Privacy and Security in Mobile Cloud Computing: Review

Sapna Malik
GGSIPU University
Delhi,India

MM Chaturvedi
Ansal University
Gurgaon,India

ABSTRACT
Mobile cloud computing is computing of Mobile application through cloud. As we know market of mobile phones is growing rapidly. According to IDC, the premier global market intelligence firm, the worldwide Smartphone market grew 42.5% year over year in the first quarter of 2012.With the growing demand of Smartphone the demand for fast computation is also growing. Inspite of comparatively more processing power and storage capability of Smartphone's, they still lag behind Personal Computers in meeting processing and storage demands of high end applications like speech recognition, security software, gaming, health services etc. Mobile cloud computing is an answer to intensive processing and storage demand of real-time and high end applications. Being in nascent stage, Mobile Cloud Computing has privacy and security issues which deter the users from adopting this technology. This review paper throws light on privacy and security issues of Mobile Cloud Computing.

General Terms
Privacy and Security.

Keywords
Cloud computing ,Mobile Cloud Computing,Privacy,Security,M-Commerce.

1. INTRODUCTION
Cloud Computing refers to computing services provided over network. A more formal definition of cloud computing from a business perspective as well as from a technological perspective given by Sean Marston et al. [2] in their research paper is as follows: "It is an information technology service model where computing services (both hardware and software) are delivered on demand to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality-of service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the cloud services employing a metering system that divides the computing resource in appropriate blocks."

A venture which needs storage and processing resources can be kicked off with its pay and go feature in no time without any botheration of resources. As Combination of cloud computing and mobile computing, Mobile Cloud Computing is a new research topic since 2009. Mobile Cloud Computing has three components, mobile device, wireless communication channel and cloud. Mobile devices have resource constraint in terms of battery power, memory, processing power and have different types of hardware, operating system, and input - output interface. Wireless communication channel has different radio access technologies such as GPRS, 3G, WLAN and WiMax with variable network conditions in terms of limited and unstable bandwidth. Cloud Computing is facing various security and privacy challenges. Security and privacy issues in mobile cloud computing are inherited from cloud computing and mobile computing. Because of resource constraints, heavy security algorithm can't be run on mobile device. We need to do efficient task portioning between cloud and mobile to resolve the security and privacy issues in Mobile Cloud Computing. The rest of paper is organized as follows. In Section 2, we present the Service Model and Deployment Model of Cloud Computing. Mobile Cloud Architecture, Mobile Cloud Models, Features of Mobile Cloud Computing and application is in Section 3. Privacy and Security Issues in Mobile Cloud Computing and its Literature Review is in Sections 4. Open Issues in Mobile Cloud Computing and Conclusion is in Section 5 and Section 6 respectively.

2. CLOUD COMPUTING

2.1 Service Model
In cloud computing there are mainly three service models:

2.1.1 Software as a Service(SaaS)
In SaaS, Users access the cloud application through interface like web Brower as per requirement and pay for use. In SaaS, it's the responsibility of cloud provider to maintain the hardware, operating system and application maintenance. Cloud provider provides the security to client as per service level agreement. Multiple Clients can access the application at the same time with their respective subscription. Examples of SaaS are SalesForce, Customer Relationship Services, Google Apps, Gmail, and Google Docs.

2.1.2 Platform as a Service (PaaS)
PaaS provide operating system and other tools for software development and allow client to deploy its application on the cloud. Client need not maintain the cloud infrastructure like storage, servers, operating system, programming tool kit, network and software licence. Client only maintains its software or application and its environment configuration deployed on cloud. Examples of PaaS are Microsoft Windows Azure, Google App Engine, Amazon Web Services, and Elastic Beanstalk.

2.1.3 Infrastructure as a Service(IaaS)
In IaaS client has direct access to CPU processing, servers, network, and storage devices. Client can install and use operating system, software's of their choice on their virtual machines accessed through IP address. Cloud provider maintains the underlying infrastructure and provides virtualized IP address to the clients for direct access to

hardware resources. Examples of IaaS are Amazon EC2, IBM Computing on Demand, GoGrid and Rackspace Cloud.

2.2 Deployment Models

In Cloud Computing there are four deployment models:

2.2.1 Private Clouds: Private Clouds are dedicated to one organisation who owns it. The organization has full control on data, servers, networking, security and quality of services. Private clouds are for enterprise critical application and operations.

2.2.2 Public Clouds: Public clouds are accessed by everyone who is subscribed for it all over the world. Public clouds are owned and maintained by the cloud provider who rents parts of services to different users. Examples are Amazon, Google etc.

2.2.3 Community Cloud: Community clouds are cloud owned by the group of organizations with similar service requirements. Community clouds are able to provide security features like those of private cloud and are economical like public clouds. Example, media cloud set up by Siemens.

2.2.4 Hybrid Cloud: Hybrid clouds are combination of two or more clouds. For example, an organization owner of private cloud can use service of public cloud for non critical operations.

3. MOBILE CLOUD COMPUTING

3.1 Mobile Cloud Architecture

There are two types of Architecture in Mobile Cloud Computing

- Cloudlet Architecture
- Non Cloudlet Architecture

In Non Cloudlet Architecture there are three components Mobile client, Transmission channel and Cloud. Mobile client requests desired service from cloud and cloud provides the service. Cloud is owned by an organization or cloud provider and services thousands of users at time. In this architecture, main disadvantage is communication latency for getting service from distant cloud. The solution to this problem is cloudlet architecture in which a local cloudlet contains cached copy of data. It is installed between client and cloud. The cost of installation is less as compared to cloud as it is only a data centre at business premises. A cloudlet services only a few users and has less communication latency as compared to cloud. Cloudlet is owned by local business [3].

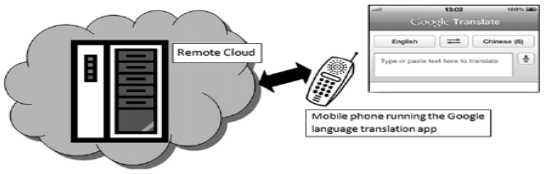

Fig. 1 Non Cloudlet Architecture [4]

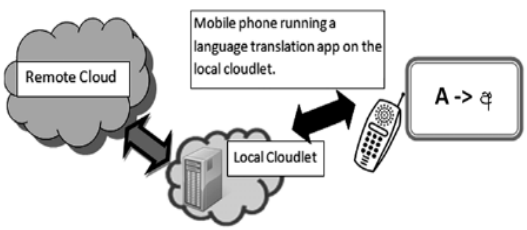

Fig. 2 Cloudlet Architecture [4]

3.2 Mobile Cloud Model

There are three Mobile Cloud Models [5]:

3.2.1 Client Model: In this model, mobile device act as client and mobile user access service is offered by cloud by thin layer of interface web browser. Cloud charges for services till the duration client is connected. Client model depicts Software as a Service model of Cloud computing.

3.2.2 Client /Cloud model: In client /cloud model, the concept of task partitioning comes in which mobile users give a part of task to cloud for processing.

3.2.3 Cloud Model: In cloud model, mobile device itself is the part of cloud. One or more mobile devices create the structure of cloud.

3.3 Features of Mobile Cloud Computing

- Network latency and limited bandwidth
- Different radio access network
- Energy and resource constraint mobile device
- Different Mobile device operating systems and hardware
- Input - output interface of mobile device
- Fluctuating network condition

3.4 Application of Mobile Cloud Computing

Because of more demand of processing and storage capability for mobile devices, Mobile Cloud Computing is gaining popularity. Some Mobile Cloud Computing applications are discussed below.

3.4.1 Mobile Commerce: Mobile commerce has made the market available in customer's hand-anywhere anytime. According to Bangalore based management consulting firm Zinnov, e-commerce is expected to increase from US$6.3 billion in 2011 to US$23 billion by 2016 [6].The buzz is growing around mobile transactions. M-commerce is creating ripples in the business world by providing instant access to customers. The sales have grown phenomenally because of the introduction of m-commerce in business which is evident in business companies like e-bay, snapdeal, mantra.com and many more.

3.4.2 Mobile Learning: Traditional education system has certain limitations like in remote areas quality education is not easily accessible, however mobile learning can bridge this gap. For example, Indian top educational Institutes IIT Kanpur [7] [8] and NIIT have launched their own cloud to facilitate research and educational activities.

3.4.3 Mobile Healthcare: Better health services can be provided with mobile healthcare by having ubiquitous access to patients, clinical data and clinical knowledge. A patient can be kept under observation without specialized doctor being physically present with the help of Mobile Healthcare. Even, authenticity of the drugs can be checked by accessing cloud database of the company through mobile [8] [9].

3.4.4 Image processing: We can give more features to Smartphone in gesture recognition, like image process applications through Mobile Cloud Computing by processing their data through cloud.

3.4.5 Speech recognition and synthesis: Speech Recognition application like language translator can help mobile user to feel comfortable in a country where language is not known or understood by the mobile user.

3.4.6 Mobile Banking: Now a day's mobile banking is gaining more popularity than e-banking because of more mobile users than internet users

3.4.7 Social Networking: Social networking like face book, what's up help in staying connected with people with Mobile Cloud Computing.

3.4.8 Mobile Gaming: As we know games demand more processing and graphic hardware, with Mobile Cloud Computing it is possible to use high end gaming application on mobile phone.

3.4.9 Mobile Security: Mobile cloud computing can provide more security to the mobile device by proving security through cloud.

4. SECURITY AND PRIVACY IN MOBILE CLOUD COMPUTING

4.1 Security and privacy risk in Mobile Cloud Computing

As Mobile Cloud Computing is combination of mobile computing and cloud computing, security risk in mobile computing 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.

4.2 Literature Review

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al. [10] proposed Cloud AV platform, malware detection system. In this architecture, mobile agent first analyses the malicious file. If its signature is not matched with the cached database, it is sent to the network service for analysis with the help of multiple detection engines running parallel on host machines with the help of virtualization technique. These techniques have the advantage of better detection of malicious software, reduced on device software complexity and power consumption but suffer from limitations of disconnected operation and accidental privacy hazard.

S Zhang et al. [11] presents security framework which adapts mobile device with changing workloads, performance goals and network latency by migrating processing weblets between cloud and mobile device. They enhance this model by trustworthy weblets container, Authentication and secure session management, Authorization and access control of weblets, Logging and auditing behaviour of weblets to make more secure framework. Although security during weblets migration can be improved by other security techniques and cloud environment can be made more trustworthy.

Xiao and Gong [12]proposed lightweight algorithm for ensuring authorization in mobile cloud environment by generating automatic dynamic credential information with mutual coordination of mobile device and cloud so frequently that it is difficult for hackers to hack credential information of users. However frequent updation of secret information of user increases processing burden and energy consumption on mobile device and communication overhead between mobile and cloud.

Wang and Wang [13]have proposed framework that uses cloud for providing number of live users in region based on historical data saved in cloud which helped in minimization of processing and communication overhead in cloud but doing spatial cloaking based on historical data can lead to privacy loss. The cloaking in mobile device increased processing overhead and energy consumption.

Huang et al. [14]presents framework – MobiCloud in which the secure computation is done with three domains (a) cloud mobile and sensing domain (b) cloud trusted domain and (c) cloud public service and storage domain. Security to critical data is provided by isolating public cloud and trusted cloud. In this scheme client uses the services of two cloud service providers so it increases the communication cost and network latency.

G. Portokalidis et al. [15] proposed scheme for threat detection in a smart phone based on CloudAV research by Oberheide et al. [9]. In cloud we have multiple replica of Smartphone which can detect different types of attacks in parallel. The proposed scheme reduced the transmission overhead below 2.5KiBps and reduced energy consumption 30%. In this technique cloud is considered fully trusted which needs to be given second thought.

H.Zhang and X Mingjun [16] proposed distributed spatial cloaking in which distributed anonymity having location information for cloaking. Distributed anonymity can handle frequent requests from users without being bottlenecked.

P.Zou et al. [17] proposes Phosphor in which interaction between Sim card and Digital Rights Management Agent has been protected by the License Status Word protocol.

R.Chow et al. [18] present authentication platform in which behavioural authentication is used based on client personal data. The cloud authentication platform responds to the client access request based on decision obtained by processing behavioural data of the authenticated client, however, passing the personal information of the client to cloud can affect the user privacy.

Itani et al. [19] proposed a cloud based energy efficient framework to ensure integrity of mobile users. In this approach there are three main components (a) mobile client (b) cloud service provider (c) trusted third party. Cloud service provider provides storage resources. The security is provided by trusted third party. The framework shows 90% saving in processing and energy but suffers from limitation of data security in public cloud and less scalability of trusted third party.

Jia et al. [20] presents framework for secure data service with proxy re-encryption (PRE) scheme and identity based encryption (IDE) scheme . In this scheme, privacy of user is secured as the cryptography of data is done by user but it increases the energy and processing requirement of mobile device.

Huangs et al. [21] proposed framework for authentication on MobiCloud, to achieve secure data processing.

.Hsueh et al [22] proposed authentication mechanism in which mobile device encrypts the credential information file and stores it on cloud but infected cloud server can steal the user credential information by decrypting user's files.

Yang et al. [23] presents public provable data possession scheme for mobile cloud computing. Client's mobile device embedded with trusted platform model (TPM) chip ensures authenticity of client and generates secret key for secure data transmission between client and trusted third agent. The secure data transfer between TPA and client is done with Diffie Hellman Key Exchange. TPA does all the heavy work of encryption, decryption and authentication on behalf of mobile device. Proposed framework uses Bilinear mapping and merble hash tree for integrity. This scheme ensures privacy, confidentiality and integrity of user data stored on cloud but leads to degradation of performance with the increase of users in TPA. Cost also increases due to two cloud service providers.

Chen et al. [24] presents security framework for location based grouped scheduling services using IMSI-based JOIN secure (IJS) algorithm that uses international mobile subscriber identity (IMSI) as user identification integrated with encryption algorithms. However, if mobile device of the client is stolen by some adversary, he can affect security in the system.

Ren et al. [25] proposed lightweight schemes with less computational overhead for ensuring data security on distributed cloud .these schemes are encryption based, coding based and sharing based.

Zhou and Huang [26] proposed a privacy preserving framework in which encryption and decryption on cloud based on Cippher text Policy attribute which inherited the security problem of Cippher text Policy.

Niroshinie Fernando et al. [4] proposed generic architecture for implementing a mobile cloud with locally available mobile devices. This architecture has components: 1) Resource Handler 2) Cost manager 3) Job handler 4) Privacy and Security Manager 5) Context Manager. Resource manager manages resources like searching and connecting other mobile devices. Cost manager takes the decision of offloading according to user's priorities like battery conservation, fast execution, monetary gain etc. Job handler partitions the job for offloading and maintains job pool. Privacy and security manager maintain the security while interfacing with other devices. Context manager helps job handler in resource monitoring and to manage mobility inside the cloud.

Saman Zonouz et. al. [27] proposed Secloud; a cloud based comprehensive and lightweight security for smartphones. Secloud runs the emulators of Smartphones in cloud which provide security to mobile device by security analysis of data in mobile device. In this architecture 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.

Table 1 summarizes the features of the various approaches described above.

5. OPEN ISSUES IN MOBILE CLOUD COMPUTING

- To develop efficient cloudlet design with minimum cloudlet installation cost and more computing power and less network latency.[3]
- To develop efficient security and privacy algorithm for ensuring confidentiality, integrity, authenticity and privacy of user data [23].
- To develop efficient task portioning algorithm for ensuring less communication cost and less energy requirement on mobile device [28][11].
- To provide software libraries with clearly defined API support for mobile cloud application developer.[29]
- To design platform independent security algorithm [30].
- To reduce the cost of security framework by removing trusted party agent between cloud and client [13][17].

6. CONCLUSION

Mobile Cloud Computing is a new paradigm since 2009 and it is still in nascent stage. The security and privacy issues in mobile cloud computing are inherited from cloud computing, however, it is difficult to resolve these issues because of resource constraint in mobile devices like energy, storage, processing etc. To address the security and privacy issues, we will have to develop efficient security and privacy framework with the objective of lesser resource requirement in mobile device and minimize the communication cost and network latency while ensuring privacy, authenticity and integrity of user's data in cloud.

Table1. Comparisons between Researches in Privacy and Security Issues in Mobile Cloud Computing.

Researchers	Year	Approach	Cloud Trust Level	Security Attribute provided	Trusted Third party	Advantages	Disadvantages
J. Oberheide et al. [10]	2008	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. [11]	2009	Cloudlet	Semi-trusted	Task partitioning	No	Good tradeoffs between processing overhead and communication cost	Security of Weblet can be improved with other techniques.
Xiao and Gong [12]	2010	Lightweight algorithm	Semi trusted	Authorization of user's data in cloud	No	Automatic Dynamic updation of credential information	More processing and energy burden on mobile device
Wang and Wang [13]	2010	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. [14]	2010	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. [15]	2010	Threat detection in Smartphone based on CloudAV	Fully trusted	Security as a Service	No	Reduced transmission overhead and energy consumption	More Cloud usage cost.
R.Chow et al. [18]	2010	Policy based cloud authenticatio n platform	Fully trusted	Authentication of user.	No	Authentication based on behavioural data of user	Privacy threat
Jia et al. [20]	2011	Proxy re-encryption (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 saved on cloud.
Yang et al. [23]	2011	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. [27]	2013	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.

7. REFERENCES

[1] IDC global market intelligence firm (2011, Dec) Worldwide Smartphone 2011-2015 forecast [Online] Available: http://www.idc.com.

[2] Marston S., Li Z., Bandyopadhyay S., Zhang J. and Ghalsasi A.,2011 ,Cloud Computing – The business perspective. Decision Support Systems, vol. 51, Issue 1, 176-189.

[3] Satyanarayanan, M., .Bahl P, Caceres R. and , Davies N. 2009, The case for VM based cloudlet in mobile computing .In proceeding of IEEE Pervasive Computing ,14-23 .

[4] *Niroshinie Fernando , Seng W, Loke Wenny, Rahayu*. "Mobile Cloud Computing: A Survey," published in Journal of Future Generation System ,Vol 29,issue 1,2013,January,2013,pp.84-106

[5] Daniela POPA ,Marcel Cremene ,Monika Borda,Karima Boudaoud ," A Security Framework for Mobile Cloud Applications," published in IEEE 11th Roedunet International Conference,2013,pp. 1-4.

[6] India Knowledge@Wharton (2013,june 13) Mobile's Dramatic Growth in India Spurs a New Era of E-commerce,[Online],Available: http://knowledge.wharton.upenn.edu/india/article.cfm?articleid=4739.l

[7] K. Raghu (2008, Sept 24).IBM's India Lab to Innovate Cloud Computing Solutions, [Online] Available: www.livemint.com/2008/09/24222631/IBM8217s-India-lab-to-innov.html.

[8] Nir ksshetri ," Cloud Computing in India" published in IEEE Computer Society,2012

[9] Times of India, C. Gopalakrishnan (2011,29 Sept).How Cloud Technology Can Help You Spot Fake Drugs,[Online],Available : http://timesofindia.indiatimes.com/tech/personal-tech/computing/How-cloud-technologycan-help-you-spot-fake-drugs/articleshow/10168266.cms

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] D. 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.

[15] 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,

[16] H. Zhangwei. and X. Mingjun," Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2,June 2010, pp. 468.

[17] P. Zou, C. Wang, Z. Liu , and D. Bao, " Phosphor: A Cloud Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), June 2010,pp. 459.

[18] 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.

[19] W. Itani, A. Kayssi, and A. Chehab," Energy-efficient incremental integrity for securing storage in mobile cloud computing," in Proceeding International Conference on Energy Aware Computing, ICEAC '10, Cairo, Egypt, Dec. 2010.

[20] 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.

[21] D. Huang, Z. Zhou, L. Xu, T. Xing and Y. Zhong," Secure data processing framework for mobilecloud computing," in Proceeding IEEE INFOCOM Workshop on Cloud Computing, INFOCOM '11, Shanghai, China, June 2011.

[22] S.C. Hsueh, J.Y. Lin and M.Y. Lin," Secure cloud storage for conventional data archive of smart phones " in Proceeding 15th IEEE International Symposium on Consumer Electronics ,ISCE '11, Singapore, June 2011.

[23] 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.

[24] Y.J. Chen and L.C. Wang," A security framework of group location-based mobile applications in cloud computing," in Proceeding. International Conference on Parallel Processing Workshops, ICPPW '11, Taipei, Taiwan, Sep. 2011

[25] W. Ren, L. Yu, R. Gao and F. Xiong," Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing," Journal of Tsinghua Science and Technology,2011,pp. 520–528.

[26] Z. Zhou and D. Huang," Efficient and secure data storage operations for mobile cloud computing," IACR Cryptology, 2011,ePrint Archive: 185.

[27] 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.

[28] Han Qi and Addullah Gani," Research on mobile Cloud Computing:review,trend and Perspectives" in preceding of IEEE second international Conference on Digital information Technology & its application,2012,pp.195-201.

[29] Paramvir Bahl,Richard Y.Han,Li Erran Li,Mahadev Satyanarayanan,"Advacing the state of Mobile Cloud Computing," in preceding of the third ACM workshop on Mobile cloud computing and services, New York,USA,2012,pp.21-28

[30] Wei Tang, Jun-hyung Lee, Biao Song,Motaharul Islam,Sangho Na,Eui-Nam Huh,"Multi-Platform Mobile Thin Client Architecture in Cloud Environment" in Precedia Environmental Science, Volume 11,Part A,2011,pp.499-504