Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing the Android Phones Using the Power of Cloud

Jaspreet Kaur Aulakh*,Sugandha Sharma
Dept. of Computer Science
Chandigarh University Gharuan Mohali,
India

Mayank Arora
Dept. Of Computer Science
CCET Punjab University Chd,
India

Abstract— This article is review of the Mobile Cloud Computing, including the meaning of Cloud computing, as well as the concept of Mobile Cloud Computing. This paper shed light on the basic model and presents a report on the approaches in mobile cloud computing. There are many issues in Mobile Cloud Computing such as operational issues, End user level issues, Service and Application level issues, Management of data. Security and privacy issue is one of the major issue in Mobile Cloud Computing. This paper proposed an architecture in which we encrypt the data of mobile phones using progressive technique in the environment of cloud. Encrypting the data on the phone using the progressive encryption scheme and analyzing the resources used while encrypting. It provides the security to mobile user and save the resources of mobile device.

Keywords - Cloud Computing, Mobile Cloud Computing, Mobile Cloud Security Issues.

I. INTRODUCTION

[1] CLOUD COMPUTING

Within the last few years cloud computing is becoming the most popular among today's technology. Cloud is a cluster or group of computers it can be a personal computer or servers which are interconnected to each other within a network providing on demand services to the users. According to the National Institute of Standards and Technology (NIST), Cloud Computing is a on-demand service that provide online resources on the demand of users according to the requirements such as network, storage space ,applications and services[6]. Cloud provides various services such as consulting service, management services, financial services, data storage services. Basically users get reliable, scalable computing resources on demand. Computing service offered as a utility where you only pay per use like electricity, gas, water etc

[2] DEPLOYMENT MODELS OF CLOUD COMPUTING:-

Public Cloud:-A public Cloud provides the software and hardware services to general people for example Google Drive.

Private Cloud: - The cloud that is owned by a particular organization for security purpose. Some organizations set up their cloud within the organization.

Hybrid Cloud:- The combination of both public and private cloud is the 'hybrid cloud' [1] It provides the services private sector as well as publically.

Community Cloud:- The 'Community Cloud' is used for the particular community such as education community, medical etc.

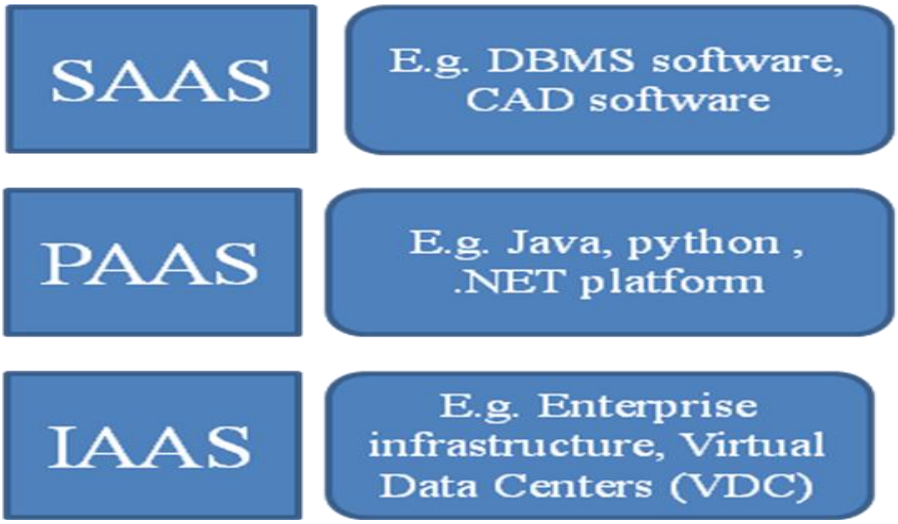


Fig. 1 Service Model of Cloud

[3] SERVICE BASED CLOUD COMPUTING:-

Service Model of Cloud Computing described by The National Institute of Standard and Technology (NIST).

IaaS:- Infrastructure as a Service. In this, the cloud provides the resources such as storage, networks and peripheral resources as a service over a network to its users.

PaaS:- Platform as a Service. Cloud provides the complete platform for development including hardware and software. It is normally used by programmers or developers.

SaaS:- Software as a service. The Cloud provides he applications to the users as a service. For example Google Docs provides Word processing software online to the users.

[4] MOBIE CLOUD COMPUTING

The term Mobile Cloud Computing means to benefit from the Mobility of Mobiles and the rich functionality and resources of the Cloud. In Mobile Cloud Computing cloud's resources are provided to the mobile devices to increase the overall efficiency and performance of mobile phone. The main benefit of Mobile Cloud Computing is that the mobile device offloads its workload by shifting large data on the Cloud. In the environment of Mobile Cloud Computing, smart phones can obtain the services in a network. In the Mobile Cloud Computing, the compute intensive part of the application (heavy part of application) or whole execution can be shifted to the Cloud for the execution. After the execution is complete, the results are sent back to the mobile device. In this way user can save the resources of mobile devices. This technique of distributing the load is known as Offloading. Mobile devices have limited capability so by using the cloud's resources user can enhance the computing power and Battery life of the mobile devices and thus making them efficient enough to cater the High End, heavy applications.

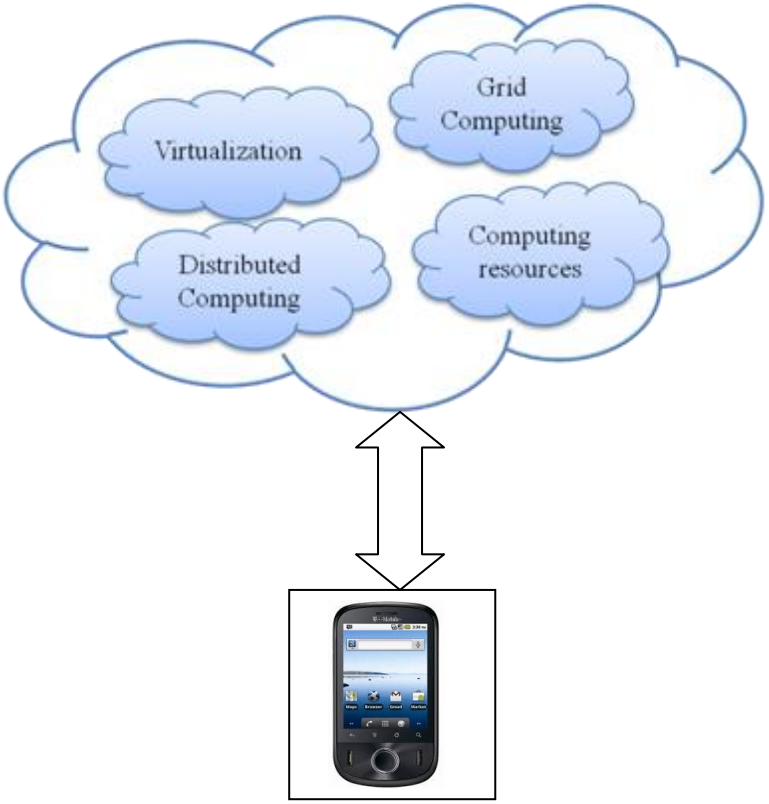


Figure 2. Basic Model of Mobile Cloud Computing

Basic model of Mobile Cloud Computing as shown in Figure 2 shows that the Cloud provides the resources such as storage, processing and software. On the other hand user i.e. a Mobile Device uses the required services on demand and could pay as per their usage [1].

[5] ADVANTAGES OF MOBILE CLOUD COMPUTING

a) Enhanced Capabilities:- If the high computation tasks could be executed on a resource rich remote server the Mobile devices could run much heavier applications than their processing power, thus enhancing their capabilities.

b) Increase Battery life:-Heavy applications use large battery. It is the major drawback of mobile device. So user can save energy by the concept of computation offloading technique of Mobile cloud computing.

c) Enhance Data storage capacity- Cloud server provides the memory to the mobile user because mobile devices have limited space for data storage.

d) Improving reliability- Mobile cloud computing improve the reliability because Information placed on number of computers at cloud's environment that means data will not be lost.

[6] SYSTEM ARCHITECTURE OF MOBILE CLOUD COMPUTING-

Mobile Cloud Computing divided into four layers-access layer, management layer, virtual layer and physical layer[1].

1. Access layer: It is an interface between user and cloud end. This layer of architecture describe service interface to the client, service registration and service access.

2. Management layer: This layer is used to manage the services. The user management section describes the mobile account management, user environment configuration, and user interaction management and accounting system. Task management manage the task scheduling and task execution. Resource management includes balance the workload; test the errors, and recovery of information. Security management includes identity authentication, access that authentication, security audits and protection of data.

3. Virtual layer: Virtual layer includes various resources such as computing resources, network resources, software resources and data storage resources. This layer describes the virtual environment, virtual system and virtual platform that does not exist in reality.

4. Physical layer: This layer includes the peripherals devices like personal computers, mobile phones, network devices and memory. The handheld devices do not require large and strong computing power but only need for input and output sources.

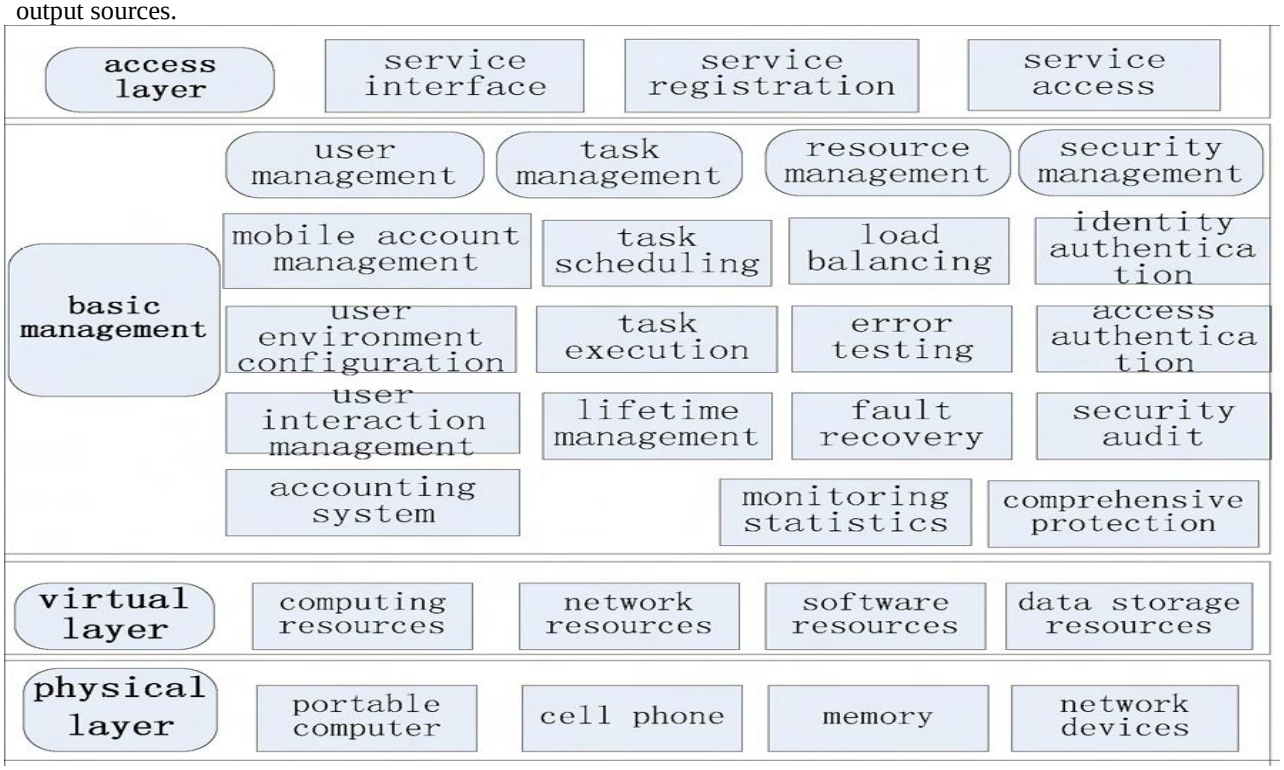


Figure3. System architecture of mobile cloud computing [1]

[7] APPLICATIONS OF MOBILE CLOUD COMPUTING:-

The applications of Mobile Cloud Computing are very broad and are increasing every day. Any application running on recourse rich server and being used by a mobile device is an application of Mobile Cloud Computing. For eg. Gmail, Google Drive provided by Google. Amazon's new "cloud-accelerated" Web browser Silk. Silk is a "split browser whose software resides both on Kindle Fire and EC2. Some other applications classified according to their nature of use are described as follows:-

Mobile-Commerce:- Online buying and selling any product by using mobile phones is known as Mobile Commerce. During the transaction many problems occurs due to low capacity of mobile devices. To enhance the capacity use the cloud's resources for commerce.

Mobile -HealthCare:- Mobile Cloud Computing is used in Medical treatment applications. Cloud provides on demand

Services to the mobile users. As a consequence it overcome problems of previous treatment in medical.

Mobile -Banking:- Mobile banking is a system which allow the user to access financial transaction by using mobile phone. The mobile banking services offered through mobile SMS or mobile web. Some special mobile applications download in mobile devices to access the banking services.

Mobile-Learning:- Mobile learning provide the learning services to user. Mobile learning that is based on Cloud Computing improve the limitation of traditional mobile learning by utilizing the powerful resources of cloud to mobile user[10].

Organization of Paper- The first section describes the introduction of Cloud Computing and Mobile Cloud Computing. Security of Mobile Cloud Computing is presented in Section 2. In Section 3 the review of related work is

explained. The proposed architecture of encryption is described in Section 4. Finally, the conclusion of the paper is in last section.

II . MOBILE CLOUD COMPUTING SECURITY

Security is a major issue in case of Mobile Cloud Computing. While considering Mobile Cloud Computing the security concerns related to Cloud Computing are in the picture as well as some issues relating to mobile are application security and the device security also jump in. The mobile device acts as node in the internet thus becomes very vulnerable to all kind of hackers and attackers. Some of the Security Issues regarding Mobile Cloud Computing are discussed as follows:-

Network Security:- In mobile devices large number of threats could come during the transaction in a network. Some applications to these devices can cause privacy issues for mobile users. The network security covers all security issues concerning the network which is used by the mobile, internet service providers etc. The networks could be Private and Public. In case of a private network the security measures could be reliable in an known organization but as a user switches the network to a public network the reliability is a big concern. For example while travelling the user uses the Wireless Internet provided in a Train. In such cases the mobile devise becomes Vulnerable as the network being used could not be trusted.

Application Level security:- The applications installed in a mobile device could be a threat to the user's confidential data. The applications installed on the phone by the user from some un-trusted sources could lead in data leakage from the mobile phone. A strong trust mechanism should be devised to ensure the applications running on a phone with confidential information may not be a threat to the user. So the user should care about the application which he want to install on device.

Privacy:- Protect the data from physical access of unauthorized party. Providing the private information to the authenticate user only. To protect the sensitive information encrypt the data using some good encrypting scheme thus if the phone is physically lost then also the data will be of no use of others.

Cloud Security:- The organization or individual store their data to the cloud's server. The security issues are

Integrity:- The user guarantee the integrity the information which is stored on the cloud. Every access they make must me authenticated and verified. Various methods are used for preserving the integrity of stored information.

Authentication*:-* To secure the data access suitable for mobile environments use the various approaches of authentication . Username and passwords given to the authenticate user so that the unknown person cannot access the data. There are three A's in Authentication management i.e. Authentication, Authorization and Auditing. Authentication means, to verify whether a user is actually an legitimate user or not. This is done by ensuring authentication policies such as username and passwords. The term authorization means that only an authorized user will be given access to a particular set of applications/data. Auditing is one of the main compliance requirement. With the help of Auditing if something goes wrong we can find out the exact cause of it, thus making the system more reliable.

Digital rights management:- The Illegal distribution and piracy of digital contents such as video, image, audio, and e-book, programs becomes more and more popular. Some provisions are given to the legal users such as digital signature. Encryption and description is used to access the secure data.

III. RELATED WORK

Security of Mobile Cloud Computing has been discussed by many researchers.

Chun et al. [5], proposed a framework in which application is partitioned using a static analyzer, dynamic profiler & an optimization solver. Migration takes place at thread level Phone always has to be kept synchronized; the details of synchronization have not been provided. Chen et al. [12] depicts the security framework for location based grouped scheduling services using IMSI-based Join Secure (IJS) algorithm. In this work IJS used International Mobile Subscriber Identity (IMSI) as user identification integrated with encryption algorithm.

Itani et al. [13] proposed a framework based on the cloud to ensure the integrity of mobile device. This framework has divided into three domains: - 1.Mobile Client 2. Cloud Service provider 3. Trusted Third Party. Mobile Client send the request to server and the Cloud Service Provider provides the resources according to the requirements. This approach is helpful to save large amount of processing and energy. But the limitation is that there is lack of data security in public cloud. Ren et al. [14] present an encryption based scheme having very less computational overhead for ensuring data security on distributed cloud. Jia et al. [15] presents a framework used proxy re-encryption (PRE) and identification based encryption (IDE) for the security of data. In this approach, cryptography of data is done by user and this procedure increase the processing power and energy rate of mobile phone.Wang and Wang [16] proposed a framework in which large number of live user in a cloud based on historical data saved in cloud. This procedure minimizes the communication and processing overhead in cloud. But cloaking used in mobile phone can lead to lack of privacy as well as increase the energy consumption. Saman Zonous et al. [17] proposed a method that provide the security for mobile phone. In this method, Secloud is used in Cloud which ensures the security of Smartphone by security analysis of data in mobile phone. Eric Y. Chen and Mistutaka Itoh[18] present a Virtual smartphone over IP system that helps to user to create virtual image of smartphone in mobile cloud. User can easily install the applications in cloud and run those applications remotely. In this approach the complete application was offloaded from the android smart phones to the cloud. This architecture provides a viable solution to data leakage problem.

Lakshmi Subramanian [19] proposes an architecture for providing security services in the cloud for smartphones within a corporate environment. This paper provides the Cloud based Security Functions such as Anti-virus, Secure Browsing, OS Integrity Checks, Remote Wiping and Versioning, Secure Storage, Policy Control .

Dijiang Huang [20] develop a pilot mobile cloud system implement the cloud trusted domain for data security. For the security and privacy develop a private application "Focus Drive" project which is conducted by Secure Networking and Computing research group.

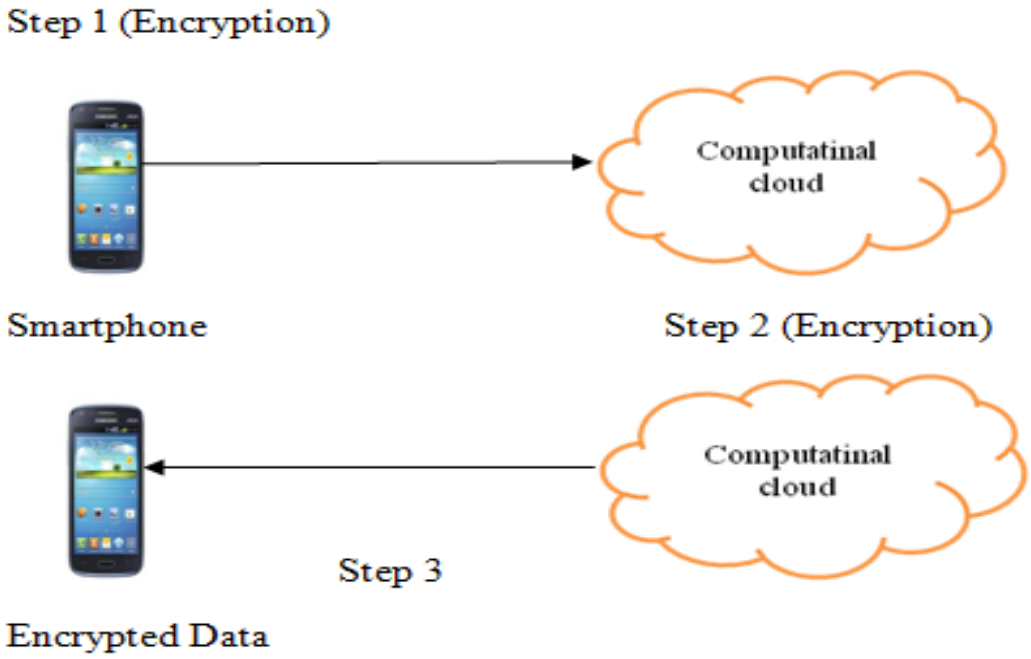
IV. PROPOSED WORK

Mobile Cloud Computing is a hot topic for the Industry as well as the researchers. It gives the benefits of Mobility using hand held devices such as smart phones or tablets as well as power of the Cloud. As more and more important tasks are being done using smart phones such as e commerce and more enterprise applications are coming forward the issue of security is also increasing. The mobile phones are more vulnerable to security threats because of their size. The operating system in the phones is also not very powerful in order to make them secure from external threats. The threats to the information while using mobile cloud computing could be categorized into two major categories:-

1. Mobile network security
2. Cloud security

Our focus will be on making the data in the smart phone secure enough so that in case of a theft the data is not misused. This could be cone by encrypting the data using some proven encryption scheme. This will ensure the safety of data but will impose an overhead on the smartphone to encrypt the code. It is proposed that if the encryption be done using the power of cloud then the process could be fast as well as it could ensure security.

The working of the proposed architecture could be better understood with the help of the following diagram. The data in the mobile phone is first encrypted at the phone side using Progressive Encoding. In progressive encoding scheme the information could be encrypted multiple times using completely different keys and will be decrypted using a single key.



So the encryption in this will be a two stage process firstly the data will be encrypted on the phone itself and then the data will be encrypted on the computational cloud and the final encrypted data will be stored in the Smartphone. Now if the phone gets lost the data will be of no use for anyone except the authentic user of the phone who possesses the Key to decrypt the data.

V. CONCLUSION

In recent years, the number of mobile users is increasing day by day, the usage scenarios are changing according to advancement in technology. A number of users are moving towards m-commerce applications and accessing sensitive information through their mobile phones. Thus making the mobile phones more lucrative subject for hackers and attackers. This makes it uttermost important to device good security mechanisms thus making Mobile Cloud Computing secure. The objective of Mobile Cloud Computing to provide the resources to the users and enhance the performance of mobile devices. In this paper, user can secure the data of mobile device through encryption as well as save the resources of mobile phone by shifting the encryption process to cloud. The various threats regarding mobile cloud computing have been discussed in this paper. The Threats could be categorized into two main categories i.e. Mobile side and Cloud side threats.

REFERENCES

[1] Weygand SONG and Xiaolong SU, " Review of Mobile Cloud Computing" IEEE 2011.

[2] Niroshinie Fernando , Seng W. Loke Wenny Rahayu,"Mobile Cloud Computing: A Survey.

[3] Han Qi and Abdullah Gani, " Research on Mobile Cloud Computing : Review , Trends and Perspectives".

[4] D. Popa1 K. Boudaoud2 M. Cremene1 M. Borda1, "Overview on Mobile Cloud Computing Security Issues".

[5] B.G. Chun, S. Ihm, P. Manitis, M. Naik and A. Patti," Clone Cloud : Elastic Execution between Mobile Device and Cloud," in Proceedings of 6th Conference On Computer Systems, 2011, pp. 301-314.

[6] The NIST Definition of Cloud Computing,"National Insitiute of Standard and Technology".

[7] Goran Kalic , Iva Bojic and Mario Kusek, "Energy Consumption in Android Phones When using the Wireless Communication Technologies" 2012.

[8] Karthik Kumar · Jibang Liu · Yung - Hsiang Lu ·Bharat Bhargava , " A survey of Computation Offloading for Mobile Systems" Springer 2012.

[9] Soeung-Kon(Victor) Ko1), Jung-Hoon Lee2), Sung Woo Kim3) , "Mobile Cloud Computing Security Considerations".

[10] JASLEEN., "Security Issues In Mobile Cloud Computing" , International Journal of Computer Science & Engineering Technology.

[11] Rohit Bhadauria, Sugata Sanyal," Survey on Security Issues in Cloud Computing an Associated Mitigation Techniques".

[12] 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.

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

[14] 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 Tsinghai Science and Technology,2011,pp. 520–528.

[15] 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 Compute Communications Workshops, INFOCOM WKSHPS, Shanghai, China, Apr. 2011.

[16] Wang, S .and S. Wang X.," In-device spatial cloaking for mobile user privacy assisted by the cloud", in Proceeding 11th International Conference on Mobile Data Management, MDM '10, Missouri, USA, May 2010.

[17] 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.

[18] Eric Y. Chen Mistutaka Itoh, " Virtual Smartphone over IP" Copyright © 2010 IEEE.

[19] Lakshmi Subramanian, Gerald Q. Maguire Jr., Philipp Stephanow, "An Architecture To Provide Cloud Based Security Services For Smartphones."

[20] Dijiang Huang, Zhibin Zhou, Le Xu, Tianyi Xing, Yunji Zhong, "Secure Data Processing Framework for Mobile Cloud Computing" IEEE INFOCOM 2011 Workshop on Cloud Computing.

