61st IETE Annual Convention 2018 on "Smart Engineering for Sustainable Development"
Special Issue of IJECSCSE, ISSN: 2277-9477

Privacy issue in mobile cloud computing-Review

Rahul R. Papalkar Nikhil S. Band Pravin R. Nerkar Gaurav K.Wadnere

Abstract: **Today Most of the People use smart application on their smart devices, but smart devices have limited resources and for avoid such limitation cloud computing play key role, hence integration of smart devices with cloud services is essential, Usermostly use intensive application those generate confidential data & we need to upload those data on cloud, hence privacy &security is the main issue, In this article we investigate the privacy & security of data in Mobile cloud computing,**

Keywords- **Mobile cloud computing, security, Privacy, Cloud services.**

I. INTRODUCTION

Cloud computing play key role in Mobile for extending the capability of mobile device, Cloud computing improve energy efficiency, scalability, Processing & storing capacity. Although mobile cloud computing can offer several important benefits such as extended battery life and higher storage, scalability, and reliability, several key challenges continue to be a major impediment to mobile cloud computing adoption. These challenges include security and privacy, bandwidth and data transfer, data management and synchronization, energy efficiency, and heterogeneity that need to be resolved [1]. Mobile cloud computing (MCC) is a concept that refers to the integration of cloud computing into the mobile environment [2].In this way, MCC allows for a rich user experience; since client applications run remotely in the cloud infrastructure, applications use fewer resources in the user's mobile devices Mobile cloud computing architecture is shown in figure 1.1

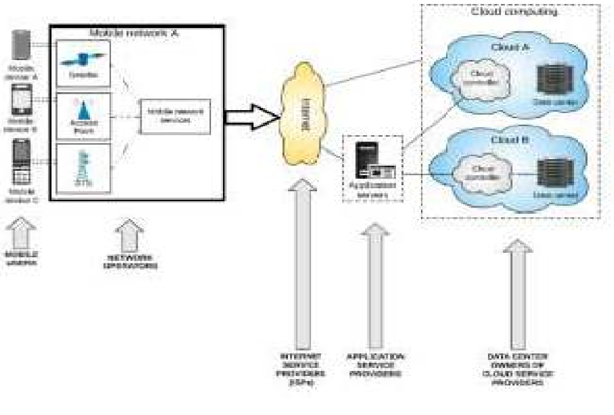


Figure 1.1 MCC Architecture

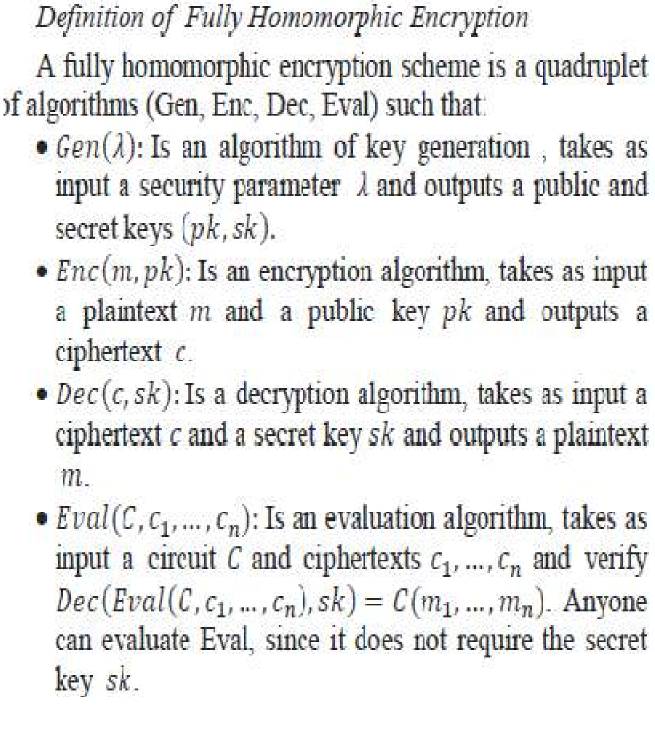
We investigate multiple research article for finding various challenges in mobile cloud computing for preserving privacy & security & other issue for research in Mobile cloud computing. To study these research architectures, we recognize several evaluation criteria. As well, we provide a holistic view of the current state of art in mobile cloud computing by presenting a quantitative analysis. The rest of paper is organized as follows in section II Literature Survey & compare abstract of different research article, In Section III. We present current state of art in mobile cloud computing specially in privacy concern. In section IV we present objectives & methodology to tackle with this issue. And finally we make some concluding remarks.

II. LITERATURE SURVEY

Mobile cloud computing has been an dynamic research area in recent years and numerous investigation have been published on this topic, conducted one of the first surveys that focus on mobile cloud computing issues. This survey presents an overview about how mobile cloud computing works, discusses some problems and possible solutions related to mobile cloud computing, and outlines the advantages of mobile cloud computing. Furthermore, the survey presents some research issues that needs to be addressed such as absence of standards, access schemes, security, and the need for elastic mobile applications [3].

Background of mobile cloud computing

Mobile computing depends on the ability to use computer resources through mobile devices. Moreover, mobile computing enables the execution of tasks that have been traditionally done by normal desktops. In general, mobile computing is supported by three basic concepts: hardware, software, and communication [7][8]. Hardware constitutes devices (e.g., tablet PCs and smart phones) that can be utilized by users. Software includes applications designed and developed to execute tasks in a mobile environment and communication which includes networks and protocols that can support the communication aspects of mobile computers such as Wireless Local Area Networks (WLAN), Long- Term Evolution 4G LTE and satellite networks. The mobile computing environment supports the following. First, there is mobility which allows mobile nodes or fixed nodes to connect with other devices' nodes in the mobile computing environment through Mobile Support Station (MSS) (e.g., servers and access points). Second, diversity of network access types refers to mobile nodes which can communicate using various types of access networks, for example Long-Term Evolution 4G LTE or Wireless Wide Area Network (WWAN) each with different communication bandwidths and overhead between the mobile nodes and the MSS. Third, frequent network disconnection means mobile nodes are not able to keep the connection consistent because of limited mobile nodes’ resources such as battery energy and communication bandwidth. Fourth, regarding the issue of poor reliability and security, mobile node signals suffer from interference and eavesdropping in mobile networks which make security increasingly more important in mobile computing. Examine security issues related to mobile cloud computing. They posit an architecture for mobile cloud computing which consists of four components including mobile client, mobile network, internet, and cloud service provider. Their survey compares: firstly, 8 existing lightweight security frameworks using a set of parameters; and secondly, 10 security applications for mobile cloud computing. The authors also discuss several research challenges regarding the following security and privacy issues in the context of mobile cloud computing: data and network security, data locality and integrity, web application security, data segregation and access, authentication and authorization, data confidentiality, and data breach.[4],Comprehensively focus on authentication methods in mobile cloud computing. Their study proposes four mobile cloud computing architecture models including i) Distant immobile cloud, ii) Proximate immobile computing, iii) Proximate mobile computing, and iv) Hybrid computing. Specifically, these authors compare authentication methods used in mobile cloud computing with the ones used in traditional cloud computing. The survey also evaluates existing authentication methods using five metrics namely; usability, efficiency, security and robustness, privacy, and adaptability to mobile cloud computing environments. Furthermore, the challenges they found requiring further analysis concerning authentication in mobile cloud computing include heterogeneous infrastructure, seamless handover, identity privacy, and resource scheduling.[4]. Privacy is key for using apps on smart devices hencewhen we upload data from mobile device to cloud it required secured interface in this paper author describe the way of accessing resources in cloud as aspect of Developers , they expect CSPs to offer a set of security features, including user authentication, single sign-on (SSO) using federation, authorization (privilege management), and SSL or TLS support, made available via the API. Currently, there is no PaaS security management standard: CSPs have unique security models, and security features will vary from provider to provider. Identity federation is an emerging industry best practice for dealing with the heterogeneous, dynamic, loosely coupled trust relationships that characterize an organization’s external and internal supply chains and collaboration model. Federation enables the interaction of systems and applications separated by an organization’s trust boundary, e.g., a sales person interacting with Salesforce.com from a corporate network. Since federation coupled with good IAM practice can enable strong authentication by way of delegation, web single sign on, and entitlement management via centralized access control services, it will play a central role in accelerating cloud computing adoption within organizations [5]. Recently, Kumar et al [6] presented a fully homomorphic encryption scheme with probabilistic encryption based on Euler’s theorem. The security of this scheme is based on factorization of big numbers. It uses a modulus composed from three big prime numbers. While it is important to base fully homomorphic encryption algorithms from number theory, this kind of conceptions simplifies the design significantly and helps in practice efficiently. We chose to follow Kumar et al’s [6] framework and construct a simpler fully homomorphic encryption scheme. Our encryption scheme will not be based on Euler’s theorem and will use a modulus of just two big prime factors.



Definition of Fully Homomorphic Encryption

A fully homomorphic encryption scheme is a quadruplet)f algorithms (Gen, Enc, Dec, Eval) such that:

- $Gen(\lambda)$: Is an algorithm of key generation , takes as input a security parameter λ and outputs a public and secret keys (pk, sk).
- $Enc(m, pk)$: Is an encryption algorithm, takes as input a plaintext m and a public key pk and outputs a ciphertext c.
- $Dec(c, sk)$: Is a decryption algorithm, takes as input a ciphertext c and a secret key sk and outputs a plaintext m.
- $Eval(C, c_1, \ldots, c_n)$: Is an evaluation algorithm, takes as input a circuit C and ciphertexts $c_1, \ldots, c_n$ and verify $Dec(Eval(C, c_1, \ldots, c_n), sk) = C(m_1, \ldots, m_n)$. Anyone can evaluate Eval, since it does not require the secret key sk.

III. SURVEY ON MCC

In this section we compare the different Research article

for analyze the privacy, security & other challenges in mobile cloud computing. We investigate following research Articles, these comparison we tabulate in to **Authors** who was elaborate, then his or her **contribution** in MCC then Author use which **Analysis Technique**. & finally put the

Challenge currently face in MCC we mention below.

SR NO	Author	Contributions	Analysis Technique	Challenges
	Chetan et al. 2010 proposed	:-overview about how MCC works :- Discuss some issues and possible solutions related to MCC. :- Present the advantages of MCC. - Provide research challenges in MCC.C6	Qualitative Synthesis	1 Absence of standards, 2.- Access Schemes, 3.- Security - 4. Need for elastic mobile Applications
	Kovachev et al. 2011 Proposed	Survey existing work in MCC.- Give a definition of MCC. – Present a comparison of 12 mobile application , models that are compatible with MCC.	Qualitative synthesis Benchmark comparison	Programming abstraction -cost model -Adaption -Cloud Integration -Trust, Security & Privacy
	Author Qi and Gani 2012 describe	Propose MCC architecture. - Present an overview of mobile computing and cloud computing. - Provide a comparison of 4 MCC architectures. - Provide research challenges in MCC.	Qualitative synthesis	Data delivery,- Task division- Better service provisioning
	Fernando et al. 2013 describe	Propose MCC architecture. - Present a taxonomy of issues in MCC. - Present an overview of 8 cost models in mobile clouds.	Qualitative synthesis	Operational - Presentation and usability - Service level - Privacy and security - Context awareness - Data management
	Rahimi et al. 2014 describe	Provide research challenges in MCC	Qualitative synthesis Benchmark comparison	Operational - Presentation and usability - Service level - Privacy and security - Context awareness - Data management
	Rahimi et al. 2014 Describe	Present a comparison of 16 different MCC systems. - Provide research challenges in MCC based on the Comparison	Qualitative synthesis Benchmark comparison	-Power and execution time efficiency - Communication bandwidth efficiency - Security and privacy
	Wang et al. 2015 Describe:	Categorize MCC into four categories. - Provide research challenges in MCC	Qualitative synthesis	- Code computation(of floading) - Task oriented mobile services - Elasticity and scalability - Security - Cloud service pricing
	Sanaei et al. 2014 Describe:	Propose MCC architecture. -Provide a taxonomy of heterogeneity roots in MCC. -Provide research challenges for MCC heterogeneity	Qualitative synthesis	Architectural - Context - awareness - Live VM migration - Mobile communication congestion - trust, security,

				and privacy
	Khan et al. 2013 describe:	Propose MCC architecture. - Present a comparison of 8 security frameworks for MCC. - Present a comparison of 10 security applications for MCC. - Provide research challenges for MCC security	Qualitative synthesis Benchmark comparison	Data and network security - Data locality and integrity - Web application security - Data segregation and access Authentication and authorization - Data Confidentiality Data breach
	Ahmed et al. 2015 describe	Propose MCC architecture. - Present a classification of seamless application execution enabling Qualitative synthesis Benchmark comparison approaches and specify their advantages and disadvantages. - Present a comparison of 14 application execution framework. - Provide research challenges for MCC application execution		- User - transparent cloud discovery - Unobtrusive application offloading - Optimal live VM migration - Seamless computational resources handoff - Agile security and privacy Mechanism
	Alizadeh et al. 2016 Describe	Propose 4 MCC architecture models. - Present a taxonomy of authentication in MCC. - Present a comparison of MCC authentication methods. - Provide research challenges for authentication in MCC	Qualitative synthesis Benchmark comparison	- Heterogeneous infrastructure - Seamless handover - Identity Privacy Resource scheduling

IV. OBJECTIVES

In this section we would like to formulate our objectives which will be try to achieve practically in our Research. For making all those problem statement we analyze above mention research paper. We mostly focus on enhance the privacy, Security, Energy efficiency & scalability of smart devices by manipulating cloud things. Following are the objectives.

1. *To Enhance the Energy Efficiency In SmartDevices.*
2. *Amplify the speed of seeking data from smart devices in MCC.*
3. *Preserve the Privacy & Security in MCC.For achieve Privacy we would like to deal with Encryption.*
4. *Modify* ***Homomorphic encryption*** *algorithm forachieve security & privacy in MCC.*

V. METHODOLOGY

This is current scenario in security & privacy domain of cloud computing, we will make it lightweight & enhance by dealing with Integer numbers, basic scenario is shown in following figure.

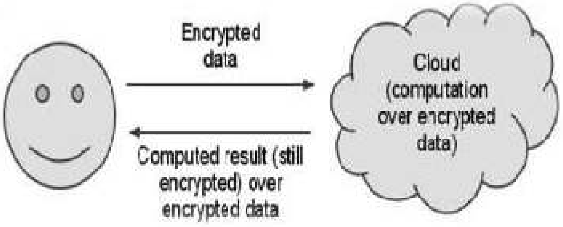

Encrypted data
Cloud (computation over encrypted data)
Computed result (still encrypted) over encrypted data

Figure 2: 2 Seeking data without decrypt.

Above model useful to enhance the access time of data these required by users, When user search data from smart devices then it connect with internet & in particular server in cloud, but data stored in the encrypted format, generally server received request from user & then decrypt it & then search in to plain text, but if we are using above mention homorphic encryption algorithm no need of decrypt still we could apply search mechanism on encrypted data, to save the time. For enhance the energy efficiency in smart devices we would like to work on offloading computation in cloud , when data load from smart devices, then we would try to upload in offloading manner for increasing the life of battery.

VI. CONCLUSION

In this paper we focus all possible challenges in privacy of MCC, we find the optimize solution on the preserving privacy in MCC by enhance the homomorphic algorithm.

REFERENCES

1. Fernando, N., Loke, S.W., Rahayu, W., 2013. Mobile cloud computing: asurvey. FutureGenerat. Comput. Syst. 29 (1), 84–106

2. A heterogeneous mobile cloud computing model for hybrid clouds SaúlAlonso-Monsalve *, Félix García-Carballeira, Alejandro Calderón ComputerScience and Engineering Department, University Carlos III of Madrid, Avda.Universidad 30, 28911 Leganés, Madrid, Spain

3. Noor, T.H., Sheng, Q.Z., Zeadally, S., Yu, J., 2013. Trust management ofservices in cloud environments: obstacles and solutions. ACM Comput. Surv.46 (1), 12.

4. Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K., 2016.Authentication inmobile cloud computing: a survey. J. Netw. Comput. Appl. 61, 59–80.

5. Preserve Identity across distributed Server using Fedrated Identity Management System Prof. Rahul R. Papalkar, Prof. Pravin R. Nerkar, Prof.N.S. Band, Prof. N.M Shivratriwar International Journal of Scientific &Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518

6. V. Kumar, R. Kumar, S. Kumar Pandey et M. Alam, "Fully Homomorphic Encryption Scheme with Probabilistic Encryption Based onEuler's Theorem and Application in Cloud Computing," chez *Big Data Analytics*, Singapore, Springer, October 2017, pp. 605-611

7. Satyanarayanan, M., 2011. Mobile computing: the next decade. ACM SIGMOB - Mob. Comput. Commun. Rev. 15 (2), 2–10.

8. Liu, L., Moulic, R., Shea, D., 2010. Cloud service portal for mobile device management. In: Proceedings of the IEEE 7th International Conference on, e-Business Engineering (ICEBE), pp. 474–478.