT

I would like to acknowledge the University of Mumbai, Mumbai, India to give me the opportunity to do the research work under the title “A study on Mobile Cloud Computing: Security and Services”. I would like to acknowledge the college L.B.H.S.S Trust’s Institute of Computer Application, Mumbai, India to support me during the research process.

REFERENCES

[1]. Prashant Pranav, Naela Rizvi “Security in Mobile Cloud Computing: A Review “
[2]. Hero Modares, Jaime Lloret, Amirhossein Moravejosharieh, Rosli Salleh “Security in cloud Computing”
[3]. Abid Shahzad, Mureed Hussain “Security Issues and Challenges of Mobile Cloud Computing”
[4]. Rahul Neware” Survey on Security Issues in Mobile Cloud Computing and Preventive Measures”
[5]. Solanke Vikas S, Kulkarni Gurudatt A, Katgaonkar Pawan, Gupta Shyam “Mobile Cloud Computing: Security Threats”
[6]. Abdullah Gani, Han Qi “Research on Mobile Cloud Computing: Review, Trend and Perspectives”
[7]. M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology”
[8]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems”
[9]. N. Fernando, S. W. Loke, and W. Rahayu "Mobile cloud computing: A survey," Future Generation Computer System.”
[10]. R. Neware and A. Khan, “Cloud Computing Digital Forensic challenges”