ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Mobile Cloud Security Issues and Challenges: A Perspective

A. Cecil Donald, S. Arul Oli, L. Arockiam
Research Scholar, Research Scholar, Associate Professor
Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India

Abstract*—Mobile Cloud Computing (MCC) is exploring vast in IT due to anywhere anytime data access. Mobile devices are enabled with rich user 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 new security threats also. In MCC, a lot 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 devices including smartphones and tablets continue to grow, web-based malicious threats will continue to increase in number to make more complex. 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 various security issues and solutions given by researchers are analyzed.

***Keywords*— Data Security Plan, Mobile Cloud Computing (MCC), Security.**

I. INTRODUCTION

The hottest wave in the IT world has now been the potential growth of mobile cloud computing. Securing data in Mobile Cloud have become more important in the recent days because of increasing usage of mobile devices with internet. Nowadays, the Smartphones are in the top of the invention list as they are built on a mobile OS, which is capable for advanced computing and faster in connectivity than ordinary mobile phones. Mobile cloud has the ability to change the life of both enterprise and users today. Nowadays, the applications targeted on mobile devices are now becoming more secure and complex for cloud users and enterprises. The global revenue of mobile networks has reached $1,200 billion in the year 2012. The size of the mobile cloud market in consumer and enterprise is poised to reach over $45 billion by 2016 [1]. Mobile cloud computing is simply defined as combining the cloud computing services into the mobile ecosystem that brings the wireless network and cloud computing, which provides outstanding services to the users. Mobile devices access centralized applications over the wireless connection based on a web browser or a thin native client. Researchers have outlined that "mobile cloud computing does not need any powerful mobile configuration since the entire complex computing are processed in the cloud itself" [2]. Before the emergence of Smartphone, Blackberry was the only accepted corporate Smartphone. Since technology is changing fast as iPhones, Android and doubtlessly Windows Phones are being used in many organizations. Organization of this paper is as follows: Section 1 introduces the MCC. The motivation for writing this paper is stated in section 2. Section 3 explains the working architecture of the MCC. Section 4 describes the various issues and threats in MCC. Section 5 deals with various existing frameworks. Section 6 conveys the possible solutions to the security issues and finally section 7 concludes the paper.

II. MOTIVATION

Mobile devices have become so integrated in the cloud environments that people are really talking about helping business people to get their work done easily. It is the fact that the Mobile Cloud Services are taken up by customers rather than enterprises rushing to use them up for their own needs. Mobile Cloud Computing can be considered by its unique advantages found in mobile computing. At present, there is a wide range of mobile cloud applications available. These applications fall into different areas such as image processing, natural language processing, shared GPS, shared Internet access, sensor data applications, querying, crowd computing and multimedia search [4]. Even though there are plenty of benefits, there are some issues to be addressed and solved. Figure 1 shows data protection risks to regulate data. Network connection dependency, data sharing and integrating applications and security are some of the challenges in MCC environment. Another key challenge for Mobile Cloud Computing is intermittency and network availability.

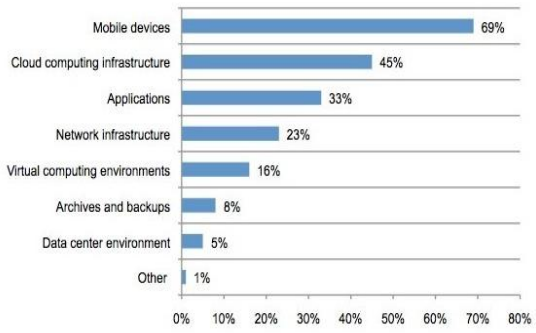

Fig 1: Data Protection Risks [5]

III. WORKING OF MCC

The architecture of mobile cloud computing is shown in the Figure 1. Here the Mobile devices connect to the mobile wireless network base stations. Some base stations are Satellite and Base Transceiver Station (BTE). They act as the interface which establishes the network connection

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

between the mobile devices and the internet. User requests are sent through the wireless network to access the cloud server by Authentication, Authorization and Accounting (AAA) mechanism. After the delivery of user requests to the cloud, the cloud controllers process those requests to provide users with the corresponding cloud services.

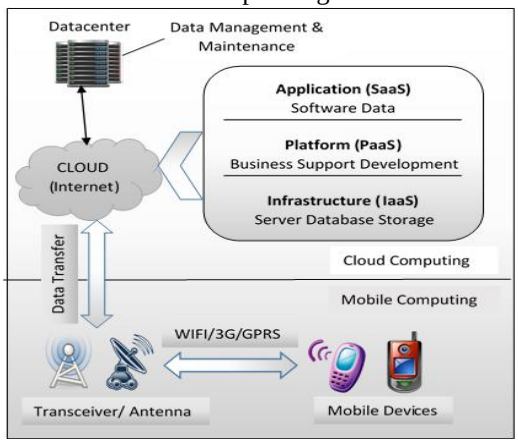

Fig 2: Simple MCC Architecture

These cloud services are developed with the concepts of Virtualization, Service Oriented Architecture (SOA) and Utility Computing [6]. There is a controller called cloud controller which helps to build, monitor and manage the wireless network. It allows user to broadcast two unique networks (one is "private" and another is "public"). A hypervisor is a program which allows the multiple OS to share a single server/machine. It is also called as Virtual Machine Manager (VMM). Application usage and maintenance are the advantages of the hypervisor.

A. Characteristics of MCC

The key characteristics of mobile cloud computing are Reliability, Scalability, Security, Agility, Device Independence, Reduced 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 as a Service [SaaS]
- Platform as a Service [PaaS]
- Infrastructure as a Service [IaaS]

Software as a Service (SaaS): This service is commonly used by business users. This service provides the complete applications to the user which is customizable within the limits. It is mainly used for achieving specific business task with the focus on end- user requirements.

Platform as a Service (PaaS): This service provides pre-built application components such as Application Programmable Interface (API). It is commonly used by developers and deployers for building the higher level applications. The developers create and deploy applications services for the users. It is not necessary to manage the OS and Databases manually.

Infrastructure as a service (IaaS): This service is mainly used by the system managers. The main advantage is that there is no need to purchase a server or manage physical data center equipment such as storage, networking, etc. Managers create platforms for service. Other than these service models, there are several service models such as *Business Process as a Service (BPaaS), Network as a Service (NaaS), Anything as a Service (XaaS), Disaster Recovery as a Service (DRaaS).*

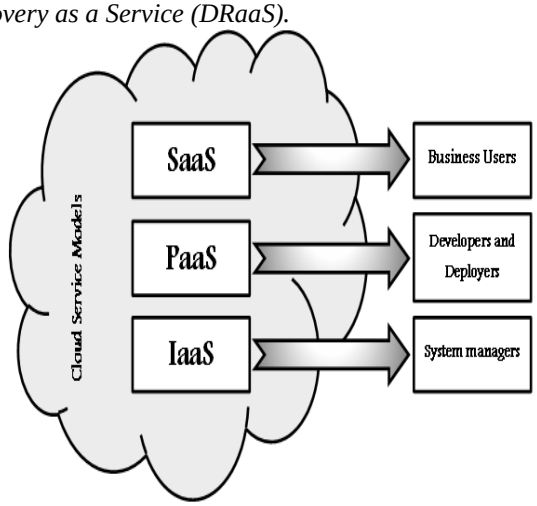

Fig 3: Service Models in Cloud Computing

C. 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. According to a recent survey, 73% of IT Executives and Chief Executive Officers are unwilling to adopt cloud services due to the associated risks with privacy and security. To attract consumers, the cloud service provider (CSP) has to target all the security issues to provide a highly secure environment.

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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

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 affects security are

1. Data loss from lost/ stolen devices.
2. Information stealing by mobile malware.
3. Data leakage through poorly written third party applications.
4. Vulnerabilities within devices, OS, design and third-party applications.
5. Insecure network access and unreliable access points.
6. Insecure or rogue marketplaces.
7. Insufficient management tools, capabilities and access to APIs.
8. 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 [17] proposed an architecture which contains three components:

a) *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.
b) *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.
c) *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 of security.

Table 1 Comparison of evaluated data security framework

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Basic Theory	Data Protection	Data Integrity	Authentication	Scalability	Data Acces
Incremental Message Authentication Code	No	Yes	No	Moderate	-
Standard Cryptographic Functions	Yes	Yes	Yes	Moderate	Automated
Merkle Hash Tree, Diffie-Hellman Key Exchange	Yes	Yes	Yes	Moderate	Automated
Exclusive-OR	Yes	Yes	Yes	Highly Scalable	Semi-Automated
Bilinear-Pairing, Access Polic Tree	Yes	No	No	Highly Scalable	Automated

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 [16]. 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.

a) *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

b) *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.

c) 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.

The table 1 shows the evaluation criteria of various security frameworks. It is evident from the table that the existing security mechanisms lack any one of the above mentioned features.

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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

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, various existing security frameworks and finally some solutions that increase the security in the Mobile Cloud Environment. Most of the frameworks overlooked the security of user data privacy, data storage and energy preserving data sharing. It is evident that user data privacy and mobile application that uses cloud are the most challenging factor. To attain 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 also to cut costs and complexity 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 effective and should provide better security and performance today.

REFERENCES

[1] RNewswire.org, http://www.reportlinker.com/, 2012.

[2] Preston A. Coz, "Mobile Cloud Computing: Devices, trends, issues & enabling technologies", 2012.

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

[4] Professor Kun Yang, Dr. Shumao Ou, Professor Hai Jin, Huazhong and Professor Amiya Nayak, "Mobile Cloud Computing and Networking", Proceedings of IEEE conference, 2013.

[5] M. Rajendra Prasad, Jayadev Gyani and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges, Journal of Information Engineering and Applications", Vol 2, No.7, 2012, Print ISSN 2224-5782, pp 7 - 15.

[6] Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[7] Soeung-Kon Victor Ko, Jung- Hoon Le and Sung Woo Kim, "Mobile Cloud Computing Security Considerations", April 30, 2012.

[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] Jibitesh Mishra, Sanjit Kumar Dash and Sweta Dash, "Mobile Cloud Computing: A Secure Framework of Cloud Computing for Mobile Application", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012, pp. 347- 356.

[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] Xiaojun Yu and Qiaoyan Wen, "Design of Security Solution to Mobile Cloud Storage",: Knowledge Discovery and Data Mining, AISC, Springer-Verlag Berlin Heidelberg H. Tan (Ed.), 2012, pp. 255–263.

[13] Robert Lemos, "Cloud's Future Security Depends on Mobile", Proceedings of RSA Conference, February 2012.

[14] V. L. Divya, "Mobile Applications with Cloud Computing", International Journal of Scientific and Research, Vol. 2, Issue 4, April 2012, ISSN 2250-3153.

[15] Han Qi and Abdullah Gani, "Research on Mobile Cloud Computing: Trends, Review and Perspectives", Proceedings of Analyses paper, University of Malaya, Malaysia, 2012.

[16] S. Chetan, Gautam Kumar, K. Dinesh, Mathew K. and Abhimanyu M.A., "Cloud Computing for Mobile World", Proceedings of Analyses paper, National Institute of Technology, Calicut, 2010.

[17] 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.

AUTHOR'S PROFILE

A. Cecil Donald received his Masters in Software Engineering from Anna University, Chennai, India. He has one year experience in IT industry as a Software Developer. Currently, he is a Ph.D research scholar in the department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Mobile Cloud Computing. He has atteneded several national and international conferences and workshops.

S. Arul Oli received his Masters in Computer Science from Bharathidasasn University, Tiruchirappalli, India. Currently, he is a Ph.D research scholar in the department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Cloud Computing. He has atteneded several national and international conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 24 years of experience in teaching and 17 years of experience in research. He has published more than 140 research articles in the International / National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored 3 books titled "Success through Soft Skills", "Research in a Nutshell" and "Object Oriented Programming with C#: A Programmer's Guide". His research interests are:

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Software Measurement, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded “Best Research Publications in Science” for 2010, 2011, & 2012 and ASDF Global Awards for “Best Academic Researcher” from ASDF, Pondicherry for the academic year 2012-13.