ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Security, Privacy and Challenges in Mobile Cloud Computing (MCC):- A Critical Study and Comparison

Nirbhay K. Chaubey[1], Darshan M. Tank[2]

Assistant Professor, Department of Computer Science, Institute of Science and Technology for Advanced Studies and Research (ISTAR), Gujarat Technological University, Gujarat, India[1]

Lecturer, Department of Information Technology, L. E. College, Gujarat Technological University, Gujarat, India[2]

ABSTRACT: Mobile Cloud Computing (MCC) is a combination of three main parts; they are mobile device, cloud computing and mobile internet. With the help of MCC, a mobile user gets a rich application delivered over the Internet and powered by cloud-backed infrastructure. The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Now a day's the major concern for mobile user is security and protection in mobile cloud computing. MCC refers to the availability of cloud computing services in a mobile environment. There are number of loopholes and challenges exist in the security policies of MCC. This paper present a review of MCC, its security & privacy issues and vulnerabilities affecting cloud computing systems, analysed and compared various possible approaches proposed by the researchers to address security and privacy issues in MCC.

KEYWORDS: cloud computing; mobile computing; mobile cloud computing; mobile cloud security; vulnerabilities; privacy

I. INTRODUCTION

Mobile devices are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of wireless communications technology as well as commerce and industry fields.

MCC is the combination of mobile computing and cloud computing, this provides full access to all technology resources through the cloud "Anytime, Anywhere, Anyhow". 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 [1].

Recently, the MCC is becoming a new hot technology. And the security solution for it has become a research focus. With the development of the mobile cloud computing, new security issues are there, which needs more security approaches.

This paper is organized as follows: - Section II introduces the concept of mobile cloud computing. Section III presents security architecture of MCC. Section IV outlines the types of security breaches and issues. Section V analysed and compared various technique proposed by the researcher to solve security issues of MCC. Finally, Section VI concludes the paper followed by future work.

II. MOBILE CLOUD COMPUTING

Cloud computing is a general term for the delivery of hosted services over the Internet. Mobile Cloud Computing refers to an infrastructure where both the data storage and the data processing occur outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones into the cloud, bringing applications and mobile computing not only to smart phone users but also to a much broader range of mobile subscribers [5].

DOI: 10.15680/IJIRCCE.2016. 0402028

Mobile devices are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications, which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security). The limited resources significantly impede the improvement of service qualities [9].

There are so many cloud storage service providers around e.g. One Drive (Microsoft Corporation), Dropbox (Dropbox Inc), Google Drive (Google Inc), Box, Amazon Cloud Drive and Apple icloud. Cloud computing applications are the cloud-based services e.g. Mobile Email, Google Maps, Google Cloud Print (Google Inc), Other Apps (Real Estate, Insurance, Surveying, Navigation app) [7].

III. SECURITY ARCHITECTURE OF MOBILE CLOUD COMPUTING (MCC)

Protecting user privacy and data/application secrecy from adversary is a key to establish and maintain consumers' trust in the mobile platform, especially in MCC. A general architecture in a broader sense depicted in Figure1.

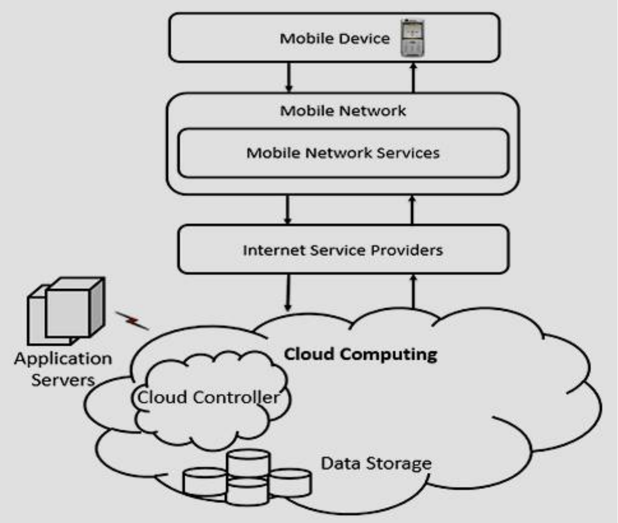

Fig 1: End to End Mobile Cloud Computing Security Architecture

The security related issues in MCC are introduced in two categories: the security for mobile users and the security for data.

A. Security for Mobile Users: Mobile devices such as cellular phone, PDA, and Smartphone are exposed to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses) and their vulnerability. In addition, with mobile phones integrated global positioning system (GPS) device, they can cause privacy issues for subscribers [6].

B. Securing Data on Clouds: Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication, and digital rights [6].

Cloud computing permits customers to utilize cloud services on the fly as pay-as-you-go manner through the Internet. There are various layered architectures available for cloud computing to provide the aforementioned services as a utility. One such cloud computing layered architecture is presented in Fig. 2 [18].

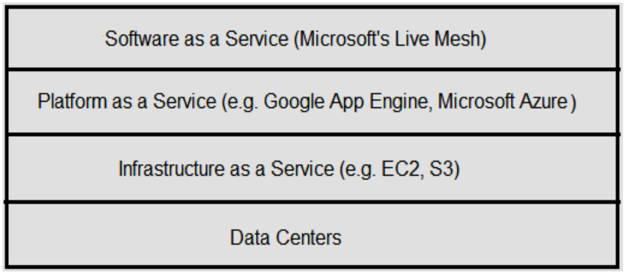
Software as a Service (Microsoft's Live Mesh)
Platform as a Service (e.g. Google App Engine, Microsoft Azure)
Infrastructure as a Service (e.g. EC2, S3)
Data Centers

Fig 2: Layered architecture of cloud computing

Generally, a cloud computing is a large-scale distributed network system implemented based on a number of servers in data centers. The cloud services are classified based on a layer concept. In the upper layers of this paradigm, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are stacked [16].

- *Data centers layer*: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high-speed networks to provide services for customers. Typically, data centers are built in less populated places, with high power supply stability and a low risk of disaster.
- *Infrastructure as a Service (IaaS)*: IaaS is built on top of the data center layer. IaaS enables the provision of storage, hardware, servers and networking components. The client typically pays on a per-use basis. Thus, clients can save cost as the payment is only based on how much resource they really use. Infrastructure can be expanded or shrunk dynamically as needed. The examples of IaaS are Amazon EC2 (Elastic Cloud Computing) and S3 (Simple Storage Service).
- *Platform as a Service (PaaS)*: PaaS offers an advanced integrated environment for building, testing and deploying custom applications. The examples of PaaS are Google App Engine, Microsoft Azure, and Amazon Map Reduce/Simple Storage Service.
- *Software as a Service (SaaS)*: SaaS supports a software distribution with specific requirements. In this layer, the users can access an application and information remotely via the Internet and pay only for that they use. Salesforce is one of the pioneers in providing this service model. Microsoft's Live Mesh also allows sharing files and folders across multiple devices simultaneously.

Although the cloud computing architecture can be divided into four layers as shown in Figure 2, it does not mean that the top layer must be built on the layer directly below it. For example, the SaaS application can be deployed directly on IaaS, instead of PaaS. Also, some services can be considered as a part of more than one layer. For example, data storage service can be viewed as either in IaaS or PaaS.

IV. TYPES OF SECURITY BREACHES AND ISSUES

A. *Data Ownership*

Cloud computing provides the facility to store the personal data and purchased digital media such as e-books, video and audio files remotely. For a user, there is a chance of risk to lose the access to the purchased media data. To avoid these types of risks, the user should be aware of the different rights regarding the purchased media. MCC utilizes the context information such as locations and capabilities of devices and user profiles, which can be used by the mobile cloud server to locally optimize the access management [13].

B. *Privacy*

Privacy is one of the biggest challenges in the mobile cloud computing environment. Some applications which hire cloud computing store user's data remotely. Third party companies may sell this important information to some government agencies without the permission of the user. For example: Mobile devices use location based services which help their friends and other persons to get the updates about the location of the user [17].

C. *Security Issues*

Mobile devices are famous for malicious code. There are many chances to lose or steal the data because mobile devices are mostly unprotected. An unauthorized person can easily access the information stored on the mobile devices [24]. The top mobile threats that affect security are mentioned as under.

1. Data loss from lost/stolen devices.
2. Information stealing by mobile malware.
3. Data leakage through poorly written third party applications.
4. Vulnerabilities within devices, Operating Systems, design and third party applications.
5. Insecure network access and unreliable access points.
6. Insecure or rogue marketplaces.
7. Insufficient management tools, capabilities and access to APIs.
8. Near Field Communication (NFC) and proximity based hacking.

Data can be sniffed by the intruders during wireless communications. Data access can be interrupted due to multiple points. This leads to the data locked in particular services. To protect the mobile devices from data loss, thin client like anti-malware, antivirus should be installed to monitor the malicious code. Malicious code includes not only viruses but also phishing from malicious social networks and domains, botnets, spam and identity theft. Wireless protocol encryption provides secured communication where intruders cannot hack the network.

The concept of data breach is that any malicious person or unauthorized person enters into a corporate network and stolen the sensitive or confidential data. Another serious threat is the potential incapacity to prevent data loss because many of the companies treat their data as a valuable asset. In our networked world, most people know that loss of data is unavoidable at one point or another. There is increasing amount of sensitive data which is relayed to cloud computing providers and this data could get lost in any number of ways, including through accidental deletion or corruption of stored data [27].

Security risk in MCC is inherited from cloud computing. Mobile Cloud Computing suffers from following risk.

- In mobile cloud computing, user does not know where his data is stored, so user has little or no control over the location of data.
- Because of physical damage of cloud server, loss of encoding key or due to malicious insider, risk of data loss may arise.
- A customer with ill intent may plant virus of phishing attack in to cloud server which may compromise data of other customers and cloud provider may not be able to track it because of privacy policy of the company.
- A gap in security of application interface of cloud services can lead to attacks like bypass attack of API attack.
- When cloud provider services a number of users, flaw in encryption algorithm can lead to unauthorized access to one’s data.
- As per regulatory compliance cloud provider has to maintain required security level
- In IaaS security risk may arise due to lack of isolation in virtualization when number of virtual machines are hosted on a single server.
- Mobile user stores and transfers critical personal and corporate information while using mobile applications like online payment, social networking etc, that can be an attacker’s new target.

V. SECURITY ISSUES OF MOBILE CLOUD NETWORK

In this section, different types of possible attacks in MCC are considered.

SQL Injection Attack: In this type of attack a malicious code is inserted into a standard SQL code. Thus the attackers get unauthorized access to a database and are able to access sensitive data [14].

Browser Security: Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user’s identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host [16].

Cross Site Scripting (XSS): It enables attackers to inject client-side script into Web pages viewed by other users. There are two methods for injecting the malevolent code into the web-page that is displayed to the user. Stored XSS and Reflected XSS. In case of Stored XSS, the malicious code is permanently stored into a resource managed by the web application. However in case of a Reflected XSS, the attack script is not permanently stored; in fact it is immediately reflected back to the user. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy [16].

Denial of Service Attacks: This attack prevents the consumer from receiving the service from the cloud [31].

Cookie Poisoning: Cookie poisoning involves changing or alerting the contents of cookie to have an illegal access to a webpage or an application [20].

Locks In: Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location [21].

Flooding Attacks: In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests. Cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfill the requests of invader making the resources inaccessible for the normal users [29].

Incomplete Data Deletion: Incomplete data deletion is treated as hazardous one in cloud computing. When data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is majorly impossible because copies of data are saved in replica [30].

Xml signature element wrapping: As clients are typically able to connect to cloud computing via a web browser or web service, the web service attacks also affect cloud computing. Although Cloud security uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the particulars in the document [30]. Comparative views of various technique, frameworks and models proposed by the researchers to provide security and privacy in MCC and their advantage and disadvantage are discussed in Table 1.

Table 1. *Comparisons analysis of various technique proposed by the researcher to solve Security and Privacy Issues in MCC*

Researchers	**Approach /Cloud Trust Level**	**Security Attribute provided**	**Trusted Third party**	**Advantages**	**Disadvantages**
J. Oberheide et al. *Virtualized in-cloud security services for mobile devices* [20]	CloudAV/ Fully trusted	Antivirus, Security as a Service	No	Reduced On Device software complexity and power consumption	Disconnected operation and privacy loss
Zhang et al. *ACM workshop on Cloud computing security* [21]	Cloudlet/ Semi-trusted	Task partitioning	No	Good tradeoffs between processing overhead and communication cost	Security of Web-let can be improved with other techniques.
Xiao and Gong et al. *International Conference on Mobile Data Management* [22]	Lightweight algorithm/ Semi trusted	Authorization of user's data in cloud	No	Automatic Dynamic updating of credential information	More processing and energy burden on mobile device
Wang and Wang et al. *11th International Conference on Mobile Data Management, MDM* [23]	Top down spatial cloaking/ Distrusted	Privacy preserving framework in location based Scheme	No	Reduced communication cost by doing spatial cloaking based on the historical data in cloud.	More energy consumption and processing burden on mobile device
Huang et al. *MobiCloud: building secure cloud framework for mobile computing and communication* [24]	MobiCloud/ distrusted	Security in Storage as a Service in MANET	Yes	Secured data while using Public Cloud	Increased cost due to two cloud providers
G. Portokalidis et al. *Annual Computer*	Threat detection in	Security as a Service	No	Reduced transmission overhead and energy	More Cloud usage cost.

Security Application Conference (ACSAC) [25]	Smartphone based on CloudAV/ Fully trusted			consumption	
R.Chow et al. *ACM Cloud Computing Security Workshop* [26]	Policy based cloud authentication platform/ Fully trusted	Authentication of user.	No	Authentication based on behavioral data of user	Privacy threat
Jia et al. *IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS* [27]	Proxy reencryption (PRE) scheme and Identity based encryption (IDE) scheme/ Semi trusted	Secure data Service	No	Reduced cost of updating of access policy and communication cost	More processing and energy burden on mobile device for encrypting the secret information
Yang et al. *Provable data possession of resource constrained mobile devices in cloud computing* [28]	extended the public provable data possession scheme/ Distrusted	ensures privacy, confidentiality and integrity of user data stored on cloud	Yes	Reduced energy and processing requirement on mobile device	Degradation of performance with the increase in no. of users in Trusted Party Agent (TPA). Cost also increases due to two cloud service providers.
Saman Zonouz et al. *Science Direct journal of Computers and security* [29]	Secloud for smartphones/ Trusted	cloud based comprehensive and lightweight security for smart phones	No	Reduced energy and processing requirement on mobile device for providing security in mobile device	Cloud assumes to be fully trusted which needs to be reconsidered .The personal data of users accessed to the cloud can affect the privacy issues
Vijay Varadharajan et al. IEEE Transactions On Network and Service Management [30]	Security as a Service Model	Virtualization technology and VMM security functionalities	No	Offers a baseline security to the provider to protect its own cloud infrastructure	Insider attack from Tenant Domain and Cloud Service Provider
Qiao Yan and F. Richard Yu et al. IEEE Communications Surveys & Tutorials [31]	Software-defined networking (SDN)	Networking-as-a-service (NaaS), control and data planes are decoupled	Yes	software-based traffic analysis, centralized control, global view of the network, dynamic updating of forwarding rules	Security of SDN itself remains to be addressed and potential DDoS vulnerabilities exist across SDN platforms

Different researchers have come up with different approaches to solve the issues of security and privacy in MCC, but none of the existing approaches offers a concrete solution against these issues. Due to resource limitation, proposed security schemes for the cloud computing environment cannot be directly applicable to the mobile device. There is a need for a lightweight secure framework that provides security with minimum communication and processing overhead.

VI. CONCLUSION AND FUTURE WORKS

Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. Security and privacy are one of the most challenging issues in MCC. The security threats have become obstacles in the rapid adaptability of the MCC paradigm.

The lack of an in-depth study of the security and privacy in MCC was detected in current available literature. Therefore, this paper has attempted to provide more insight to this field of research by studying and theoretical comparison of different approaches proposed by the researchers to provide security and privacy in MCC.

The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer. Thus there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices.

There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud. We also need to address issues pertaining to data security, network security, data integrity, authentication, authorization and access control.

To achieve a secure MCC environment, security threats need to be studied and addressed accordingly. In the future, our research work focus on to propose a security model framework to enhance security and privacy in MCC.

REFERENCES

1. Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. “A survey of Mobile Cloud Computing: Architecture, Applications, and Approaches,” Wireless Communications and Mobile Computing, 2011.
2. S.c. Hsueh, lY. Lin, M.Y. Lin, Secure cloud storage for conventional data archive of smart phones, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, TSCE ' II, Singapore, June 2011.
3. W. Jla, H. Zhu, Z. Cao, L. Wei, X. Lin, SDSM: a secure data service mechanism in mobile cloud computing, in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China, Apr. 2011.
4. Abdul Nasir Khana, M.L. Mat Kiah a, Samee U. Khanb, Saljad A Madanic, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, August 2012.
5. Dimitrios Zissis, Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems Volume 28, Issue 3, March 2012, Pages 583-592
6. Hui Suo, Zhuohua Liu, Jiafu Wan “Security and Privacy in Mobile Cloud Computing” 978-1-4673-2480-9 ©2013 IEEE
7. Ranbijay Kumar, Dr. S. Rajalakshmi “Mobile Cloud Computing Standard approach to protecting and securing of mobile cloud ecosystems” 2013 IEEE International Conference on Computer Sciences and Applications
8. Ahmad Salah Al-Ahmad, Syed Ahmad Aljunid “Mobile Cloud Computing Testing Review” 2013 IEEE International Conference on Advanced Computer Science Applications and Technologies
9. N. Fernando, S. W. Loke, and W. Rahayu, “Mobile cloud computing: A survey,” Future Generation Computer Systems, vol. 29, no. 1, pp. 84–106, January 2013.
10. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” Wireless Communications and Mobile Computing, 2013.
11. Khanai, R. ; Dept. of Electr. & Electron. Eng., Gogte Inst. of Tech., Belgaum, India; Kulkarni, G.H. ; Torse, D.A. "Neural Crypto-Coding as DES: Turbo over Land Mobile Satellite (LMS) channel" Published in Communications and Signal Processing (ICCSP), 2014 International Conference on 3-5 April 2014 ,Melmaruvathur .
12. Rajashri Khanai, G. H. Kulkarni, "Crypto-Coding as DES-Convolution for Land Mobile Satellite Channel", International Journal of Computer Applications © 2014 by IlCA Journal Volume 86 - Number 18 Year of Publication: 2014.
13. Honggang Wang, Shaoen Wu, Min Chen, Huazhong ,Wei Wang, Secunty ProtectIOn between Users and the Mobile Media Cloud" IEEE Communications Magazine ,Volume 52,issue 3, March 2014
14. Dr. Vineet Shanna, Preeti Garg “An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function” 978-1-4799-2900-9 ©2014 IEEE
15. Iehab AL Rassan, Hanan AlShaher “Securing Mobile Cloud Computing using Biometric Authentication (SMCBA) ” 2014 IEEE International Conference on Computational Science and Computational Intelligence
16. Dipayan Dev, Krishna Lal Baishnab “A Review and Research towards Mobile Cloud Computing” 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering

17. Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, “Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges,” IEEE Communications Surveys and Tutorials, vol. 16, no. 1, 2014, pp. 369-392.
18. R. Buyya, “Introduction to the IEEE Transactions on Cloud Computing,” IEEE Transactions on Cloud Computing, vol. 1, no. 1, 2014, pp. 3-9.
19. H. Hu, Y. Wen, T.S. Chua and X. Li, “Toward Scalable Systems for Big Data Analytics: A Technology Tutorial,” IEEE Access, vol. 2, 2014, pp. 652-687.
20. Oberheide, J., Veeraraghavan, K., Cooke, E. and Jahanian, F.2008,Virtualized in-cloud security services for mobile devices. In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt),31- 35.
21. Zhang, X., Schiffman, J.,. Gibbs S, Kunjithapatham, A., and Jeong S.2009,Securing elastic applications on mobile devices for cloud computing.In Proceeding ACM workshop on Cloud computing security, CCSW ’09, Chicago, IL, USA.
22. Xiao, S. and Gong ,W.,2010. Mobility can help: protect user identity with dynamic credential.In Proceeding 11th International Conference on Mobile Data Management, MDM ’10, Missouri, USA, May 2010.
23. Wang, S .and S. Wang X.,” In-device spatial cloaking for mobile user privacy assisted by the cloud”, in Proceeding 11th Interantional Conference on Mobile Data Management,MDM ’10, Missouri, USA, May 2010
24. Huang, X. Zhang, M. Kang and J. Luo,” MobiCloud: building secure cloud framework for mobile computing and communication,” in Proceeding 5th IEEE International Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China, June 2010.
25. G. Portokalidis,P. Homburg,K. Anagnostakis and H. Bos,”Paranoid Android: versatile protection for smartphones,” in Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), September 2010,pp. 347-356.
26. R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi and Z. Song,” Authentication in the clouds: a framework and its application to mobile users,” in Proceeding ACM Cloud Computing Security Workshop, CCSW ’10, Chicago, USA,Oct. 2010.
27. W. Jia, H. Zhu, Z. Cao, L. Wei and X. Lin,” SDSM: a secure data service mechanism in mobile cloud computing,” in Proceeding IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China, Apr. 2011.
28. J. Yang, H. Wang, J. Wang, C. Tan and D. Yu1, “Provable data possession of resource constrained mobile devices in cloud computing,” Journal of Networks ,2011,pp. 1033–1040.
29. Saman Zonouz, Amir Houmansadr, Robin barthier, Nikita Borisov,William Sanders,”Secloud:A cloud based comprehensive and lightweight security solution for smartphones,” published in Science Direct journal of Computers and security ,Volume 37, 2013, pp. 215-227.
30. Vijay Varadharajan, Senior Member, IEEE, and Udaya Tupakula, Member, IEEE "Security as a Service Model for Cloud Environment" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 11, NO. 1, MARCH 2014
31. Qiao Yan, F. Richard Yu, Senior Member, IEEE, Qingxiang Gong, and Jianqiang Li "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges" DOI 10.1109/COMST.2015.2487361, IEEE Communications Surveys & Tutorials
32. O. Khalid, M. Khan, S. Khan, and A. Zomaya, “Omni Suggest: A Ubiquitous Cloud based Context Aware Recommendation System for Mobile Social Networks,” IEEE Transactions on Services Computing, 2014.
33. Pallavi Kulkarni and Rajashri Khannai, Member, IEEE “Addressing Mobile Cloud Computing Security Issues: A Survey” IEEE ICCSP 2015 Conference

BIOGRAPHY

Nirbhay K. Chaubey, Senior Member of IEEE, currently working as an Assistant Professor of Computer Science at Institute of Science & Technology for Advanced & Studies, Vallabh Vidyanagar, Gujarat, India. He obtained his PhD Degree in Computer Science from Gujarat University, Ahmedabad in year 2014.

Darshan M. Tank currently working as a Lecturer at L E College, Morbi, Gujarat, India. He obtained his Master's from D.D.University, Nadiad. His areas of interest include cloud storage, mobile computing, mobile cloud computing and wireless networks.