***TOPIC***

***Authors***

***Abstract****­­****—* In the paper, we describe the privacy and security issues faced by the Mobile Cloud Computing(MCC) technology . The issue faced in integrating green computing technology is discussed in this research paper.**

***Keywords—*Privacy, Security, Green Computing, Service**

I.INTRODUCTION

Applications created for the mobile can be classified as online and offline. Offline could lead to have a negative impact on the cloud structure on emergence, since it has a reliance on the mobiles abilities unlike the online mode. In the online mode, Cloud enable the mobile to have an interaction with the servers and thus this will be beneficial as the mobile having limited resources or abilities will be able to able to execute operations without the need to carry them locally. This paper provides a comprehensive study of the Architecture of the Mobile Cloud Computing, Security, Challenges that the technology faces and solutions for the same, and discusses the Future of the technology. The paper is organized into various sections from Introduction to Conclusion.

II.CHALLENGES AND SOLUTIONS

In MCC there exists challenges in various parts like operations, services of the applications, management of data, security, privacy etc… In addition, the Quality of Service can be easily affected by the presence of the varying landforms, weather and buildings. In the following section, we will look at these challenges and discuss challenges and needs in different important areas stated below and further discussed in the paper:

1. Privacy
2. Threats
3. Architecture and Infrastructure of Mobile Cloud
4. Quality of Service
5. Green Computing
6. Privacy:

Unwanted or unscrupulous emails you receive everyday may constitute an attack or violation of your privacy. These emails are inexorable and they cannot be stopped. A large amount of personal information is collected by the cloud providers which is equivalent to a treasure of information that is yet to be explored. This information stored on cloud serves to be detrimental to the personal privacy and has long term effects, we have not come across yet.

Cloud has been efficient in solving the problem of storing the data on the initially used computer hard disks or the USB drives, thereby reducing the amount of data being compromised when the USB is lost or the computer is either sold or recycled. However, there are other problems that the cloud possess:

* The providers of the system are responsible for protecting the data as the users are do not physically possess the storage.
* If the users, wishes to change the cloud and wants to migrate to some other cloud provider, migration of this data can be a challenge. It cannot be verified too whether the data on the old cloud will be completely deleted.
* What if the cloud provider goes bankrupt? Or the cloud providers discontinue the service? In that case what would be done with the data? In addition to the above problems, another problem that arises is that there do not exist enough means to check the safety of storing data on the cloud and to select the safest cloud provider. There do not exist enough means for a general user to verify if their data is safe or is it being shared with unauthorized parties for any kind of hideous functions. With the growth of these mobile clouds, the privacy problem might become even more serious and detrimental. Governments are trying to impose laws, but the free service providers earn from advertisements, and these advertisements usually demand personal data. If too much protection is provided, it might even lead to change of the providers to fee based services.

The solution to the problem is, providing the users with more transparency about the process i.e. about eh information that is being collected, the information that is being shared or sent out. In addition to the transparency the users shall be given more controls and flexibility of choices, to select the privacy preferences.

1. Threats:

Mobile loud systems can take advantage of the monitoring, malware protection, security detection etc… but this does not imply that that these applications are totally safe. It only implies that the difficulty of the violation or attack or invasion on the system has considerably increased, and its not easy to break into or cause any kind of breach.

The issue that concerns the cloud providers is about the security of these platforms. There can be threats to the system, which can be divided into three categories:

* A. Physical threats:
* Challenge: The devices can be stolen, or lent to someone, which can result in access to the personal data or applications. Although, the devices are equipped with security systems, they can often be broken into by methods and applications stored in the devices, sometimes give direct access to the data stored on the cloud. The SIM(Subscriber-Identity-Module) cards can be easily removed from most of the phones thereby leaving the access to anyone who has the card.
* Possible Solution: Sensitive data is usually accessed at the application level, so to protect this data, the developers can add here an extra level of security. Also, the SIM cards should not be used to store too much data. Biometrics can be used in the security system of the device to keep the security of the device effective. Also there should be ways to take back up of data from the cloud, which has been lost in the device.
* B. Mobile Network Security threats:
* Challenge: Smart are accessible using various access facilities like connection to internet using 3G, 4G or 5G cellular networks, Wi-Fi, Bluetooth. Using the above services, smartphones can use Internet Services, make phone calls, using Short Messaging Services (SMS) etc… These services have interfaces which possess dangers of breach of data and is susceptible to various attacks. They are all a part of wireless networking technology, unlike wired networks they are more susceptible to attacks likes eavesdropping, man in the middle attack, denial of service attack. There are other fraud related threats too which the wireless networks are vulnerable to. Dealing with them is a major challenge. The MCC is inherently federated and highly virtualized, thus there is a need of an approach that is developed to manage identities across different clouds.
* Possible Solution: The primary solution will be to provide education to all the smartphone users about the correct ways of utilizing the networks. There is a need of established policies to govern the use of these devices and networks. An additional security benefit can be attained when we use One Time Passwords (OTP) for authentication instead of the stored passwords. There should be strict rules for the people who can access the data of the cloud, to prevent unauthorized access. There should be new security controls that stand above the cloud providers.

C. Malware threats:

* Challenge: As the number of the smartphone users is increasing, the Web based network is exponentially expanding, thereby attracting malware creators towards the highly sophisticated smartphones. These malwares pose a serious security issue in the form of phishing attacks, identity theft, viruses, botnets and spams. Mobile devices use a wide array of technology to interact with each other and thus there is a requirement of protection from sophisticated threats to the security. The increasing number of applications per user makes the identity layer harder.
* Possible Solutions: As a solution to this challenge, official software can be used authorized by the cloud providers, and they should be pre-installed on the devices. When the devices are attacked by the malwares this software would be used in effectively restoring the back up. These threats can be avoided by providing the users with the education to use the mobile networks or applications in a safe and conducive way. Network Infrastructure should be upgraded to help the user to restrict any type of malware, spyware and other unauthorized sites/spams using anti malware, anti-spyware and other security sites.

1. Architecture and Infrastructure of Mobile Cloud:

There are various papers available on the subject addressing mobile cloud infrastructures and architectures. On observing these papers, we found out that there are few issues and needs in the mobile cloud infrastructures. Two of them are:

* Cloud computing Infrastructures that are network oriented: Many challenges in network cloud infrastructure need to be addressed to meet the demands of the latest generation of cloud services, which provides auto resource provision, balancing the load, improvised standards of connectivity and green computing.
* There is a need for the new technology for connectivity and solutions: In the present systems, there are issues like limitations on the existing network bandwidth, speed in compatibility between the servers used for computing and networks. To resolve these issues, we need an improvised technology and infrastructure solutions.

1. Quality of Service:

Unlike the wired networks, the MCC system is based on wireless networks, which do not use any physical connections. Thus due to the existing clearance in network overlay, the rate of transfer of data in the MCC environment is constantly changing and discontinuous. Additionally there is a large distance between the data centre present in large enterprises , the Internet service provider resources and the end users. In such kind of connections the latency delay might be 200 milli seconds in the last mile unlike that in the wired networks (which has latency delay of 50 milli seconds).

Various other factors like weather, varying application throughput, user mobility etc… lead to the changes in the bandwidth and network overlay, thereby increasing the handover delay in wireless networks.

1. Green Computing:

In past few years Green Computing has remained the most interesting and hot topic of the discussion and there are various research projects being taken up with respect to the conservation of the energy involved in the computing.

The protocols to support mobile communication in MCC need to be more energy efficient. There is a need for energy efficient migration and synchronization techniques. We need an upgradation using more efficient technologies for the future wireless connectivity infrastructure, which can deal with various and networks and technologies and make the consumption of energy more efficient. Infrastructure that is Energy Efficient and similar data centres are the necessary requirement for the future technology. The future infrastructure of cloud storage and networks must include energy efficient resource allocation and management methods and solutions. There is also a need of solutions that can cross different layers such as infrastructures, platforms, mobile SaaS (software development and deployment approach) to provide system-level energy monitor and analysis so that cost-driven and green-based resource allocations and management decisions can be made.

REFERENCES

[5] Imad A. Elzein and Moustapha Kurdi, “Analyzing the

Challenges of Security Threats and Personal information in

Mobile Cloud Computing Infrastructure”, 02 June 2020,

IEEE Conference. DOI:[10.1109/ICD47981.2019.9105711](https://doi.org/10.1109/ICD47981.2019.9105711)

[6] Imen Merdassi, Cherif Ghazel and Leila Saidane,

“Surveying and Analyzing security Issues in Mobile Cloud

Computing”, 1-3 Dec. 2020, IEEE Conference.

DOI: [10.23919/PEMWN50727.2020.9293077](https://doi.org/10.23919/PEMWN50727.2020.9293077)

[7] [Ruay-Shiung-Chang](https://ieeexplore.ieee.org/author/37273837400), [Jerry Gao](https://ieeexplore.ieee.org/author/37279696100), [Volker Gruhn](https://ieeexplore.ieee.org/author/37267105100), [Jingsha He](https://ieeexplore.ieee.org/author/37278606700)

, [George Roussos](https://ieeexplore.ieee.org/author/37297438000)and [Wei-Tek Tsai](https://ieeexplore.ieee.org/author/37270013800), “Mobile Cloud

Computing Research - Issues, Challenges and Needs”,

10 June 2019, IEEE Conference.

DOI: [10.1109/SOSE.2019.96](https://doi.org/10.1109/SOSE.2013.96)