IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

A Survey on Challenges and Its Possible Solutions in Mobile Cloud Computing

Santosh Kumar Sharma[1*], Saurabh Jha[2], Nayan Chitransh[3]

[1,2,3]Department of Computer Applications, PSIT College of Higher Education, Kanpur

[*]*Corresponding Author: santosh.sharma.ddn@gmail.com, Mob No: 08791302181*

Available online at: www.ijcseonline.org

Accepted: 10/Jul/2018, Published: 31/Jul/2018

Abstract— Mobile Cloud Computing is a technological platform through which we can share resources like platform, software application, infrastructure, business processes and so on using mobile phones. It is a platform which combines the advantages of Mobile Computing and Cloud Computing and also it suffers from the common drawbacks of Mobile Computing (such as battery utilization) and Cloud Computing (such as privacy and security). In this technology, a user needs not to worry about the high configuration of the mobile phone because all the computations are done at the cloud not on the mobile device. In this paper, we present a survey on the research which has been done on MCC including challenges and open research issues.

Keywords- Mobile Computing, Cloud Computing, Security, Offloading, Virtualization

I. INTRODUCTION

Now a day's mobile devices like smart phones, PDAs, tablets have become an important and integral part of our daily life. With the advancement of Information and Communication Technology (ICT), these devices play an important role in the field of e-commerce, business, medical, education, etc. But still some drawbacks like limited storage, limited battery life and computation power of mobile devices have become the challenges of mobile computing. For this, cloud computing is used where large scale of storage space and strong computing power are available. Cloud Computing is a combination of virtualization of large amount of resources and with distributed computing paradigm which incorporates the feature of SAAS, PAAS and IAAS. Cloud computing uses the concepts of Computation Offloading which means all the computations are done at the cloud side.

The paper is divided into seven sections. Section I contains the introduction to problems faced by mobile users where storage space, battery life and computing power is the main focus areas. Section II discusses the different cloud computing environments like SAAS, PAAS, IAAS and XAAS. Section III discusses the advantages of Mobile Clouding Computing environment.Section IV discusses the applications of Mobile Cloud Computing for the mobile users. Section V discusses the challenges in Mobile Cloud Computing like Accessing Schemes, Elasticity and Scalability, Security, User Data Privacy, Virtualisation Techniques, Security Attacks. Section VI gives a conclusion that Mobile Cloud Computing provides rich facilities and advantage to the mobile users with some future challenges.

II. BACKGROUND

The basic idea of cloud computing was first introduced by John McCarthy in 1961[1]. Then it has become so popular and broadly applied in different application and business environments. Cloud computing shares resources, software & information and infrastructure as a utility through internet. Using cloud computing, a user can complete their demands at a very low cost. The service model used by Cloud computing are software as a service (SAAS), Platform as a Service (PAAS), infrastructure as a service (IAAS) and anything as a service (XAAS) [2]. Software as a Service provides end users the access to applications such as Yahoo, Facebook, Gmail, blog, etc. Infrastructure as a service provides end users the resources such as servers, computation facilities and storage. Platform as a Service provides the services to those customers who want to develop, run and test their applications such Amazon web service. Cloud computing uses the deploy model such as public cloud, private cloud, hybrid cloud, community cloud and virtual cloud. Mobile cloud computing provides the flexibility to the mobile users that they can access the resources like huge amount of storage capacity, CPU speed, memory capacity, etc via internet regardless of heterogeneous environment on pay-per-use principal [3].

III. ADVANTAGES OF MOBILE CLOUD COMPUTING

There are several advantages of MCC over mobile computing such as [5].

1. Since all the calculations of processing and data storage happen outside the device in cloud so it automatically enhances the battery life of the mobile device. It has been observed that offloading task into cloud like large-scale matrix computation can reduce the battery power by 45%, and in the case of chess game using cloud, a 45% energy saving is possible [4]. So it can be said that offloading and task migration would be the better solution to extend the battery life of the mobile devices.
2. As we know that storage was the big issue in mobile devices as they have limited storage capacity. But MCC provides large data storage capacity, where a client can store their data safely and access them.
3. Another big problem of mobile devices is processing power which can be increased in MCC by computation offloading.
4. Reliability in MCC is very high because data is stored in multiple computers and there is no loss of data. Disaster management has become faster because of multisite availability of user data. Many of the time cloud provides the copyright to the digital content so preventing unauthorized access of the data.
5. MCC is completely an on demand service which means user needs not to install the application software to their mobile devices but can use these recourses on demand basis whenever they need.

IV. APPLICATIONS OF MOBILE CLOUD COMPUTING

In these days so many cloud computing based applications are used by mobile users like mobile commerce, mobile learning, mobile gaming, mobile health monitoring, cloud mobile media, mobile social networks and cloud assisted Internet of Things etc. These applications are developed in such a way that they are able to fulfil the users demand in a secure and effective way [6, 7, 8, 9, 10, 11, 12].

V. CHALLENGES IN MOBILE CLOUD COMPUTING

1. Mobile devices: As we know that mobile devices has limited capability and resources when it is compared to the personal computer. Its limited resource is the big challenge because if we want to run an application that require high volume of energy on mobile device then it is an effective work. This limitation is reduced up to some extent using computation offloading technique but it need more work on it [13,14]. Several works have been done to address the problems in mobile devices [15,16].
2. Accessing Schemes: The second challenge is the accessing schemes used in MCC to access the resources in mobile cloud as compared to Cloud Computing since in MCC there are heterogeneous wireless mediums where the most communication takes place. Due to this, managing the quality of wireless communication, response time and service delivery are directly affected. Access management can be enhanced by using location information in mobile devices. Cho et al. [17] combined location-based services with social networking based on social relationship and human mobility to improve the access method in mobile devices. WhereStore [18] is a store location algorithm based on the location history of a Smartphone.
3. Elasticity and Scalability: Elasticity means all kind of resources must be available and purchased without any limitation and interrupt where as scalability refers to allocate proper computing resources to each and every virtual machine across multiple data centers. Several works have been done to develop elastic and scalable applications [19,20]. [21] Proposed a secure elastic mobile application which includes authentication, secure communication and migration within mobile and cloud application components in Cloud Computing. Still some more work is required to develop an elastic applications data security.
4. Security: In MCC security of user data is major challenge since the user data is stored and processed in the clouds which are located at service provider's end. To ensure security in MCC, V. Odelu, et. al suggested an encryption method cipher-text policy attribute-based encryption (CP-ABE) which restricts unauthorized access [22]. The methods defined in [22] are referred as secure and lightweight CP-ABE and constant size and secrete keys (CP-ABE-CSCTSK). Mobile users can securely access the resources and outsource computational processing from their devices to the cloud. M.Qiu, et al presents another novel approach, dynamic secure data scheme (P2DS) to provide protection against unauthorized access in cloud [23] for the financial industry. This scheme uses three algorithm Static Decryption Attribute Algorithm, Corresponded Decryption Attribute algorithm and Proactive Determinative Encryption Algorithm. P2DS method is extended in [24] where authors used divide and conquer table method (DCT) that can efficiently dynamic data operations. This approach can be applied on large data scale data storage with minimal computation cost. Several other approaches are also defined to provide data security in cloud which is defined in [25, 26, 27, 28].
5. User's data Privacy: As we know that mobile user's data and applications are stored on heterogeneous distributed cloud servers. The cloud servers are located in different location and they are managed by service providers not by mobile users and the service providers are not responsible for any data loss. In this case, the user lost the control over data privacy and protection. Pasupuleti SK, et al proposed a solution to preserve the mobile device's outsourced data in the cloud using a probabilistic public key encryption technique and ranked keyword searching algorithm [29].

In this approach, an index is created for all file collection and then both index and file collection are stored in the cloud in an encrypted form. Later for retrieving the data files, a trapdoor of keywords is created by the authorized user and sends it the server. After receiving the trapdoor by the cloud server, it starts searching of the corresponding file over the encrypted data via trapdoor of keywords. If corresponding matched file is returned to the user in ranked sequence, then the original data file can be decrypted using decryption operation. This scheme also verifies the integrity of data. A lot of work has been done to protect the privacy of mobile user's data files [30,31,32].

6. Trust in offloading: As we know that all the computational task and processing are done at the cloud server rather than mobile device. This offloading process needs wireless network to access the offloading controls, but the point is that these offloading processes are not under the control of mobile user and so it increases the risk of unauthorized access to the offloading content. Also there is a possibility for the violation of the content integrity and confidentiality. Dhanya N.M. proposed an adaptive and secure application partitioning algorithm for offloading application in mobile cloud computing to reduce the above risk by providing secure offloading processes [33]. According to this algorithm the applications are divided into two categories as sensitive and insensitive applications. Sensitive part of the application is executed locally on mobile device whereas insensitive parts are executed remotely on the cloud server. Although both applications are interconnected. A lot of work has been done and techniques are defined to established and build the trust in the cloud in [34,35,36,37]. But still more works are required in the field of encryption, decryption, authentication and authorization techniques to protect the user data to resolve the trust issue in MCC.
7. Security on Virtualization techniques: With the help of virtualization techniques cloud services are accessed in Mobile Cloud Computing. The tasks of mobile devices are offloaded to the virtual machines for processing and these virtual machines (image) of mobile devices are installed at the cloud servers. Due to this several threats of security are created such as unauthorized access, security threats within virtual machines, security challenge within hypervisor, security threats to the confidentiality of user data, etc. [38,39]. Jiaqi Tan et al proposed a security data and execution model 'STOVE' for untrusted applications which is a framework for cloud infrastructure [35]. This model uses two parts, first, it limits and isolates the untrusted application from the system it runs on so that prevents the code from directly accessing any data. Second, all data accesses are performed on behalf of the untrusted applications so that all data access is observable. Another security framework is defined by Nicolae Paladi et al for data and operation security in IaaS [40]. This framework uses a trusted launch of VMs and domain based storage protection protocol. According to this framework a trusted virtual machine is launched before launching guest virtual machine. In this way a trust is established by remotely attesting host platform and ensures the data confidentiality in cloud storage using cryptographic techniques which are created and maintained outside of the IaaS domain.
8. Other Security Attacks: Since cloud services are distributed over multithreaded network infrastructure, therefore malware, email phishing, spam and other security breaches are the most common security threats to mobile cloud computing and user's privacy [41]. A lot of work has been done to prevent such attacks on mobile devices [42, 43].

VI. CONCLUSION

Mobile cloud computing provides a rich facilities and advantage to the mobile users. But still there are some challenges that need to be explored in deep. In this paper we have given some overview of MCC along with its advantages and applications. We have also explored some challenges and their possible solutions. However this field is a burning research area where some issues need to explored in deep like mobile devices, application partitioning and offloading techniques, data integrity, security and privacy, transformations of cloud services, QoS and pricing.

REFERENCES

[1] . J. McCarthy, "Life in the Cloud, Living with Cloud Computing", Available: http://computinginthecloud.wordpress.com/2008/09/25/utility-cloudcomputingflashback-to-1961-prof-john-mccarthy/.

[2] Jitendra verma, C.P. Katti, "Study of Cloud Computing and its Issues: A Review", Smart Computing Review, vol. 4, no. 5, October 2014.

[3] S. Deshmukh, and R. Shah, "Computation offloading frameworks in mobile cloud computing: a survey", in IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), (pp. 1-5). March 2016.

[4] E. Cuervo, A. Balasubramanian, D. K. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, MAUI: Making smartphone last longer with code offload, in *Proceedings of the Eighth International Conference on Mobile Systems, Applications, and Services*, San Francisco, CA, ACM, pp. 49–62,2010.

[5] H. Dinh, T. C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches",Wireless communications and mobile computing, 13(18), pp. 1587-1611, 2013.

[6] S. Bera, S. Misra and J. J Rodrigues",Cloud computing applications for smart grid: A survey, " IEEE Transactions on Parallel and Distributed Systems, 26(5), pp. 1477-1494, 2015.

[7] G. Gao, W. Zhang, Y. Wen, Z. Wang and W. Zhu",Towards cost-efficient video transcoding in media cloud: Insights learned from user viewing patterns",IEEE Transactions on Multimedia, 17(8), pp.1286-1296, 2015.

[8] W. Zhao, Y. Sun and L, Dai,"Improving computer basis teaching through mobile communication and cloud computing technology",in IEEE 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 1, pp. V1-452, August 2010.

[9] G. Nan,.Z. Mao, M. Yu, M. Li, H. Wang and Y.Zhang, "Stackelberg game for bandwidth allocation in cloud-based wireless live-streaming social networks",IEEE Systems Journal, 8(1), pp. 256-267. 2014.

[10]W. Cai and V. C Leung",Decomposed cloud games: Design principles and challenges",in IEEE International Conference on Multimedia and Expo Workshops (ICMEW), pp. 1-4, July 2014.

[11]K. E Psannis, S. Xinogalos and A. Sifaleras",Convergence of Internet of things and mobile cloud computing",Journal Systems Science & Control Engineering, 2(1), pp. 476-483. 2014.

[12]A. Botta, W. De Donato, V. Persico and A. Pescapé",Integration of cloud computing and internet of things: a survey ",Future Generation Computer Systems, 56, pp. 684-700, 2016.

[13]A. Ellouze, M. Gagnaire and A. Haddad, " mobile application offloading algorithm for mobile cloud computing",in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 34-40, March 2015.

[14]X. Chen, L, Jiao, W. Li, and X. Fu", Efficient multi-user computation offloading for mobile-edge cloud computing", IEEE/ACM Transactions on Networking, 24(5), pp. 2795-2808. 2016.

[15]Y. Jun, L. Shan and X. Lizhen",Research of cache mechanism in mobile data management",in IEEE Conference on Web Information Systems and Applications (WISA), pp. 159-162, November 2012.

[16]H. Mao, N. Xiao, W. Shi and Y. Lu",Wukong: A cloud-oriented file service for mobile Internet devices",Journal of Parallel and Distributed Computing, 72(2), pp. 171-184, 2012.

[17]Cho, E.,Myers, S. A., & Leskovec, J. (2011). Friendship and mobility: user movement in location-based social networks. In *ACM SIGKDD international conference on knowledge discovery and data mining*, pp. 1082–1090.

[18]Stuedi, P., Mohomed, I.,&Terry, D. (2010).Wherestore: Location-based data storage for mobile devices interacting with the cloud. In *ACM workshop on mobile cloud computing and services: Social networks and beyond*, pp. 1–8.

[19]Rai, A., Bhagwan, R., & Guha, S. Generalized resource allocation for the cloud. In *ACM symposium on cloud computing*, pp. 15:1–15:12.

[20]He, Y., Elnikety, S., Larus, J., & Yan, C. (2012). Zeta: Scheduling interactive services with partial execution. In *ACM symposium on cloud computing*, pp. 1–14.

[21]. X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham and S. Jeong, " Securing elastic applications on mobile devices for cloud computing, " in proceedings of the 2009 ACM workshop on Cloud computing security, pp. 127-134, November 2009.

[22]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, May 2016.

[23]M.Qiu, K. Gai, B.Thuraisingham, L. Tao, and H. Zhao, H", Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry", Future Generation Computer Systems, February 2016.

[24]M.Sookhak, A. Gani, M. K. Khan and R. Buyya,"Dynamic remote data auditing for securing big data storage in cloud computing",Information Sciences, 380, pp. 101-116. 2017.

[25]Y. Yu, Y. Li, M. H. Au,., W. Susilo, K. K. R. Choo and X Zhang,"Public cloud data auditing with practical key update and zero knowledge privacy, " in Australasian Conference on Information Security and Privacy, pp. 389-405, July 2016.

[26]M. Louk, and H. Lim",Homomorphic encryption in mobile multi cloud computing",in IEEE International Conference on Information Networking (ICOIN), pp. 493-497, January 2015.

[27]H. Wang, S. Wu, M. Chen and W. Wang,"Security protection between users and the mobile media cloud",IEEE Communications Magazine, 52(3), pp. 73-79, 2014.

[28]K.Zkik, G.Orhanou and S. El Hajji,"Secure scheme on mobile multi cloud computing based on homomorphic encryption",in IEEE International Conference on Engineering & MIS (ICEMIS), pp. 1-6 September 2016.

[29]S. K.Pasupuleti, S. Ramalingam and R. Buyya, "An efficient and secure privacy preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications, 64, pp. 12-22. 2016.

[30]B.Niu, Q. Li, X. Zhu, G.Cao and H. Li,"Enhancing privacy through caching in location-based services",in IEEE Conference on Computer Communications (INFOCOM), pp. 1017-1025, April 2015.

[31]M.Chen, W. Li, Z. Li, , S. Lu and D. Chen,"Preserving location privacy based on distributed cache pushing",in IEEE Wireless Communications and Networking Conference (WCNC), pp. 3456-3461, April 2014.

[32]H. Zhang, N. Yu and Y. Wen,"Mobile cloud computing based privacy protection in location-based information survey applications",Security and Communication Networks, 8(6), pp. 1006-1025, 2015.

[33]N. M. Dhanya and G. Kousalya,"Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing,"in International Symposium on Security in Computing and Communication, pp. 45-53, August 2015.

[34]W. Wang, Z. Li, R. Owens and B.Bhargava,"Secure and efficient access to outsourced data",in Proceedings of the ACM workshop on Cloud computing security, pp. 55-66, November 2009.

[35]J.Tan, R.Gandhi and P. Narasimhan",STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications",in 6th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 644-649, December 2014.

[36]Q. Xiu-feng, L.Jian-Wei and Z. Peng-Chuan,"Secure cloud computing architecture on mobile internet",in 2nd IEEE International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp. 619-622, August 2011.

[37]S. Dey, S. Sampalli and Q. Ye,"A context-adaptive security framework for mobile cloud computing", in 11th International Conference on Moile Ad-hoc and Sensor Networks (MSN), pp. 89-95, December 2015.

[38]S.Singh, P. K.Sharma and J. H. Park,"A Security Model for Protecting Virtualization in Cloud Computing",in International Conference on Computer Science and its Applications, pp. 385-388, December 2016

[39]D.Sgandurra and E. Lupu",Evolution of attacks, threat models, and solutions for virtualized systems",ACM Computing Surveys (CSUR), 48(3), pp. 46. 2016.

[40]N. Paladi, C. Gehrmann and A. Michalas, "Providing user security guarantees in public infrastructure clouds",IEEE Transactions on Cloud Computing, pp.1-1, 2016.

[41]A. Arabo and B. Pranggono,"Mobile malware and smart device security: Trends, challenges and solutions",in 19th IEEE International Conference on Control Systems and Computer Science (CSCS), pp. 526-531, May 2013.

[42]J. Walls and K. K. R Choo,"A Review of Free Cloud-Based Anti-Malware Apps for Android",in IEEE Trustcom/BigDataSE/ISPA, 1, pp. 1053-1058, August 2015.

[43]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, 33(12), pp.1347-1360, 2014.

