Mobile Cloud Computing Issues and Solution Framework

Dipali S. Yadav, Prof. Kanchan Doke.

Computer Engineering Dept. Bharti Vidyapeeth College of Engineering, Navi Mumbai.
Professor, Computer Engineering Dept. Bharti Vidyapeeth College of Engineering, Navi Mumbai.

---***---

Abstract - *The computing capability of mobile systems is enhanced by Cloud computing. Mobile devices can rely on cloud computing to perform computationally intensive operations such as searching data mining etc. The use of mobile cloud computing overcomes performance related obstacles e.g. bandwidth, storage capacity and battery life, as well as environment related issues e.g. availability, scalability and heterogeneity. Cloud computing is transforming the Internet computing infrastructure. Since most of the services will be access from cloud through the Internet, Mobile Cloud Computing has been introduced.*
The security threat have become obstacle in the rapid enhancement and large use of mobile cloud computing paradigm. The security threats have become obstacles in the rapid adaptability of the mobile cloud computing paradigm. Significant efforts have been devoted in research organizations and academia to build secure mobile cloud computing environments and infrastructures. This paper reviews the concept of mobile cloud computing as well as the security issues inherent within the context of mobile application and cloud computing. The main vulnerabilities in systems with possible solutions are discuss here.

***Key Words*:Mobile Computing, Mobile Cloud Computing(MCC).**

1.INTRODUCTION

Mobile devices are now a days become essential part of human life for communication. [1] Cloud computing and mobile are remarkable techniques in last few years. When cloud computing, mobile computing and wireless networks are combined together to form a mobile cloud computing which give rich computational resources to mobile users. *Mobile cloud computing (MCC)*, 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 the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client. In mobile computing technologies, the resources in mobile cloud computing are virtualized and assigned in a group of numerous distributed computers instead of local computers or servers. Many applications based on Mobile Cloud Computing, such as Google's Gmail, Maps and Navigation systems for mobile, Voice Search, and some applications on Android platform, MobileMefrom Apple, LiveMesh from Microsoft and Motoblur from Motorola have been developed and served to users. .key technologies such as virtualization, mass distributed data storage, distributed data management, parallel programming model, wireless networks and security, etc. provided by MCC in order to deliver its implementation objectives. The aim of MCC is to enhance the opportunities derived from mobile devices by leveraging on the strengths of cloud computing, it is still a relatively new area of research, where many open problems are yet to be resolved.

2. ARCHITECTURE

Mobile Cloud Computing (MCC) is basically the interconnection of cloud computing, mobile computing and wireless networks to make powerful computational resources to mobile users, network operators, as well as cloud computing providers. This availability enables mobile users to use the cloud infrastructure to overcome the limitations of mobile technology. [3][4]

The ultimate goal of MCC is to enable execution of rich mobile applications on a platform of mobile devices, with a rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers.

More comprehensively, MCC can be defined as "a rich mobile computing technology that maintain integrity between resources of varied clouds and network technologies toward that provide, undefinable storage, and mobility to gain a multitude of mobile devices anywhere.1. The main architecture is composed from the components: mobile users, mobile operators, internet service providers (ISP), and cloud service providers, respectively. The architecture is shown in Figure[1].

Mobile users- The mobile users are the end users that deploy various services through handy cell phones, tablets which are in motions.

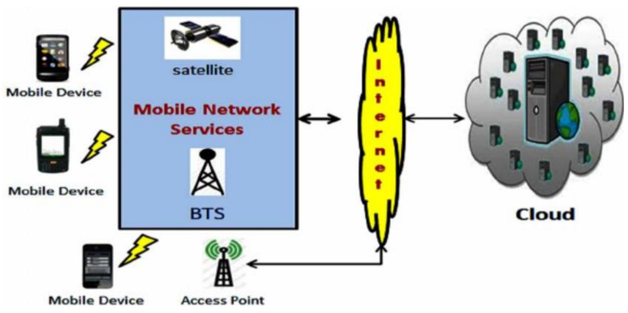

Fig. 1-MCC Architecture

Mobile Operator-
The mobile operator are wireless service provider which has the rights or own the rights to provide access to user to services like radio spectrum, wireless infrastructure, retail ,billings, customer care, and providing backbone services. An important characteristic of a mobile network operator is that it must own or control access to a radio spectrum license from a regulatory or government entity. A second most defining characteristic of an MNO is that an MNO must own or control the elements of the network infrastructure necessary to provide services to subscribers over the licensed spectrum.[3][4].

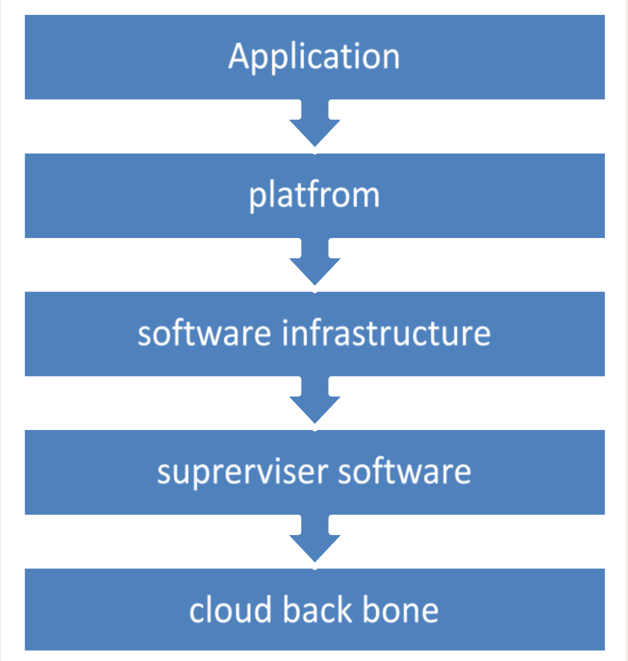

Fig. 2- Layered architecture of MCC

The layer architecture is shown in Figure[2]. The backbone layer constitutes the security surveillance on cloud physical systems. This helps in monitoring the servers and machines in the cloud infrastructure. [5] 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. To attract consumers, the cloud service provider (CSP) has to target all the security issues to provide a highly secure environment.

Security threats-

1. Confidentiality- As cloud environment involves large no. of user to provide service, increases large no. of access points of mobile users and applications. Each user's data should be secure and privately managed. Only authorized user have rights to access authorized data.

2. Privacy- Privacy is desire of a person to control user's personal information. In cloud many possibilities like insider user threats, external attacker threats, data leakage etc. can damage privacy of cloud user.

3 .Multi-tenancy- In multi-tenancy of cloud, group of user shared service provided by single software or application. In such a scenario, each mobile user's data is isolated and remains invisible to other mobile user.

4. Object reusability- A model capable of developing cloud based applications with reusability by retrieving the components from the cloud component repository by using pattern matching algorithms and various retrieval methods.

5. Data remanence- It is the residual representation of data that have been in some way nominally erased or removed. Data confidentiality could be breached unintentionally, due to data remanence.

6. Software Confidentiality- It is refers to trusting that specific application or processes will maintain and handle the user's personal data in secure manner.

7. Integrity- Integrity in cloud refers to protected from unauthorized deletion, modification, theft.
Data integrity in simple terms is the maintenance of intactness of any data during transactions like transfer, retrieval or storage.Deletion, modification can be intentionally or unintentionally.

8. Authorization- It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

9. Availability- Availability is major factor which provide access to services, data and tools anywhere, anytime. It has long been the case that to build systems with this kind of reliability and availability means large costs for companies.

3. SOLUTION FRAMEWORK

A. Encryption and Steganography-

To increase the battery life and to save energy in prolonged operation time of mobile devices computational offloading is done. In computational offloading, certain computing tasks are transferred from mobile device to external platform or from external platform to mobile devices, external platform can be cloud, grid, cluster etc. Offloading data to the cloud has implications of privacy and security, which can be handled using encryption and/or steganography. [7][8]

The data can be encrypted before uploading to the cloud. The data can be stored on a cloud in two ways. In one scenario the data remain in encrypted format, so that unauthorized access of data can be prevented even if storage is breached. In the other scenario to perform operation on data, [9] the cloud vendor will decrypt the data using the decryption key provided by the mobile user. Steganography is to hide data into another data before sending them to cloud so that unauthorized access of data can be prevented.

B. Trusted Third Party

In such a scenario, the use of a trusted third-party (TTP) preserve the confidentiality, integrity and Authenticity in performing the required auditing tasks as well as it serves a bridge between the cloud and the mobile client. This is an individual or organization, which has proficiency and skills to evaluate and expose the threat of cloud storage services rather than cloud users upon request. This is considered a trusted entity.[6]
Trusted third party is considered as a cost effective approach in which mobile client outsource the encryption key management to a trusted TPA. The TPA, on the other hand, is responsible for both managing the encryption keys and checking the integrity of outsourced data on behalf of mobile client. This would allow for effective key management and ensure data integrity, thus alleviating many of the concerns surrounding cloud data encryption. In addition, the use of TPA allows the mobile client not to have relatively high computational power on their devices which might be needed to perform data encryption, encryption keys management, message authentication of the outsourced data. Therefore, the use of TPA allows every mobile client with ordinary mobile devices to easily access the outsourced data and enjoy the real benefits of cloud computing

C. Incremental Cryptography-

The goal of incremental cryptography is to design cryptographic algorithms with the property that having applied the algorithm to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than having to recomputed it from scratch.

The mobile cloud architecture with incremental cryptography consists of three parts 1) Mobile Client 2) Trusted Third Party 3) Cloud .The Mobile Client utilizes the services provided by the cloud .The cloud will responsible for managing and allocating the resources efficiently. The tamperproof coprocessor is configured and installed by the Trustedthird party(TPP) on remote cloud. Multiple mobile client are registered with each coprocessor. The coprocessor distributes secret key(SK) with associated mobile clients and generates message authentication code on behalf of mobile client.

D. Proxy Re-encryption and identity based encryption

With the help of proxy re-encryption and identity based encryption it is possible to provide secure data services for data exchange between two end user, one the owner of the data and other is authorized receiver.
Identity Based Encryption (IBE) is Public key encryption technology that allows the public key to be calculated from an identity and the corresponding private key to be calculated from the public key. [10] A trusted server called the private key generator use a cryptographic algorithm and calculates the corresponding private key from the public key. Advantage of IBE is that receiver does not need advance preparation and simple identity can be used for public key generation.
Proxy re-encryption is a cryptographic technique used to re-encrypt the ciphertext from one's private key to another. The work of this technique is done by cloud which has the copy of message and copy of user's private key.

E. Certificate Based Authentication-

In cloud, cloud service provider and mobile user are not from same security domain. Users are identified by their characteristic or attributes therefore attributes of user need to be authorized by trusted unit because traditional identity based access control is not so effective. Certificate is issued to mobile user by certification authority which acts as trust center. [6] Attribute of user is information about user. Cloud is large scale environment. It need trusted center. Every user is allow access by access decision made by authentication center of cloud based on attributes of user. This provide flexibility and scalability that are essential to large environment such as cloud.

F. Watermarking techniques

The scalable authentication can be achieved through watermarking techniques which can be adapted to the size of scaled image from cloud. Watermarking algorithm is used for authentication between mobile user and cloud. [11] In secure sharing the data is divided into multiple pieces and it itsuploaded to different clouds, so that if single cloud is hacked no complete information can be hacked from that single cloud. The secure sharing and watermark technique can be used together to protect the data in mobile cloud.

G. Security Service Admission Model (SSAM)

The propose of a Security Service Admission Model (SSAM) based on Semi-Markov Decision Process is used to model the system reward for the cloud provider.

[12] First, system states are defined by a tuple represented by the numbers of cloud users and their associated security service categories, and current event type (i.e., arrival or departure).Then the system steady-state probability and service request blocking probability are derived by using the proposed SSAM. Numerical results show that the obtained theoretic probabilities are consistent.

6. CONCLUSION

Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model. However, resources are ubiquitous, scalable, highly virtualized. Contains all the traditional threats, as well as new ones.In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms ofLoss of control, Lack of trust, Multi-tenancy problems.

REFERENCES

[1] EweoyaIbukun and OlawandeDaramola "A Systematic Literature Review of Mobile Cloud Computing "International Journal of Multimedia and Ubiquitous Engineering , Vol.10, No.12 (2015), pp.135-152.

[2] PallaviKulkarni and RajashriKhanai,"Addresing Mobile Cloud Computing SercurityIssues:A Survey"IEEE ICCSP 2015.

[3] Trusted Platforms to secure Mobile Cloud

[4] Computihttps://en.wikipedia.org/wiki/Mobile_cloud_computingng.

[5] Cecil Donald, S. Arul Oli, L. Arockiam"Mobile Cloud Security Issues and Challenges: A Perspective "International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013 401

[6] Dimitrios zissi, Dimitrios Lekkas, "Future Generatrion Computer System" 2010.

[7] W. Itani, A Kayssi, A Chehab, Energy-efficient incremental integrity for securing storage in mobile cloud computing, in: Proc. Int. Conference on Energy Aware Computing, ICEAC ' 10, Cairo, Egypt,

Dec. 20 10.

[8] Karthik Kumar, Yung-HsiangLU,"Cloud Computing For Mobile Users:Can Offloading Computation Save Energy" IEEE J, Computer Volume:PP , Issue: 99, 18 March 20 10.

[9] S.Masiperiyannan,C.M.MehathafBegum,I.MohammedFarookAli,G.MayuriPriya,S.Sudhakar,"Security in Offloading Computations in Mobile Systems Using Cloud Computing "International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering(IJAREEIE)Vol. 3, Issue 3, March 2014.

[10] Ardi Benusi, Dolantina Hyka, "A Framework for secure data exchange in mobile cloud computing" International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 8, No. 2 (2014).

[11] Honggang Wang, Shaoen Wu, Min Chen, Huazhong ,Wei Wang,"Security Protection between Users and the Mobile Media Cloud", IEEE Communications Magazine ,Volume 52,issue 3, March 2014

[12] Hongbin Liang1,2, Dijiang Huang3, Lin X. Cai2, Xuemin (Sherman) Shen2, Daiyuan Peng1 "Resource Allocation for Security Services in Mobile Cloud Computing", IEEE INFOCOM 2011 Workshop on M2MCN-2011

[13] Ms.Gayathri M R1, Prof K. Srinivas, "A Survey on Mobile Cloud Computing Architecture, Applications andChallenges", Acharya Institute of Technology, Bangalore,2014.

[14] Shantanu Deshmukh, Prof. Rinku Shah, "Computation Offloading Frameworks in Mobile Cloud Computing : A Survey", Vidyalankar Institute of Technology,Mumbai, India, 2016.

[15] Wassim Itani Ayman Kayssi Ali Chehab,"Energy-Efficient Incremental Integrity for Securing Storage in Mobile Cloud Computing", Department of Electrical and Computer Engineering American University of Beirut

Beirut, Lebanon.