INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

CURRENT TREND IN MOBILE CLOUD COMPUTING [MCC] SECURITY & FUTURE RESEARCH CHALLENGES

G. Kishore Kumar[1], Dr. M. Gobi[2]

[1]Research Scholar, vgkishorekumar@gmail.com
[2]Assistant Professor, mgobimail@yahoo.com
[1,2]Dept. of Computer Science, Chikkanna Government Arts College, Tiruppur, India.

Abstract: - Cloud Computing is an evolving area, and a Combination of Mobile Computing and Cloud Computing is called as Mobile Cloud Computing (MCC). MCC integrates the cloud computing into the mobile environment and overcomes obstacles/hurdles 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) in mobile computing. Already there are several security issues in cloud computing as it encompasses many technologies viz. operating systems, networks, databases, etc. In addition, Mobile application integration grabs more security issues into the MCC environments. This paper enlightens the current trend in Mobile Cloud Computing Security, role of algorithms, and associated research challenges in which our research would be focusing on using Cryptography.

Keywords*:* Cloud Computing, Mobile Cloud Computing [MCC], Algorithms, issues, challenges, Cryptography, ECC, HECC

1. Introduction

1.1. Cloud Computing

Cloud Computing refers to the exercise of using a network, which comprises remote servers, hosted on the Internet to process, manage and store data, as opposed to a personal computer or a local server. It is a type of Internet-based computing, which offers shared computer handling resources and data to computers and/or other devices required on demand. It is a prototype for facilitating on-demand and global access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services).

Cloud consists of the below given essential characteristics:

- On-Demand self-service
- Pervasive network access
- Location-independent resource pooling
- Rapid elasticity
- Measured service

Below given are the Cloud delivery models:

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

[3]Many specialized variants of the above-said three base cloud delivery models have emerged in which each is comprised of a unique combination of IT resources. Below given are the few examples:

- Storage-as-a-Service
- Database-as-a-Service
- Security-as-a-Service
- Communication-as-a-Service
- Integration-as-a-Service
- Testing-as-a-Service
- Process-as-a-Service

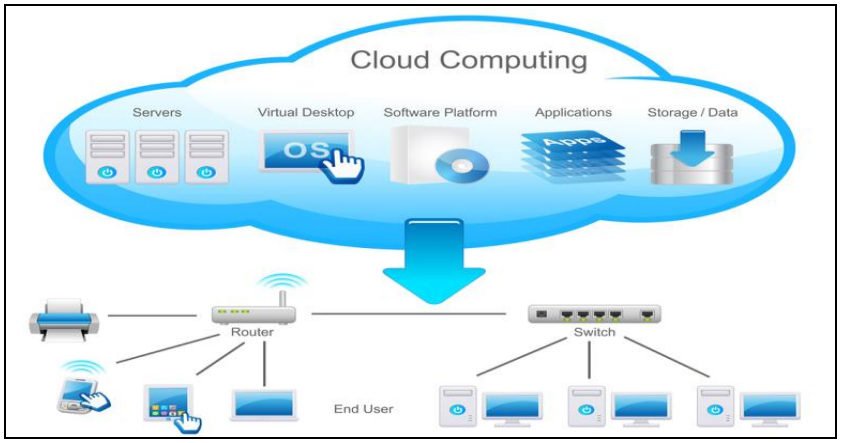

Fig. 1 Cloud Computing

1.2. Mobile Cloud Computing

Mobile Cloud Computing is a fresh concept that can be termed as the availability of Cloud Computing resources and services for mobile devices. Below given are few standard definitions of MCC:

Mobile Cloud Computing is defined in[1] as follows:
"Mobile cloud computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart-phone users but a much broader range of mobile subscribers."

Another definition given in[2]:
"Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available sensing and interactivity capabilities of mobile devices."

According to http://www.mobilecloudcomputingforum.com/

"Mobile cloud computing at its simplest refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and MC to not just smartphone users but also a much broader range of mobile subscribers."

1.3. Mobile Cloud Computing Technology Overview

Mobile Cloud Computing (MCC) consists of the below given components/modules:

- Hardware – Mobile devices
- Software – Mobile applications installed in the devices
- Communication – Mobile networks, data delivery & various protocols.

The mobile cloud is composed of five layers:

- Cloud Application Layer
- Cloud Software Environment Layer
- Cloud Software Infrastructure Layer
- Software Kernel
- Hardware and Firmware

The below given diagram describes the MCC architecture:

Fig. 2 MCC Architecture

1.4. Benefits of Mobile Cloud Computing

Mobile Cloud Computing eliminates the necessity of computing power and data storage availability in the mobile phones and incorporates into the cloud so that the mobile computing can be made available not only to the smart phone users, but also to the wide range of mobile subscribers.

The following are few benefits of MCC, which helps:

- To overcome the limitations of mobile devices in precise of the processing power and data storage.
- To extend the battery life by moving the execution of commutation-intensive application to the cloud.
- To increase the security level for mobile devices accomplished by a central monitoring and maintenance of software.
- To have a one-stop shopping option for mobile device users as MCC-Operators in parallel can act as virtual network operators through which they can provide e-payment services, software and data storage, etc. as a service.

- To have a number of new technical functionality that can be provided by mobile clouds.
- To have the business in Cloud Computing, which is currently can address the business to customers completely, & benefits the customers.
- To have the Extending battery life as the Computation-offloading techniques that have been suggested to migrate the large computations from limited resources such as mobile devices to resourceful machines like Cloud servers.
- To improve the data storage, processing power and save energy by using wireless networks into the cloud.
- To have intensive computation which can be performed on the Cloud (ex. Mobile healthcare, Mobile commerce, Mobile learning, Mobile gaming, etc.)
- To have dynamic provisioning which is a flexible way to access data/services whenever preferred.
- To improve reliability as the data storage/computation are being replicated in different cloud nodes.

2. Need of Security in Mobile Cloud Computing

2.1. Mobile Cloud Computing Security & it's Classification

It is obvious/known that there are some major issues and challenges in MCC. The MCC security issues can be classified as follows:

- **Mobile threats** - Mobile network user's security
- **Cloud threats** - Cloud security

The security related issues further can be divided into two broad categories as follows:

- **Mobile Cloud Infrastructure Issues**: These are the issues faced by organizations providing software-, platform-, or infrastructure-as-a-service via the cloud.
- **Mobile Cloud Communication Channel Issues**: These are the issues faced by customers, i.e. that the companies or organizations who host applications or store data on the cloud.

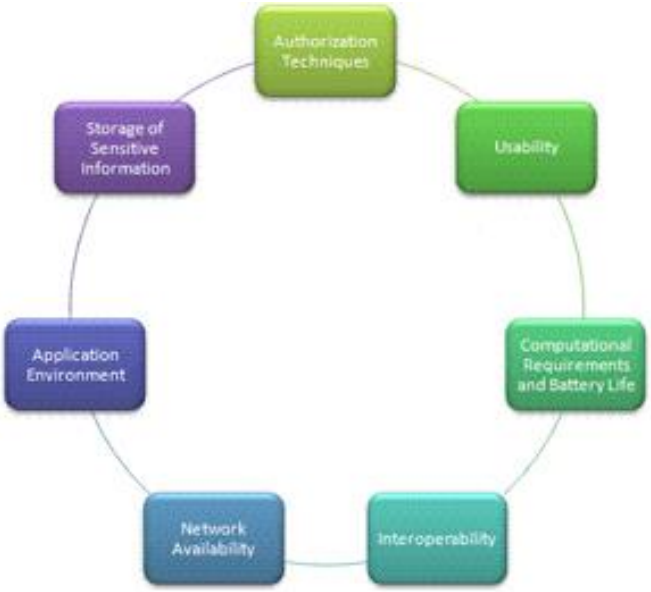

Fig. 3 MCC Security Issues/Concerns

2.2. Various Areas of MCC needs Security

With the development of MCC & its computing technologies, various security measures are required in MCC environment, which would improve the security of the environment. The proposed solutions must boost the use of various technologies/ tools to mitigate the various associated security issues. In addition, the Security recommendations must be considered in such a way that the reliability is increased. The below are the few areas identified in MCC security:

- Data delivery
- Task division
- Better service
- Standard interface
- Quality of service
- Trust, security, and privacy issues
- Network Access Management
- Pricing
- Live VM migration issues

In terms of live VM, new security threats to be undertook due to the lack of seamless isolation amid various VM instances running on the same physical server.

The utmost challenging facts in MCC is assuring user privacy and providing mobile application security, which consumes cloud resources. The service providers need to address the issues relating to

- Data integrity
- Data access
- Data security
- Network security
- Data locality
- Web application security
- Data segregation
- Authorization
- Authentication
- Data confidentiality
- Data breach issues and various other factors

For a secured MCC environment. Security threats need to be studied and accordingly to be addressed.

2.3. Role of few Encryption Algorithms existing in Security

The encryption algorithms play significant role and acting as a fundamental tool for secure network connection and data protection as well. The process in encryption algorithms is converting the data into jumbled from by using the "key" and the decryption is done using the same key by the user only. There are two types of encryption methods available:

- Symmetric – Both encryption and decryption will be done by only one key.
- Asymmetric – Two keys will be used viz. Private for decryption and Public for encryption.

2.3.1. RSA

RSA algorithm is used for public-key cryptography and it is an asymmetric algorithm being the first and still most commonly used. It involves two types of keys – public and private keys. The public key is known to all and used for encrypting messages. The encrypted message with a public key can be decrypted only by using private key.

2.3.2.MD5- (Message-Digest algorithm 5)

Cryptographic hash function algorithm which is a widely used one with a 128-bit hash value and processes a variable length message into a fixed-length output of 128 bits. In this process, the input message is split up into pieces of 512-bit blocks. Then the message is padded to get divisible by 512 as a total length. Also, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message.

2.3.3.AES- Advanced Encryption Standard (AES)

It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively by ensuring the hash code is encrypted in a very secure manner. Below given are the steps involved:

- Key Expansion
- Initial round
- Add Round Key
- Rounds
- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key
- Final Round
- Sub Bytes
- Shift Rows
- Add Round Key

2.3.4.Digital Signature

Public key algorithms used in Cryptographic digital signatures for delivering data integrity. In this authentication scheme, public key authentication is implemented in the server by signing a unique message using a private key, thus creating is called as a digital signature. Then the signature is returned to the client and later it is verified using the server's known public key.

Table 1: Abbreviations and Acronyms

CSA	Cloud Security Alliance
ECC	Elliptic curve cryptography
HECC	Hyper elliptic curve cryptography
SLA	Service Level Agreement
MCC	Mobile Cloud Computing
IBE	Identity Based Encryption
PKI	Public Key Infrastructure
MCC	Mobile Cloud Computing
LDSS	lightweight data sharing scheme
SMD	Smart Mobile Devices
DAPF	Distributed Application Processing Frameworks

3. Conclusion/Future Research Directions

In general, new/latest technology is prone to security threats. As MCC being a new & latest technology, which can bring new threats as flawless security does not exist. The need of security is very much essential on various areas in MCC. Our future research would be focusing on enhancement of existing security frameworks & multi-factor authentication technologies for highly secured data using cryptography. Our

research would be introducing/enhancing any available algorithm, which will help in accumulating more secured data storage while storing/retrieving data between mobile and cloud.

REFERENCES

[1] Mobile Cloud Computing Forum, *in http://www.mobilecloudcomputingforum.com*
[2] Chandra Shekhar Jammi,Venkata Sri Krishnakanth Pulla,Prashant Tiwari, "Mobile cloud computing is a model for transparent elastic augmentation"
[3] www.WhatIsCloud.com, Arcitura™ Education
[4] White Paper, 2010, "Mobile Cloud Computing Solution Brief" *in AEPONA*
[5] Amit K. Sharma, Priyanka Soni, 2013, " Mobile Cloud Computing (MCC): Open Research Issues", *in International Journal of Innovations in Engineering and Technology (IJIET) - Vol. 2 Issue 1*
[6] C Shravanthi, H S Guruprasad,"MOBILE CLOUD COMPUTING AS FUTURE FOR MOBILE APPLICATIONS", *in IJRET: International Journal of Research in Engineering and Technology*
[7] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, 2013,"Mobile cloud computing: A survey", *in Future Generation Computer Systems 29 84–106*
[8] D. Popa1 K. Boudaoud, M. Cremene, M. Borda, 2013,"Overview on Mobile Cloud Computing Security Issues", *in Tom 58(72), Fascicola*
[9] Abdul Nasir Khana, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, 2013,"Towards secure mobile cloud computing: A survey", *in Future Generation Computer Systems 29 1278–1299*
[10] Pragaladan. R, Leelavathi .M, 2014,"A Study of Mobile Cloud Computing And Challenges", *in International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7*
[11] Jaspreet Kaur Aulakh, Sugandha Sharma , Mayank Arora, 2014,"Mobile Cloud Computing Security Issues: Overview ", *in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5*
[12] JASLEEN," Security Issues In Mobile Cloud Computing", *in International Journal of Computer Science & Engineering Technology (IJCSET)*
[13] Pragya Gupta, Sudha Gupta, 2012," Mobile Cloud Computing: The Future of Cloud", *in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3*
[14] Nitesh Kaushik, Gaurav, Jitender Kumar, 2014," A Literature Survey on Mobile Cloud Computing: Open Issues and Future Directions", *in International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 5, Page No. 6165-6172*
[15] Nitesh Kaushik, Gaurav, Jitender Kumar, 2014," A Literature Survey on Mobile Cloud Computing: Open Issues and Future Directions", *in International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 5, Page No. 6165-6172*
[16] Mandeep Kaur Saggi, Amandeep Singh Bhatia, 2015,"A Review on Mobile Cloud Computing: Issues,Challenges and Solutions", *in International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6*
[17] S M Shamim,Angona Sarker,Ali Newaz Bahar,Md. Atiqur Rahman, 2015,"A Review on Mobile Cloud Computing", *in International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 16*
[18] Awodele Oludele,Otusile Oluwabukola, 2016,"A Survey of Mobile Cloud Computing Applications: Perspectives and Challenges", *in Proceedings of IMCIC – ICSIT*
[19] Cloud Security Alliance (CSA)
[20] US National Institute of Standards and Technology (NIST, http://csrc.nist.gov)

A Brief Author Biography

***G. Kishore Kumar* –** Research scholar in Department of Computer Science, Chikkanna Government Arts College, Tirupur, India. He has completed Master of Computer Applications [MCA] in Alagappa University, Karaikudi, India. His major field of study in Network Security and Cryptography.

***Dr M.Gobi* –** Associate Professor in Department of Computer Science in Chikkanna Government Arts College, Tirupur, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Cryptography, Java, Software Engineering and Information Systems Security.