Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.972 – 977

RESEARCH ARTICLE

Mobile Cloud Computing: Issues from a Security Perspective

[1]M. Padma, [2]M. Lakshmi Neelima
[1, 2] Assistant Professor, Computer Science Department, GPREC, Kurnool
[1] padma.gprec@gmail.com, [2] neelimedum@gmail.com

Abstract: Mobile Cloud Computing (MCC) is exploring prodigious storm in IT due to anywhere anytime data access. Mobile contrivances are enabled with affluent utilizer experience especially, Smartphones. Apple, Google, Facebook and Amazon are the top four horsemen in the mobile world. That is why the mobile cloud computing technology is growing rapidly among the users and at the same time it introduces the incipient security threats withal. In MCC, teemingness of investigations are being carried out to eradicate the issues to make IT more reliable and secure because more precious data are stored in the cloud environment. As the Internet-enabled mobile contrivances including smartphones and tablets perpetuate to grow, web-predicated malignant threats will perpetuate to increment in number to make more involute. Securing data is more critical in the Mobile Cloud Environment. In MCC, Security is the major issue. In this paper, the working concepts of MCC and its assorted security issues and solutions given by researchers are analyzed.

Keywords: Mobile Cloud Computing, Threats, Security, Architecture, cloud computing

I. INTRODUCTION

Mobile cloud computing (MCC) has been introduced to be a potential technology for mobile services. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance (e.g., battery life, storage, and bandwidth), environment (e.g., heterogeneity, scalability, and availability), and security (e.g., reliability and privacy) discussed in mobile computing. The term “mobile cloud computing” was introduced not long after the concept of “cloud computing” launched in mid-2007. It has been attracting the attentions of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, of mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost, and of researchers as a promising solution for green IT. Mobile cloud computing is gaining stream. According to the latest study from Juniper Research, the number of mobile cloud computing subscribers is expected to grow rapidly in the next five years. Cloud-based mobile market will generate annual revenue of $9.5 billion in 2014 from $400 million in 2009, at an average annual increase of 88%.Network operators, Mobile users and Cloud providers are benefitted from MCC. Organization of the paper as follows: Section I introduces the Mobile Cloud Computing. The motivation for writing this paper. Section III, explains the working architecture of MCC. Section IV describes various issues and threats in MCC. Section V deals with various existing frameworks. In Section VI conveys the possible solutions to the security issues. Section VII, Conclusion of the paper is outlined.

II. MOTIVATION

The widely use of mobile phone lead to the prosperity of mobile services. Dream of “Information at your fingertips anywhere, anytime” has become true. However, mobile devices still lack in resources compared to a conventional information processing device such as PCs and laptops. Also, the limitation of battery restricts working time. How to augment capability of mobile phone has become the important technical issue for mobile computing. The paradigm of cloud computing brings opportunities for this demand. Cloud computing provide new supplement, consumption, and delivery model for IT service. Cloud-based services are on-demand, scalable, device-independent and reliable. Thus, there comes Mobile Cloud Computing, which aims at using cloud computing techniques for storage and processing of data on mobile devices, thereby reducing their limitations.

III. WORKING OF MCC

The mobile cloud computing is a development of mobile computing and an extension to cloud computing. In mobile cloud computing, the previous mobile device-based intensive computing, data storage and mass information processing have been transferred to ’cloud’ and thus the requirements of mobile devices in computing capability and resources have been reduced, so the developing, running, deploying and using mode of mobile applications have been totally changed. On the other hand, the terminals which people used to access and acquire cloud services are suitable for mobile devices like smartphone, PDA, Tablet, and iPad but not restricted to fixed devices (such as PC),which reflects the advantages and original intention of cloud computing. Therefore, from both aspects of mobile computing and cloud computing, the mobile cloud computing is a combination of the two technologies, a development of distributed, grid and centralized algorithms, and have broad prospects for application.

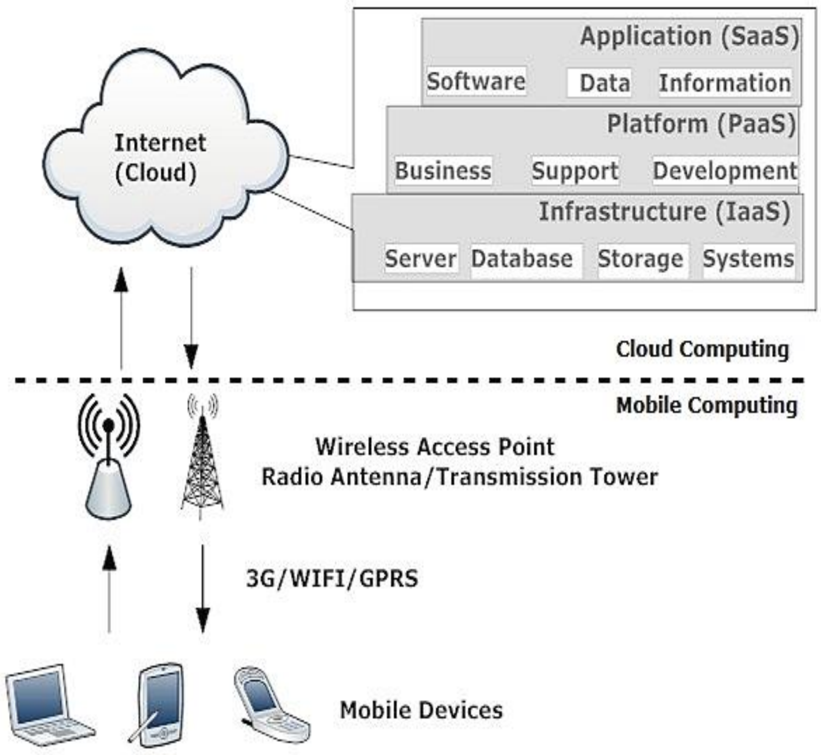


Fig 1:Architecture of Mobile Cloud Computing

As shown is the Fig1, mobile cloud computing can be divided into cloud computing and mobile computing. Those mobile devices can be laptops, PDA, smartphones, and so on. which connects with a hotspot or base station by 3G,WIFI, or GPRS. As the computing and major data processing phases have been migrated to 'cloud', the capability requirement of mobile devices is limited, some low-cost mobile devices or even non-smartphones can also achieve mobile cloud computing by using a cross-platform mid-ware. Although the client in mobile cloud computing is changed from PCs or fixed machines to mobile devices, the main concept is still cloud computing. Mobile users send service requests to the cloud through a web browser or desktop application, then the management component of cloud allocates resources to the request to establish connection, while the monitoring and calculating functions of mobile cloud computing will be implemented to ensure the QoS until the connection is completed.

A. Characteristics of MCC

The key characteristics of mobile cloud computing are Reliability, Scalability, Security, Agility, Device Independence, Low Cost, and Reduced Maintenance [3].

B. Service Models in Cloud

According to NIST, Cloud Computing services can be readily broken down into three layered service models. It is also known as the SPI model where SPI stands for Software, Platform and Infrastructure.

- Software or Application as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

1. Software or Application as a service (SaaS)

It is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. The capability provided to the End users is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web enabled e-mail). The end users does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

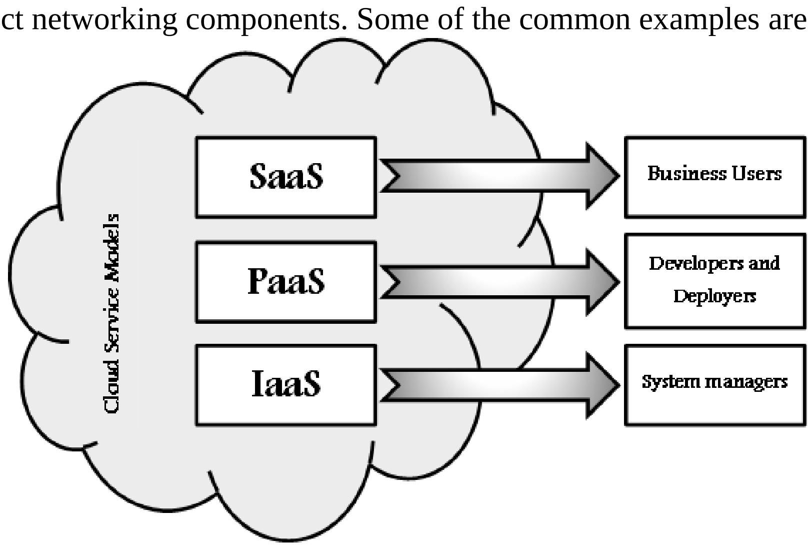
2.Platform as a Service(PaaS)

It is the delivery of computing platform and solution stack as a service. The capability provided to the end users is to deploy onto the cloud infrastructure user created or acquired applications created using programming languages and tools supported by the provider. The end user does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. PaaS providers offer a predefined combination of OS and application servers, such as WAMP platform [4] (Windows, Apache, MySql and PHP), LAMP platform (Linux, Apache, MySql and PHP), and XAMP(X-cross platform) limited to J2EE, and Ruby etc. Google App Engine, Salesforce.com, etc are some of the popular PaaS examples.

3. Infrastructure as a Service(IaaS)

It is the delivery of computer infrastructure (typically a platform virtualization environment) as a service.

The capability provided to the end users is to provision processing, storage, networks, and other fundamental computing resources where the end user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control the underlying cloud infrastructure but it has control over operating systems, storage, deployed applications, and possibly limited control of select networking components. Some of the common examples are Amazon,GoGrid,3tera etc.



C. Cloud Application Deployment Models

There are three deployment models for Cloud computing: public, private, and hybrid [4]-[7].

1. Public Cloud

In this model, computing resources are dynamically provisioned over the Internet via Web applications or Web services from an off-site third party provider. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks.

2.Private Cloud

The physical infrastructure may be owned by and managed by the organization or the designated service provider [9] with an extension of management and security control planes controlled by the organization.

3.Community Cloud

This model of Cloud computing is used by a group of Entities and organization or individuals .This cloud used by a group of entities who have sharing interest .

4 .Hybrid Cloud

This model of Cloud computing is a composition of two or more Clouds (public or private) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

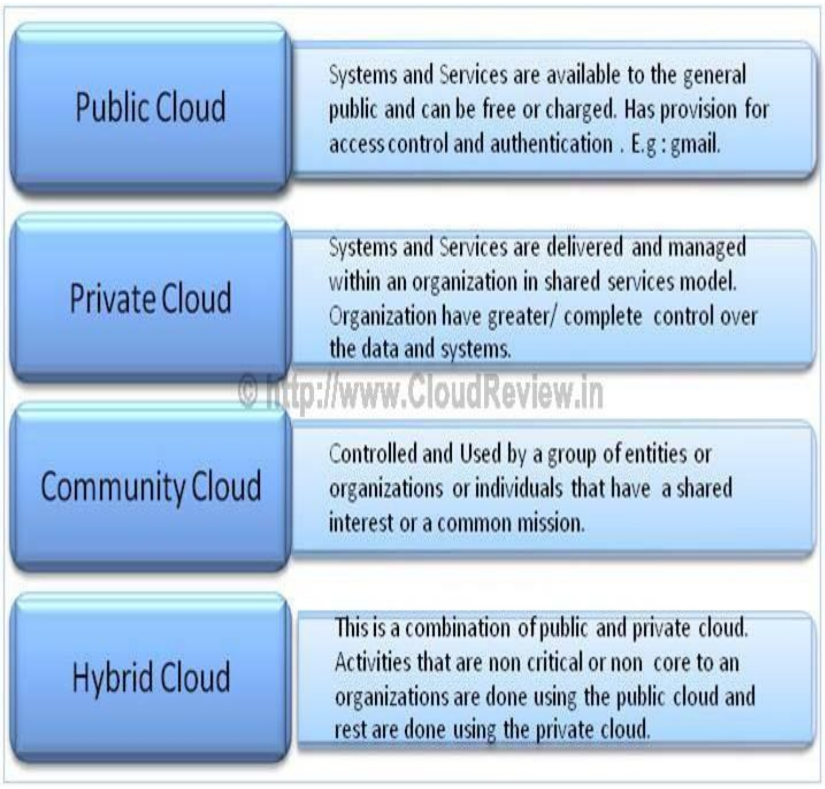

Public Cloud
Systems and Services are available to the general public and can be free or charged. Has provision for access control and authentication . E.g : gmail.
Private Cloud
Systems and Services are delivered and managed within an organization in shared services model. Organization have greater/ complete control over the data and systems.
© http://www.CloudReview.in
Community Cloud
Controlled and Used by a group of entities or organizations or individuals that have a shared interest or a common mission.
Hybrid Cloud
This is a combination of public and private cloud. Activities that are non critical or non core to an organizations are done using the public cloud and rest are done using the private cloud.

Fig 2:Cloud Deployment Models

D. Mobile Cloud Computing vs Cloud Computing

Both cloud computing and mobile computing have to do with using wireless systems to transmit data. Beyond this, these two terms are quite different. Cloud computing relates to the specific design of new technologies and services that allow data to be sent over distributed networks, through wireless connections, to a remote secure location that is usually maintained by a vendor. Cloud service providers usually serve multiple clients. They arrange access between the client's local or closed networks, and their own data storage and data backup systems. That means that the vendor can intake data that is sent to them and stores it securely, while delivering services back to a client through these carefully maintained connections.

Mobile computing relates to the emergence of new devices and interfaces. Smartphones and tablets are mobile devices that can do a lot of what traditional desktop and laptop computers do. Mobile computing functions include accessing the Internet through browsers, supporting multiple software applications with a core operating system, and sending and receiving different types of data. The mobile operating system, as an interface, supports users by providing intuitive icons, familiar search technologies and easy touch-screen commands.

While mobile computing is largely a consumer-facing service, cloud computing is something that is used by many businesses and companies. Individuals can also benefit from cloud computing, but some of the most sophisticated and advanced cloud computing services are aimed at enterprises. For example, big businesses and even smaller operations use specific cloud computing services to make different processes like supply-chain management, inventory handling, customer relationships and even production more efficient. An emerging picture of the difference between cloud computing and mobile computing involves the emergence of smart phone and tablet operating systems and, on the cloud end, new networking services that may serve these and other devices.

E. Mobile Security Service Layers

The security services in mobile ecosystem are divided into three different layers.

- Backbone layer
- Infrastructure layer
- Application and Platform layer

The backbone layer constitutes the security surveillance on cloud physical systems. This helps in monitoring the servers and machines in the cloud infrastructure. The infrastructure layer monitors the virtual machines in the cloud. Various activities such as Storage verification, VM migration, Cloud Service Monitoring, VM Isolation, Risk Evaluation and Audits are carried out in this layer to secure cloud host services. Application layer performs activities such as user management, key management, authentication, authorization; encryption and data integration.

F. Challenges and Solutions

The main objective of mobile cloud computing is to provide a convenient and rapid method for users to access and receive data from the cloud, such convenient and rapid method means accessing cloud computing resources effectively by using mobile devices. The major challenge of mobile cloud computing comes from the characteristics of mobile devices and wireless networks, as well as their own restriction and limitation, and such challenge makes application designing, programming and deploying on mobile and distributed devices more complicated than on the fixed cloud devices [13]. In mobile cloud computing environment, the limitations of mobile

devices, quality of wireless communication, types of application, and support from cloud computing to mobile are all important factors that affect assessing from cloud computing.
1) Limitations of mobile devices: While discussing mobile devices in cloud the first thing is resource-constrain. Though smartphones have been improved obviously in various aspects such as capability of CPU and memory, storage, size of screen, wireless communication, sensing technology, and operation systems, still have serious limitations such as limited computing capability and energy resource, to deploy complicated applications. By contrast with PCs and Laptops in a given condition, these smartphones like iPhone 4S, Android serials, Windows Mobile serials decrease 3 times in processing capacity, 8 times in memory, 5 to 10 times in storage capacity and 10 times in network bandwidth. Normally, smartphone needs to be charged everyday as dialing calls, sending messages, surfing the Internet, community accessing, and other internet applications. According to past development trends, the increased mobile computing ability and rapid development of screen technology will lead to more and more complicated applications deployed in smartphones.

Table 1 gives an overview of proposed challenges and some solutions about mobile cloud computing.

Challenges	Solutions
Limitations of mobile devices	Virtualization and Image, Task migration
Quality of communication	Bandwidth upgrading, Data delivery time reducing
Division of applications services	Elastic application division mechanism

If the battery technology cannot be improved in a short time, then how to effectively save battery power in smartphone is a major issue we meet today. The processing capacity, storage, battery time, and communication of those smartphones will be improved consistently with the development of mobile computing. However, such enormous variations will persist as one of major challenges in mobile cloud computing.
2) Quality of communication: In contrast with wired network uses physical connection to ensure bandwidth consistency, the data transfer rate in mobile cloud computing environment is constantly changing and the connection is discontinuous due to the existing clearance in network overlay .Furthermore, data centre in large enterprise and resource in internet service provider normally is far away to end users, especially to mobile device users. In wireless network, the network latency delay may 200 ms in 'last mile' but only 50 ms in traditional wired network. Some other issues such as dynamic changing of application throughput, mobility of users, and even weather will lead to changes in bandwidth and network overlay. Therefore, the handover delay in mobile network is higher than in wired network.
3) Division of application services: In mobile cloud computing environment, due to the issue of limited resources, some applications of compute-intensive and data-intensive cannot be deployed in mobile devices, or they may consume massive energy resources. Therefore, we have to divide the applications and use the capacity of cloud computing to achieve those purposes, which is: the core computing task is processed by cloud, and those mobile devices are responsible for some simple tasks only. In this processing, the major issues affecting performance of mobile cloud computing are: data processing in data centre and mobile device, network handover delay, and data delivery time. For a given standard, providing a quality guaranteed cloud service should consider the following facts: optimal division of application between cloud and mobile device, interaction between low-latency and code offload, high-bandwidth between cloud and mobile device for high speed data transmission, user-oriented cloud application performance, self-adaptation mechanism of mobile cloud computing, and optimal consumption and overhead of mobile devices and cloud servers.
The following strategies can be used to response to the challenges:
1. Upgrade bandwidth for wireless connection, make the web content more suitable for mobile network using regional data centres.
2. Deploy the application processing node at the 'edge' of cloud in order to reduce data delivery time.
3. Duplicate mobile devices to cloud using virtualization and image technologies, to process Data-Intensive Computing (DIC) and Energy-Intensive Computing, such as virus scanning in mobile devices.
4. Dynamically optimize application push in cloud and the division with mobile terminals.

IV. **TYPES OF SECURITY BREACHES AND ISSUES**

Though there are several advantages in mobile cloud ecosystem, there are some issues and challenges in mobile cloud computing. Some of the major issues in security are
Data Ownership, Privacy, Data Security and other Security issues [7].

A. Data Ownership

Cloud computing provides the facility to store the personal data and purchased digital media such as e-books, video and audio files remotely. For a user, there is a chance of risk to lose the access to the purchased media data. To avoid these types of risks, the user should be aware of the different rights regarding the purchased media. MCC utilizes the context information such as locations and capabilities of devices and user profiles, which can be used by the mobile cloud server to locally optimize the access management.

B. Privacy

Privacy is one of the biggest challenges in the mobile cloud computing environment. Some applications which hire cloud computing store user's data remotely. Third party companies may sell this important information to some government agencies without the permission of the user. *For example:* Mobile devices use location based services which help their friends and other persons to get the updates about the location of the user [6].

C. Data Security and other Security Issues

Mobile devices are famous for malicious code. There are many chances to lose or steal the data because mobile devices are mostly unprotected. An unauthorized person can easily access the information stored on the mobile devices. The top mobile threats that affect security are

- Data loss from lost/ stolen devices.
- Information stealing by mobile malware.
- Data leakage through poorly written third party applications.
- Vulnerabilities within devices, OS, design and third-party applications.
- Insecure network access and unreliable access points.
- Insecure or rogue marketplaces.
- Insufficient management tools, capabilities and access to APIs.

- Near Field Communication (NFC) and proximity-based hacking.

Data can be sniffed by the intruders during wireless communications. Data access can be interrupted due to multiple points. This leads to the data locked in particular services. To protect the mobile devices from data loss, thin client like anti-malware, antivirus should be installed to monitor the malicious code. Malicious code includes not only viruses but also phishing from malicious social networks and domains, botnets, spam and identity theft. Wireless protocol encryption provides secured communication where intruders cannot hack the network.

V. EXISTING SOLUTIONS PROVIDED FOR SECURITY ISSUES

Anand Surendra Shimpi [8] proposed a secure framework for processing data in mobile cloud computing. This framework stores data in a secured fashion which helps in protecting the user's privacy. In addition, he has implemented a project named "Focus Drive" which improves the driving safety of teenagers. Jibitesh Mishra [9] proposed a secure architecture for MCC to integrate mobile applications with the various cloud services. This architecture improves the storage and processing of data on mobile devices in a secured manner. It helps in maintaining the integrity and security of data. Itani et al [10] proposed a framework which was energy efficient for mobile devices to assure mobile user's integrity i.e. using *incremental cryptography and trusted computing,* the data/files of users are stored in the cloud. This framework results in saving 90% of processing energy on the mobile devices when compared to other conventional techniques with more security. Eugene E. Marinelli [11] developed *Hyrax*, a platform from Hadoop which supports cloud computing on Smartphones. It allows user's applications to utilize data and computing process on networks on Smartphones. It offers a sane performance in data sharing and tolerates node departure. Eugene also implemented a distributed media search and data sharing approach. Jon Oberheide [12] proposed an architecture which contains three components:

1) *Host Agent*: It is a lightweight process that runs on each device and inspects the activities of the files on the system. It stores the unique identifier (such as hash) in the cache for files received. If a new file does not hold file identifier, it will be sent to the Network Service.

2) *Network Service*: This service analyses the files sent by the host agent. There can be multiple instances of Network Services that are running on the cloud using virtualization technique which supports parallel detection of multiple files sent by multiple host agents.

3**) *Caching: Local private cache (LPC) and Global shared cache (GSC)*** are the two cache agents where LPC can be put into the identifier of inspected files and GSC cache resides on the Network Service which has the identifiers of all inspected files received so far. Security and privacy are always a key issue when the data are shared between mobile devices and the cloud. Even though WPA2 (Wi-Fi Alliance, 2012) provides layer-2 encryption of the data, layer-6 encryption is still a requirement because it requires some external applications like bioinformatics or computational chemistry that are executed on mobile devices and remotely on rented/ commercial cloud platforms (such as Google (2012, AWS (2012), Microsoft (2012)) which require an additional layer.To fight and protect against the security threats, the current mobile devices run the threat detection services on the mobile device itself. This service consumes both computation and power [13].

To prevent wildcat access to mobile devices and to provide protection to cloud-access, there are two measures which can be followed by enterprises that maintain a group of smartphones for employees.

1) *Cloud-access protection*: Strong authentication method ensures that only legitimate user with authorization can access cloud-based services. It can be followed by enterprises to maintain a better security level using security mechanisms like one-time passwords (OTP) and Open Authentication (OATH) in the mobile cloud environment

2) *Embedded device identity protection*: It is possible to embed a personalized configuration profile on each employee's mobile device, thereby implementing a credential or personal security token on their mobile device. For this reason, employees with reliable devices that act accordingly with corporate security policy can access corporate data and applications.

3) Security Policies: There are some other security features and policies that can be enforced to maximize the security on mobile devices, especially in a corporate context. Certainly the Mobile Cloud is an enabler for improving the smartphone and tablets security levels that are increasing more and more prevalent in business and everyday use.

VI. POSSIBLE SOLUTIONS FOR THE SECURITY ISSUES

Of all the above discussed issues, data security is the most prevalent issue during data transfer. Here are some possible solutions. The first solution is to come with a new model of security where detection services like Intrusion Detection System (IDS) and Cloud Intrusion Detection System Services (CIDSS) take place in the cloud which obviously saves the device CPU process and memory. This detection services solution have several benefits:

- Better detection of malicious code.
- Reduced consumption of resources on mobile devices.
- Reduced Software complexity of mobile devices.

Next, it is possible to achieve the security by implementing the homomorphic encryption mechanism with the combination of level-6 encryption that can be adopted when the data passes between the cloud, mobile and cloudlet without any requirement of external applications. Level-6 encryption is mainly used for secure text encode and decode which requires the use of JavaScript and browsers. To save the mobile resources, level-6 encryption should rely and be executed remotely on the cloud. This solution provides the best security and scalability feature during data sharing.

- If the data with malicious codes are downloaded by a user, the cloud account and data will be extracted and the unfair accounting will occur.
- Only verified data should be downloaded and the applications with abnormal activities should be blocked.
- Through broadcasted SSID, the information can be leaked and unauthorized user can gain access.
- Disable the SSID broadcast and utilize an enhanced key authentication algorithm.

Here are some steps given for winning the battle of breaches:

1. Prioritize the objectives and set the risk tolerance.

Protecting data assets in the workplaces has been a challenge to the security professionals for decades. The truth is that there is no such thing as 100-percent secure. Hard decisions should be made at different levels of protection needed for different parts of the business.

2. Protect the data with proactive security plan.

Security planning is not an easy task for an organization. This includes understanding the threat landscape (i.e. hacking cybercrime attacks, media & social scams, etc.) and working to protect the organization against these threats, require both policy and technology.

3. Prepare the response to the inevitable sophisticated attacks.

With the evolution of advanced continual threats, hackers aim on finding vulnerability. It is certain that eventually the organization will move towards data breach. Since the malware attacks are on the increase in today's technology, the unified and tested response plan is under critical state for the right resources and skills.

4. Promote the culture of security awareness.

It is important to note that the careless mistakes of one employee will affect the master plan of chief security officer. That's why every employee must work in a group with security professionals to ensure the safety of enterprise data. Security must be built on the culture of the organization.

VII. CONCLUSION

This paper investigates the concepts of Mobile Cloud Computing (MCC), challenging security issues and breaches, assorted subsisting security frameworks and conclusively some solutions that increase the security in the Mobile Cloud Environment. Most of the frameworks overlooked the security of utilizer data privacy, data storage and energy preserving data sharing. Data privacy and mobile application that utilizes cloud are the most challenging factor. To procure more security in mobile cloud environment, threats need to be addressed and studied accordingly. To address all these security issues, the data security plan needs to be developed which reduces the security risks and additionally to cut costs and elaboration to adopt the cloud computing in mobile environment. It is essential to keep in mind that the designing of the future framework solutions should be more cost effectual and should provide more predominant security and performance.

References

[1] Han Qi, and Abdullah Gani,*"Research on Mobile Cloud Computing: Review,Trend and Perspectives*," available at IEEE Conference Publications 2012.

[2] A. Cecil Donald, S. Arul Oli, L. Arockiam "*Mobile Cloud Security Issues and Challenges: A Perspective*,"IJEIT, ISSN: 2277-3754, Volume 3, Issue 1, July 2013.

[3] Schneider, "*Essential characteristics of Mobile Cloud Computing*", Marquette University, United States, 2012.

[4] R.J. Bayardo, and R. Srikant (2003) *Technological Solutions for Protecting Privacy*. IEEE Computer, 36(9), p. 115-118.

[5] E. Bertino (2009) *Privacy-preserving Digital Identity Management for Cloud Computing*. IEEE Data Engineering Bulletin, 32, p. 21-27.

[6] J.Brodkin (2008) *Seven Cloud-Computing Security Risks. InfoWorld. seven-cloud-computing-security-risks*, p.853.

[7] R. Buyya, C.S. Yeol, and S. Venugopal (2008) *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities*. In Proc. of 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08), p.5-13.

[8] Anand Surendra Shimpi and R. Chander,"*Secure Framework in Data Processing for Mobile Cloud Computing",* International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012

[9]https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[10] Itani et al, "*Towards secure mobile cloud: A survey", Proceedings of Analyses paper*, 2012

[11] Eugene E. Marinelli, "*Hyrax: Cloud Computing on Mobile Devices*", Dissertation of Thesis, Carnegie Mellon University, Pittsburgh, 2009

[12] Jon Oberheide and Evan Cooke, "*Virtualized in-cloud security services for mobile devices*", Proceedings of the First Workshop on Virtualization in Mobile Computing, ACM, New York, USA, 2008, pp 31–35.

[13] S. Chetan, G. Kumar, K. Dinesh, K. Mathew, and M. Abhimanyu,"*Cloud computing for mobile world*," available at chetan. ueuo. com.

Author's Profile

1]M.Padma, Assistant Professor in CSE dept received B.Tech degree in Computer Science and Information Technology from JNTU-Hyderabad and M.E degree in Computer Science and Engineering from Sathyabhama University, chennai. She had total 10.6 years of teaching experience. Presently she is working in G.Pulla Reddy Engineering College ,Kurnool,A.P. Her areas of interest are cloud computing and wireless network . She has two Research Papers published in International journals to her credit.padma.gprec@gmail.com

2]Presently **Ms M.Lakshmi Neelima** is working as an Asst.Prof in CSE.Dept, GPREC, Kurnool. She has done M.Tech(CSE) from JNT University, Anantapur, 2012, AP, India. She has total teaching experience of2.5 years. She has two Research papers published in International journals to her credit. Her main research interests are Cloud Computing and Distributed Systems. neelimedum@gmail.com