Survey on Security Issues in Mobile Cloud Computing and Preventive Measures

Rahul Neware
[1]Computer Science & Engineering Department, GHRCE Nagpur, Maharashtra, India
neware_rahul.ghrcemtechcse @raisoni.net

Abstract. Mobile Cloud Computing (MCC) is a recent technology used by various people worldwide. In 2015, more than 240 million users used mobile cloud computing which earns a profit of $5.2 billion for service providers. MCC is a combination of mobile computing and cloud computing that presents various challenges like network access, elasticity, management, availability, security, privacy etc. Here, the security issues involved in both mobile computing and cloud computing, such as data security, virtualisation security, partitioning security, mobile cloud application security and mobile device security are considered extremely important. This paper presents a detailed study of security issues in mobile cloud computing and enumerates their preventive measures.

Keywords: mobile computing; cloud computing; security; virtualisation; privacy; authentication; storage

1 Introduction

Mobile cloud computing (MCC) is a recent technology used by various people in their daily lives. It is estimated that roughly 1.5 billion smartphone users and 640 million tablet users in the world use mobile cloud computing. Mobile Cloud Computing (MCC) is the blend of cloud computing, mobile computing and wireless networks that brings rich computational resources to mobile users, network operators, as well as cloud computing providers [1]. The simplified definition of mobile cloud computing is: Distributed computing is characterised as the pattern in which resources are given to a customer on an on-demand premise, for the most part by methods through the web [1]. Mobile cloud computing uses infrastructure as a service platform of cloud for storage and processing, and cloud based applications move the computational power and information storage into the cloud [2]. MCC is a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage and mobility, and serves a multitude of mobile devices anywhere anytime through the Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle [3]. Mobile Cloud Computing is used by user using various browsers available like Chrome, Firefox. UC Browser etc [4].

Mobile Cloud Computing is one of the quickest developing segments of the cloud computing worldview. Apple and Google are the two playing the main role in

development of mobile cloud computing. By 2016, 60% of mobile development industries have used cloud services as pay-as-use that reduces resource deficiency and makes devices compatible to use cloud services in mobile devices.

2 Mobile Cloud Service Models

The concept of mobile cloud computing is categorised in different service models. Some of the prominent models of mobile cloud services are as follows:

2.1 Mobile Cloud Infrastructure as a Service (MIaaS):

This service model provides cloud environment and storage facility for the mobile user. It is like the infrastructure as service model of cloud which provides all the infrastructure for cloud. The example of MIaaS is Apple iCloud: it is Apple's own cloud-based storage system and initially it gives 5GB free storage. The other examples are Amazon Cloud, Dropbox, Google Drive, Microsoft OneDrive etc.

2.2 Mobile Network as a Service (MNaaS):

This service model offers network infrastructure to users for creating network. In other words, we can say that mobile network as a series is used to create virtual network and for connecting mobiles with servers. The example of MNaaS is OpenStsck: it is used to create virtual networks. The other examples are CoreCluster, OpenVZ, SmartOS etc.

2.3 Mobile Data as a Service(MDaaS):

This service model provides database service so that mobile cloud users can perform data management and other operations to their data. Example: CloudDB-Cloud based database made for mobile cloud computing. Oracle's mobile cloud data as a service [5].

2.4 Mobile Multimedia as a Service(MMaaS):

This service model offers a platform to access or run the multimedia in cloud environment, like playing high-memory capacity required games, playing high-definition videos etc. [6].

2.5 Mobile App as a Service(MAppaaS):

This service model provides a platform to users for executing app, and the using app also manages the apps using wireless network. Examples: Apple app store, Google play store etc.

2.6 Mobile Community as a Service(MCaaS):

This service model offers the facility to mobile users to create community network or social network and to manage all such networks and get the services needed for them [7].

3. Generalised Security Requirements

International Telecommunication Union (ITU) and US National Security Agency [8][9] have defined and laid down certain generalised security requirements of mobile cloud computing. They are as follows:

3.1 Confidentiality:

Confidentiality is a fundamental requirement because mobile users' data is processed through public network and is also stored in public servers. So there is a high chance of unauthorised access of mobile users' data, owing to which the issue of confidentiality is a big challenge to mobile cloud service providers.

3.2 Availability:

Availability means cloud service is always available for users 24/7 when they need the service. There are various attacks that affect availability, but mobile cloud computing service providers need to prevent them and always ensure the service is available for mobile users.

3.3 Authentication and Access Control:

This means identifying the valid user of the system by some login patterns or any other mechanism called authentication. Giving access to limited resources to authenticate users of the system as they want to do some task is called access control. Actions performed by users like reading, writing, updating, erasing data etc. are all controlled in access control.

3.4 Integrity:

Integrity means prevention of data loss or data modification while transmitting it through public network. Integrity deals with consistency and accuracy of user data.

3.5 Privacy:

Privacy is security of mobile user's personal data while communicating in cloud, achieved through confidentiality, integrity and authentication.

4 Challenges in Mobile Cloud Computing

Mobile cloud computing is a service of cloud computing used in smartphones or in tablets. Mobile computing and cloud computing combine together to form mobile cloud computing and give services of cloud to mobile computing users like on-demand self-service, resource pooling measured services, elasticity, broad network access [10][11]. Mobile cloud computing uses wireless communication technology to communicate between mobile and cloud [12]. Owing to the combination of mobile computing and cloud computing and use of wireless communication, we face many challenges in mobile cloud computing, such as limited resources for mobile devices, stability challenge occurring due to limitation of wireless network, cost of network access going high various times in mobile cloud computing, elasticity challenge,

security and privacy challenge, bandwidth of channel, energy efficiency, quality of service etc. [13][41].

This paper is divided into four sections. The introduction section throws light on the journey of mobile cloud computing, its various definitions, statistics, service models, security requirements of mobile cloud computing and challenges it faces. The second section discusses the security issues of mobile cloud computing. The third section presents preventive measures relating to security issues, and fourth section gives the conclusion.

Fig 1.1 Issues in Mobile cloud computing

5 Security issues in Mobile Cloud Computing

5.1 Data Security issues

In mobile cloud computing mobile user's data is available and stored in cloud and the processing of that data is also done in IaaS of cloud. Many attacks are executed on data of mobile cloud computing like, data loss, data breach, data recovery from damage, data locality, data correctness etc. In data loss, user's data is mossed while performing any computational task; for example, while transmitting data through public network. In data breaches, an authorised user's data is accessed by an unauthorised person by injecting into cloud or by getting it using any unwanted activity. In data recovery from damage issues, a user should get a valid data of his own while recovering due to damage of system or mobile device. Cloud stores the data in any data centre; so the location of that data not known to anyone. So the challenge is that the user should know where his important data is stored. Data

management is done in the service providers' premises and they need to maintain confidentiality and integrity. [14]

5.2 Virtualisation Security issues

Cloud services are provided to mobile users using virtualisation. A virtual machine of mobile is re-installed in cloud, which is called as mobile clone, and this cloud-based virtual machine does all the processing. The main advantage of using virtual machine is that it creates instances of various machines and this is achieved through hypervisor. But the challenges to virtual machine used in cloud computing are unauthorised access to the main machine through virtual machine, root attack, VM to VM attack, communication in virtualisation and confidentiality of data while being processed through hypervisor [15][16].

5.3 Offloading Security issues

Offloading means transformation of task to external platform. Mobile cloud computing requires wireless network for offloading in cloud, but precisely because of this, unauthorised access of data is possible during offloading. The main issue in offloading is availability which happens because of jamming of the mobile device while the offloading is taking place. Also, while offloading of data if it contains any malicious content, then it affects the confidentiality and privacy of the mobile user.

5.4 Mobile Cloud Applications Security Challenges

Various mobile cloud applications are affected by various malware, worms, Trojan-horse, botnet etc., which in turn affect the confidentiality and integrity aspects. These malwares are run in mobile devices and bind themselves in the application and mutate, which cause very serious issues to mobile cloud computing [17][18][19].

5.5 Mobile device Security issues

This is the most ubiquitous issue in mobile cloud computing occurring due to theft or loss of mobile device. Here, the main loss is of user's data. If the attacker gets access into any mobile device then unauthorised access to data and application occurs. The device can also be used to do some unwanted tasks like botnet: to carry out DoS or DDoS attack through mobile device [20]. A new attack related to power consumption is carried out on mobile devices when the device is connected to the wireless network; then its power consumption increases to discharge device battery fast [21]. Mostly a mobile device stores user's personal information into internal storage; but when the user uses mobile cloud computing then all data is synchronised to cloud and there the security of user's personal data becomes insecure. In mobile computing, malware and viruses constitute the very old methods of attacks but they are effective and work in mobile devices because mobile operating system is neither secure nor strong.

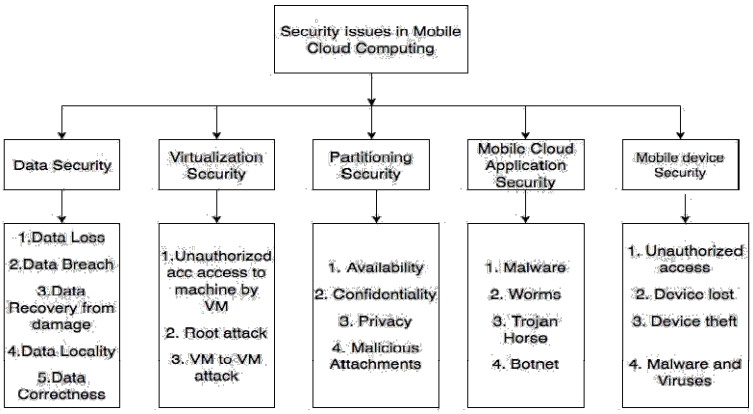

Fig 2.1 Security issues in Mobile Cloud Computing

6 Preventive measures to current security issues of MCC

6.1 Preventive methods for Data Security issues

Mollah et al. [22] has given data sharing and searching technique for mobile devices for sharing and searching data in cloud securely through public and private key encryption and digital signature. Sookhak et al. [23] introduced the remote data audition method which verifies and stores data integrity in cloud. He also developed divide and conquer table(DCT), which updates at block level. Odelu et al. [24] proposed a technique to access control and outsourcing computational process from cloud to mobile. Here, two schemes are developed: SL-CP-ABE (Secure and lightweight CP-ABE) and CP-ABE-CSCTSK (CP-ABE- Constant size type text and secret key).

Li et al. [25] developed secure accessing in cloud platform 2SBM (Inter crossed Secure Big Multimedia Model), which is based on ontology access recognition and matching algorithm. Alqahtani and Kouadri-Mostefaou [26] designed the framework based on distributed multi-cloud storage, encryption and data compression, in which data is divided in segments, then the encryption of segments takes place and then these encrypted segments are compressed.

6.2 Preventive methods for Virtualisation Security issues

Liang et al. [27] have given a technique to secure virtual machine deployment, which uses mandatory access control technique to control resources and gives powerful isolation from guest virtual machines. Hao et al. [28] invented new SMOC technique which gives permission to make copy of operating system and application of mobile to virtual machine on cloud for data security. Paladi et al. [29] developed cloud infrastructure which includes virtual machine launching and data protection protocol. Virtual machine launching is used before guest virtual machine and data protocol ensure confidentiality using cryptographic technique.

Jin et al. [30] developed H-SVM (Hardware-Assisted Secure Virtual machine) technique which secures guest virtual machine from infected hypervisor by

memory virtualisation. This technique is very useful and it is less vulnerable. Vaezpour et al. [31] developed SWAP technique for phone clone. This technique is based on two other techniques: first, securing mobile clone to lessen the threats for data leakage from virtual machine and second, migration of clone when threatened virtual machine is at high level risk.

6.3 Preventive methods for Offloading Security issues

Duan et al. [32] have given application offloading technique in which users' private information is kept within the mobile while offloading is being performed. Owing to this, unauthorised access and integrity security problems do not occur. This technique preserves privacy and also saves energy. Al-Mutawa and Mishra [33] used data partitioning technique to prevent exposure of user's personal information during offloading. This technique consists of three steps: in the first, data is divided into sensitive and non-sensitive segments, in the second, sensitive data processing takes place on device and in the third, non-sensitive data processing takes place in cloud.

Saab et al. [34] have given mobile application offloading technique that comprises profiling, decision-making and offloading engine. Profiling and decision-making are used for dynamic partitioning to reduce power consumption and decrease security issues. Offloading engine is used to offload app to cloud for processing. Khan et al. [35] proposed CMReS (Cloud Manager based Re-encryption scheme) cryptographic method which protects offloading. This method uses encryption, decryption and re-encryption of data for more security while offloading and, additionally, it is under the control of client organisation.

6.4 Preventive methods for Mobile Cloud Applications Security issues

Tang et al. [36] proposed API (Application program interface) model consisting of three factors: first, authentication with user registration with storing passwords, second, security mechanism like encryption, decryption, digital signature and third, API with backend services. Popa et al. [37] SMC (Secure Mobile Cloud) developed application to confirm the security of data communication in cloud as well as in mobile device. It measures the integrity of application when interacting with mobile device. In application integrity, first verification of application takes place, and then its signature is matched with original application signature for finding any attachment in it. In this application six different managers are used: mobile manager, mobile security manager, cloud security manager, optimisation manager, application manager and policy manager.

6.5 Preventive methods for Mobile device Security issues

Sitová et al. [38] have given a technique for authentication of user by using biometric features. In this technique, biometric includes the hand movement of user grasping the mobile which generates patterns and those patterns are used for identification of authorised and unauthorised users. In [39] is given details about Google device policy application which provides facility to the mobile user that when mobile is stolen or lost, data in device is cleaned online and mobile device toking facility is available. Imgraben et. al. [40] have given the approach of OpenFlow in which OpenFlow switch is integrated with mobile to do the job of redirection, while

communication of mobile and all cloud data is passed through OpenFlow, so that the data is secure while being transmitted.

7 CONCLUSION

In first section of this paper mobile cloud computing is explained in detail, which includes definition, history and security introduction about MMC. Various security issues are available for mobile cloud computing. However, the issues discussed in this paper are basic and very important. The prevention measures enumerated are very recent solutions to security issues of mobile cloud computing.

References

1. http://www.cse.wustl.edu/~jain/cse574-10/ftp/cloud/index.html, https://en.wikipedia.org/wiki/Mobile_cloud_computing
2. A Report of Worldwide Smartphone Markets: 2011 to 2015, May 2011: http:// www.researchandmarkets.com/research/7a1189/worldwide_smartphone
3. Z. Sanaei, S. Abolfazli, A. Gani, and M. Shiraz, "SAMI: service-based arbitrated multi-tier infrastructure for mobile cloud computing," in Communications in China Workshops (ICCC), 2012 1st IEEE International Conference on, 2012, pp. 14-19.
4. Rahul Neware. “Computer Forensics for Private Web Browsing of UC Browser.” IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 4, 2017, pp. 56–60.
5. L. Lei, S. Sengupta, T. Pattanaik, and J. Gao, "MCloudDB: A Mobile Cloud Database Service Framework," in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2015 3rd IEEE International Conference on, 2015, pp. 6-15.
6. W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing," Signal Processing Magazine, IEEE, vol. 28, pp. 59-69, 2011.
7. D. Kovachev, D. Renzel, R. Klamma, and Y. Cao, "Mobile community cloud computing: emerges and evolves," in Mobile Data Management (MDM), 2010 Eleventh International Conference on, 2010, pp. 393-395.
8. Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications: https://www.itu.int/itudoc/itu-t/85097.pdf. online: 2016
9. US National Security Agency: Information Assurance: http://www.nsa.gov/ia/ia_at_nsa/ index.shtml.online:2016
10. M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology," in Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on, 2012, pp. 1-6.
11. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, pp. 599-616, 2009
12. N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future Generation Computer Systems, vol. 29, pp. 84-106, 2013.
13. R. Neware and A. Khan, ‘Cloud Computing Digital Forensic challenges’, in *2nd International conference on Electronics, Communication and Aerospace Technology* (ICECA 2018), Coimbatore, India, 2018.

14. Neware, R. (n.d.). Recent threats to cloud computing data and its prevention measures. International journal of engineering sciences & research technology 6(11), 234-238.
15. R. Sharma, S. Kumar, and M. C. Trivedi, "Mobile Cloud Computing: Bridging the Gap between Cloud and Mobile Devices," in Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, 2013, pp.553-555.
16. Rahul Neware, Nishi Walde. Survey on Security issues of Fog Computing. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 5, Issue 10, October 2017, 15731-15736. DOI: 10.15680/IJIRCCE.2017. 0510009.
17. V. Prokhorenko, K.-K. R. Choo, and H. Ashman, "Web application protection techniques: A taxonomy," Journal of Network and Computer Applications, vol. 60, pp. 95-112, 2016.
18. J. Peng, K.-K. R. Choo, and H. Ashman, "User profiling in intrusion detection: A review," Journal of Network and Computer Applications, vol.72, pp. 14-27, 2016.
19. D. Quick and K.-K. R. Choo, "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts," Journal ofNetwork and Computer Applications, 2016.
20. L. Liu, X. Zhang, G. Yan, and S. Chen, "Exploitation and threat analysis of open mobile devices," in Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, 2009, pp. 20-29.
21. R. Racic, D. Ma, and H. Chen, "Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery," in Securecomm and Workshops, 2006, 2006, pp. 1-10.
22. M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things," IEEE Cloud Computing, vol. 4, pp. 34-42, 2017.
23. M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," Information Sciences, vol. 380, pp. 101-116, 2017.
24. V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment," Computer Standards & Interfaces, 2016.
25. Y. Li, K. Gai, Z. Ming, H. Zhao, and M. Qiu, "Intercrossed Access Controls for Secure Financial Services on Multimedia Big Data in Cloud Systems," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 12, p. 67, 2016.
26. H. S. Alqahtani and G. Kouadri-Mostefaou, "Multi-clouds Mobile Computing for the Secure Storage of Data," in Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 495-496.
27. H. Liang, C. Han, D. Zhang, and D. Wu, "A Lightweight Security Isolation Approach for Virtual Machines Deployment," in Information Security and Cryptology, 2014, pp. 516-529.
28. Z. Hao, Y. Tang, Y. Zhang, E. Novak, N. Carter, and Q. Li, "SMOC: A secure mobile cloud computing platform," in Computer Communications (INFOCOM), 2015 IEEE Conference on, 2015, pp. 2668-2676.
29. N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, 2016.
30. S. Jin, J. Ahn, J. Seol, S. Cha, J. Huh, and S. Maeng, "H-SVM: Hardware-Assisted Secure Virtual Machines under a Vulnerable Hypervisor," Computers, IEEE Transactions on, vol. 64, pp. 2833-2846, 2015.
31. S. Y. Vaezpour, R. Zhang, K. Wu, J. Wang, and G. C. Shoja, "A New Approach to Mitigating Security Risks of Phone Clone Co-location Over Mobile Clouds," Journal of Network and Computer Applications, 2016.

32. Y. Duan, M. Zhang, H. Yin, and Y. Tang, "Privacy-preserving offloading of mobile app to the public cloud," in 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 15), 2015.
33. M. Al-Mutawa and S. Mishra, "Data partitioning: an approach to preserving data privacy in computation offload in pervasive computing systems," in Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, 2014, pp. 51-60.
34. S. A. Saab, F. Saab, A. Kayssi, A. Chehab, and I. H. Elhajj, "Partial mobile application offloading to the cloud for energy-efficiency with security measures," Sustainable Computing: Informatics and Systems, vol. 8, pp. 38-46, 2015.
35. A. N. Khan, M. M. Kiah, M. Ali, and S. Shamshirband, "A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach," Journal of Grid Computing, vol. 13, pp. 651-675, 2015.
36. S.L. Tang, L. Ouyang, and W.T. Tsai, "Multi-factor web API security for securing Mobile Cloud," in Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on, 2015, pp. 2163-2168.
37. D. Popa, M. Cremene, M. Borda, and K. Boudaoud, "A security framework for mobile cloud applications," in Roedunet International Conference (RoEduNet), 2013 11th, 2013, pp. 1-4.
38. Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, et al., "HMOG: New behavioral biometric features for continuous authentication of smartphone users," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 877-892, 2016.
39. Device Policy for Andriod: Overview for Users: http://www.google.com/support/mobile/bin/answer.py?hl=en&answer=190930. Online: 2016
40. J. Imgraben, A. Engelbrecht, and K.-K. R. Choo, "Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users," Behaviour & Information Technology, vol. 33, pp. 1347-1360, 2014.
41. Rahul Neware, “Internal intrusion Detection for Data Theft and Data Modification using Data Mining”, International Journal of Science and Research(IJSR), https://www.ijsr.net /archive/v6i8/v6i8.php, Volume 6 Issue 8, August 2017, 2176-2178, #ijsrnet.