Secure Data Storage in Mobile Cloud Computing

Preeti Garg, Dr. Vineet Sharma

Abstract—In cloud computing highly scalable computing resources are supplied as an outer service through internet on pay-as-usability basis. Portio research [1] estimates that mobile subscribers will reach 6.5 billion by the end of 2012, 6.9 billion by the end of 2013. Due to increasing use of mobile devices the requirement of cloud computing in mobile devices arise, which gave birth to Mobile Cloud Computing (MCC). Mobile Cloud Computing refers to an infrastructure where data processing and storage can happen away from mobile device. Mobile devices do not need to have large storage capacity and powerful CPU speed. Due to storing data on cloud there is an issue of data security. Because of the risk associated with data storage many IT professionals are not showing their interest towards Mobile Cloud Computing. This paper explores: (i) The concept of Mobile Cloud Computing and issues associated in it (ii) Security of data stored in cloud with various mechanisms (iii) Proposed a possible solution to provide confidentiality, access control as well as integrity of data.

Index terms— cloud, cloud computing**,** data storage, mobile cloud computing, mobile device, mobile user, security.

1 INTRODUCTION

TODAY, the market of mobile phones is growing at a very high speed. Everyone has a mobile phone which provides the facility to move anywhere and access the data anytime. With the emergence of Cloud computing in mobile web, mobile users can use infrastructure, platform, software provided by cloud providers on on-demand basis. Emergence of Cloud Computing with mobile devices gave birth to Mobile Cloud Computing.

1.1 Cloud computing

Cloud computing is an emerging technology in the field of information technology. Cloud Computing is the use of computing resources (hardware and software) that are delivered as a service over a network like internet. More or less Cloud computing describes highly scalable computing resources supplied as an outer service through internet on pay-as-usability basis.

The name of cloud computing comes from the cloud shaped symbol which is used to illustrate a remote resource connected via the web. Cloud computing can be explained as: In case of electricity users can simply use it. They do not need to worry where the electricity is from, how it is generated, or transported. At the end of the month, they will get a bill for the amount of electricity they consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Main call for Cloud computing is that user only utilizes what they required and only pay for what they really use.

- *Preeti Garg is currently pursuing masters degree program in computer science engineering from K.I.E.T. Ghaziabad, India. E-mail: preeti.itgarg@gmail.com*
- *Dr. Vineet Sharma is currently professor in Deptt. of CSE K.I.E.T Ghaziabad, India. E-mail:drvineetsharma.cse@gmail.com*

1.2 Mobile Cloud Computing

Mobile Cloud Computing is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access [2].

Aepona [3] describes MCC as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds.

The mobile devices do not need a powerful configuration (e.g., CPU speed capacity) because all the complicated computing modules can be processed in the clouds. There are many limitations in mobile devices like limited processing power, low storage, less security, unpredictable Internet connectivity, and less energy. To augment the capability, capacity and battery time of the mobile devices, computationally intensive and storage demanding jobs should be moved to cloud.

1.3 Issues with Mobile Cloud Computing

Cloud is extremely powerful to perform computations while computing ability of mobile devices has a limit so many issues occur to show how to balance the differences between these two. So there are some issues in implementing cloud computing for mobile. These issues can be related to limited resources, related to network, related to security of mobile users and clouds [4]. Some issues are explained as follows:

1.3.1 Limited Resources

Having limited resources in mobile device make use of cloud computing in mobile devices difficult. Basic limitations related to limited resources are limited computing power, limited battery and low quality display.

1.3.2 Network related issues

All processing in MCC is performed on the network. So there are some issues related to the network like Bandwidth, latency, availability and heterogeneity.

1.3.3 Security

Most of mobile devices have almost same functionalities like a desktop computer. So mobile devices also have to face a number of problems related to security and privacy. To overcome this problem threat detection services are now performed at clouds but this also has to face a lot of challenges. Some security issues are like device security, privacy of mobile user and securing data on cloud etc. There are so many security threats like viruses, hacking, Trojan horses in mobile devices also. The use of global positioning system (GPS) in mobile devices gives birth to the privacy issues.

2. Security in Mobile Cloud Computing

2.1 Security framework in Mobile Cloud Computing

Mobile cloud computing is growing day by day due to the popularity of cloud computing and increasing uses of mobile devices. Many researchers are showing their interest towards this technology. There are many issues in mobile cloud computing due to many limitations of mobile devices like low battery power, limited storage spaces, bandwidth etc. Security is the main concern in mobile cloud computing. Security in mobile cloud computing can be explained by broadly classifying it into 2 frameworks [5].

2.1.1 Security of data/files

The main issue in using mobile cloud computing is securing the data of mobile user stored on mobile cloud. The data/file of a mobile user is very sensitive; any unauthorized person can do changes in it, to harm the data. So the main concern of cloud service provider is to provide the security of data/files created and manipulated on a mobile device or cloud server. The data/file security is very essential for owner of the data/file as it can contain any confidential information of his.

2.1.2 Security of mobile applications or application models

Securing the mobile applications or application model is also important because these provide better services to mobile users by utilizing cloud resources. These mobile application models use the services of the cloud to increase the capability of a mobile device.

In this paper we are going to discuss the security of data or files of mobile users stored on mobile cloud.

2.2 Why data storage security is needed

The data of owner is stored on the cloud server; once the data is stored the owner does not have that data on his own device. Thus, there is risk related to data security and confidentiality of the data. It is not accepted by the owner that his data/file is disclosed to someone who is not an authorized person. Before discussing why data security is needed there is a need to discuss the security threats to the data stored on the cloud. There are following security risk related to data stored on the cloud server.

These attacks affect the data stored on the cloud. For owner the integrity of the data is very important. If any unauthorized person performs changes in data of other person then it can harm the integrity of the data. Any person after finding confidential information of other person can harm that person. So, data confidentiality is also a concern of data owner. Authentication of user is also important to verify who the originator of the file is.

TABLE 1
DIFFERENT SECURITY THREATS

Name of the Attack	Description
Information disclosure	The secure information of owner is disclosed to any unauthorized user.
Tampering	When any unauthorized person does some changes in other user's data.
Repudiation	When a person refused after sending a message that he did not send it.
Viruses and worms	These are very known attacks. These are the codes whish degrade the performance of any application.
Identity Spoofing	In this attack a person impersonate as someone who is the owner of the data.

3. Data Storage Security with Various Available Solutions

For the last few years Mobile Cloud Computing has been an active research field, as mobile cloud computing is in initial stage, limited surveys are available in various domain of MCC. In this paper our main focus is on securing the data storage in mobile cloud computing. Significant efforts have been devoted in research organizations to build secure mobile cloud computing. This paper explores the various methodologies for data security in Mobile Cloud Computing.

Itani et Al. [6] proposed an Energy efficient framework for integrity verification of storage services using incremental cryptography and trusted computing. In this paper the authors provided a framework for mobile devices to provide data integrity for data stored in cloud server. Incremental cryptography has a property that when this algorithm is applied to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than to re-compute it from scratch. In this system design three main entities are involved:

Mobile User (MU): Mobile user/client is a person who utilizes the storage services provided by Cloud service provider (CSP).

Cloud Service Provider (CSP): CSP provides storage services to client. CSP is also responsible for operating, managing and allocating cloud resources efficiently.

Trusted Third Party (TTP): TTP installs coprocessors on remote cloud; who is associated with a number of registered mobile user/client. Coprocessor provides secret

key (SEK) to mobile user and is also responsible for generating message authentication code for mobile client.

There are a number of operations involved in this scheme shown by "Fig. 1":

1) Updating File on the Cloud: Before uploading file on cloud, mobile user is required to generate an incremental Message Authentication Code (MACfile) using SEK.

$$MACfile = \sum_{k=1}^{n} HMAC(Filek , SEK). \quad (1)$$

Where, n is total logical partitions of file and Filek is kth part of the file.

After generating MACfile, mobile client uploads the file on the cloud and stores MACfile on local storage.

2) Inserting or deleting a block: At any time mobile client can insert (delete) a data block in file stored on cloud server. For this client sends request to CSP, in its response CSP sends requested file to mobile client as well as to trusted coprocessor (TCO) associated with that client. TCO generates MACtco and sends it to client to match this MAC generated by TCO (MACtco) with MAC stored in client's local storage (MACfile). If these two MAC matches , the client can perform insertion/deletion in the file and again computes MACfile with help of old MACfile, SEK and inserted/deleted block. For avoiding communication overhead only updated block is uploaded on cloud server.

3) Integrity Verification: At any time mobile client can verify the integrity of data stored on cloud server by sending request to cloud server, on receiving request cloud server sends file to TCO for integrity verification. TCO generates incremental authentication code and sends it to mobile client directly. Now mobile client compares this MACtco with stored MACfile to verify integrity. If these two matches then integrity is verified.

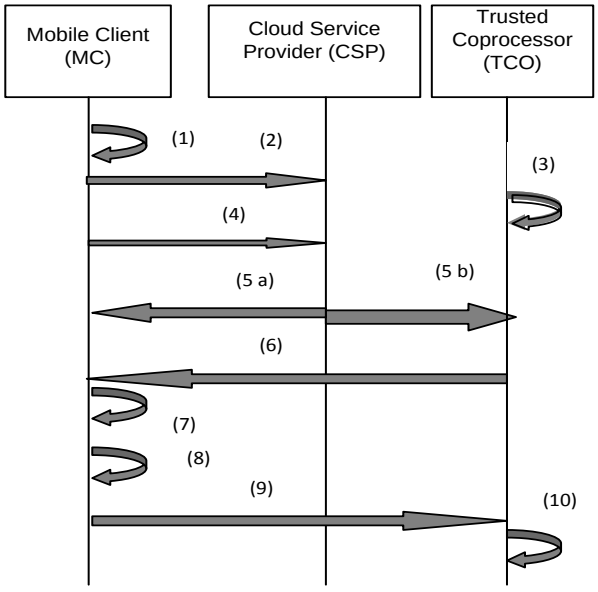

Fig 1: Communication between mobile client, Cloud Service Provider and Trusted Coprocessor [5]

Where,
(1): MC generate MACfile and stores MACfile in local memory
(2): MC uploads file on server
(3): CSP stores file on cloud
(4):MC sends request to CSP for performing insertion/deletion in the file
(5a): CSP sends requested file to MC
(5b): CSP forwards requested file to TCO
(6): TCO sends MACtco to MC directly
(7): MC compares MACfile and MACtco for verifying integrity
(8): MC insert/delete a block in file and computes MAC for that block
(9): MC uploads updated block on cloud
(10): CSP stores updated file.

Jia et al. [7] provide a secure data service mechanism through Identity based proxy re-encryption. This mechanism provides confidentiality and fine grained access control for data stored in cloud by outsourcing data security management to mobile cloud in trusted way. The goal of this protocol is that only authorized persons/sharer can access the data while unauthorized sharer will learn nothing. Identity based encryption is that user encrypt the data through his identity (Id). This encryption scheme is based on bilinear pairing.

A bilinear map is e: G1 × G2 →GT where G1 and GT be cyclic multiplicative group with prime order q and g be generator of G1, having the properties of bilinearity, non degeneracy and computability. Proxy based re-encryption is used by mobile user to provide access control capability to cloud, which could grant access to an authorized users by transferring cipher text encrypted by data owner's identity to one with sharer's identity.

In this mechanism 3 entities are involved: Data owner (DO), Data Sharer (DS) and Cloud Servers (CSs). Both DO and DS utilize data storage service to store and retrieve file. CSs provide services to mobile clients.

This protocol has following phases:

1) Setup Phase: Here system master key(SEK) and system parameters are generated, where SEK is private to data owner.

2) Key Generation Phase: In this phase decryption key corresponding to user's identity (dkid) is generated by following equation: dkid=H1(Id)s where, Id∈ {0,1}* , H1: {0,1}*→ G1 and s∈Zq is randomly selected.

3) Encryption Phase: Here file F is divided into k blocks such that F=(n1,n2……..nk), for each block ni data owner performs encryption by:

$$Ni=(gr,n,e(gs,H1(ID)r)) \quad (2)$$

where, r∈Zp is randomly selected.

After implementing encryption of F, mobile user uploads encrypted file (EF)=(N1,N2……Nk) to cloud.

4) Re-encryption Key Generation: On basis of SEKid generated in second phase and identity of Sharer (IDB), re-encryption key of sharer (REK) is generated.
REK=(H1(IDA)-s, IBEIDB(X)). (3)
where, X is randomly selected from GT and IBE is Identity based encryption.
5) Re-encryption phase: Re-encryption key is send to cloud for re-encryption phase. Here re-encryption cipher text C= (C1,C2,C3)=(gr,m.e(gr,H2(X)),IBEIDB(X))
6) De-encryption phase: Sharer request cloud server for re-encrypted file, cloud checks the re-encrypted key to sharer. If key existed, cloud server sends corresponding file to sharer. Now, sharer can decrypt the file without involvement of data owner. Where ni=$\frac{c2}{e(c1,H2(X))}$ By doing so sharer gets the entire file F=(n1,n2……nk).
7) Policy Updating: Mobile user may want to update the list of sharers, so he can update the list without retrieving and decrypting cipher text from cloud.

Yang et al. [8] provides provable data possession scheme of resource constrained mobile devices by using Diffie-Hellman key exchange, Bilinear mapping and Merkle Hash Tree (MHT). Provable Data Possession (PDP) scheme ensures confidentiality, privacy and integrity of mobile user's data stored on cloud. Diffie-Hellman key exchange is used to securely distribute symmetric key. A bilinear map is e: G1 × G2→GT where G1 and GT be cyclic multiplicative group with prime order q and g be generator of G1. Merkle Hash Tree (MHT) is constructed as binary tree where leaves in MHT are the hash value of authentic data. Verifier only needs to verify the root of the tree. There are 3 participants involved in this scheme:

Mobile end user/client: Mobile user has Trusted Platform Model (TPM) chip in mobile device to produce and store secret key. Mobile end user uses the services provided by cloud.

Trusted Party Auditor (TPA): TPA performs all encryption/decryption on behalf of mobile user.

Cloud Storage Service Provider (CSP): CSP provides storage services to client and also provide proof of data possession by any number of times whenever needed.

PDP schemes includes following phases:
1) Set-Up phase: It is assumed in this scheme that end user has already completed remote identification with TPA. In this phase firstly Diffie-Hellman scheme is used to exchange key between client and TPA.
Client to TPA: g, gα. TPA to Client: gβ .

Now client and TPA shares a symmetric key gαβ. Client encrypt the file with this key and sends it to TPA. TPA generates a combination of symmetric key (ek,dk) for encryption and decryption respectively. Now TPA encrypt file F under ek and calculate the hash value of root of MHT (H(R)). TPA sends H(R) and dk to client encrypted with shared key gαβ. Client signs H(R) with private key (SK) to get Sigsk(H(R))=(H(R))α and sends it to TPA. TPA sends { Sigsk(H(R)), F',φ} to CSP. Here, F'={mi}, φ={σi}={H(mi) umiβ where 1 ≤i≤ N , u is randomly chosen from G1 and mi is ith chunk of file.
2) Integrity Verification: A client or TPA may send a challenge to CSP for integrity verification. According to challenge (chal) CSP performs verification and sends it back to TPA, TPA after verifying proof sends result to client. In this phase TPA sends server a challenge chal={i,vi}, where 1 ≤i≤ *c*, c is random number in the set {1,N} to constitute sequence subset I for each i∈ I, vi∈ Zp is randomly selected. After receiving chal CSP perform verification by generating proof={μ, ω,[H(mi), Ωi],Sigsk(H(R))}, where Ωi is additional information used for rebuilding the root H(R) of MHT.
μ=$\sum_{i=1}^{c}$ vi mi ∈Zp and ω= $\prod_{i=0}^{c}$ σivi ∈Gi are computed by CSP as part of proof.
After receiving proof TPA performs verification by testing these two equations:

$$E(Sigsk(H(R)),g) \stackrel{?}{=} e(H(R),g\alpha) \text{ and} \quad (4)$$

$$e(\omega, g\alpha) \stackrel{?}{=} e(\Pi(H(mi)vi)\ u\mu, g\alpha\beta) \quad (5)$$

If these two equations are equal then it will return true; otherwise false and result is sends back to client.
3) File retrieval: For retrieving a file client and TPA needs to negotiate a symmetric session key ks through Diffie-Hellman. Client sends request for file F to TPA along with decryption key dk encrypted by ks. Now TPA request for file F to CSP;CSP send the file to TPA. Then TPA decrypt the encrypted file F under decryption key dk and sends the file F to end user through secure communication channel.

Zhou et Al. [9] proposed a scheme for efficient and secure data storage operations by introducing the concepts of Privacy Preserving Cipher text Policy Attribute Based Encryption (PP-CP-ABE) and Attribute Based Data Storage (ABDS) system. Through PP-CP-ABE lightweight devices can securely outsource encryption/decryption operations to Cloud Service Provider (CSP). The entities involved in this scheme are:

Data Owner (DO): A DO can be a wireless mobile device or a sensor which uses the storage service of cloud.

Trust Authority (TA): TA is responsible for distributing cryptographic keys and is very trusted.

Encryption Service Provider (ESP): ESP encrypts the file of data owner without knowing the actual encryption key. In this scheme encryption operations are offloaded to ESP.

Decryption Service Provider (DSP): DSP provides decryption service to data owner. DSP does not have any information about actual content.

Storage Service Provider (SSP): SSP provides storage services to clients; before uploading file on cloud, file is encrypted by ESP.

The system model of this scheme is shown in "Fig. 2".

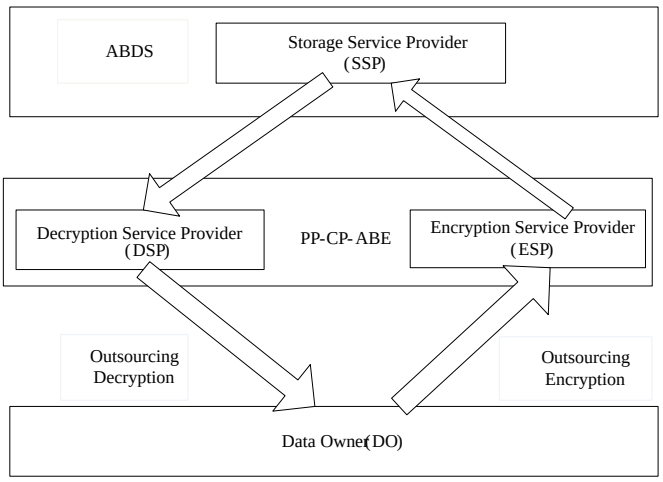

Fig. 2: System architecture

In this scheme following phases are involved:

1) Setup and Key Generation Phase: Trusted authority first chooses bilinear map e: G0× G0→G1 of prime order p having generator g for setting up PP-CP-ABE. Public parameters are:

PK={ G0, g, h=gβ, f=g1/β, e(g , g)α}.

Where, α, β are randomly selected α, β∈ Zp. Master Key MK = (β, gα) is only known to TA. Every user is required to register to TA, who authenticates user's attributes and generate private key for user by using a set of attributes S assigned to user as input. An attribute can be any descriptive string, which defines, classifies or annotates the user, to which it is assigned. Private Key (SK) is generated by following equation:

SK = { D = g(α+r)/β ; $\forall$ j∈S : Dj=gr × H(j)ri; D′j=grj}.

Where, r∈ZP and rj∈ZP are randomly selected for each attribute j ∈S. TA sends SK to Data Owner through a secure channel.

2) Encryption Phase: DO defined a policy tree T=TESP ^ TDO to outsource encryption where, ^ is logical AND operator and TESP , TDO are two subtrees. TESP is data access policy by ESP and TDO is data access policy controlled by DO. TDO is small in size, it can be a subtree with just one attribute. If TDO has 1 attribute then DO may specify an 1-degree polynomial qR(x) and sets s= qR(0), s1= qR(1) and s2= qR(2). DO sends {s1,TESP} to ESP.

Now, ESP generates cipher text:

CTESP = { $\forall$ y∈YESP : Cy = gqy(0), C′y= H(att(y))qy(0)}.

Where, YESP is set of leaf nodes in TESP.

$\forall$x ∈ TESP, a polynomial of degree dx = kx-1 is randomly chooses where kx is secret sharing threshold and qx(0)=qparent(x)(index(x)).

At the meantime, DO computes CTDO = {$\forall$ y∈Y2 : Cy = gqy(0), C′y= H(att(y))qy(0)} , Ĉ = M e(g , g)αs and C = hs, where M is the message. DO sends {CTDO , C , Ĉ } to ESP. After receiving message from DO, ESP generates Cipher Text CT={T = TESP ^ TDO; Ĉ = M e(g , g)αs; C = hs ; $\forall$ y ∈ YESP U YDO : Cy = gqy(0), C′y= H(att(y))qy(0)} and sends CT to SSP.

3) Decryption Phase: DO first blind its private key as

SKblind = { Dt =gt(α+r)/β,∀ j∈S : Dj = gr . H(j)rj,D′j=grj }.

where, t∈ZP and Dt = gt(α+r) /β. DO first checks whether its attributes satisfy the access policy tree, if yes then DO sends SKblind to DSP and request to SSP for the encrypted file.

Now, SSP sends CT′ = { T; C = hs ; $\forall$ y ∈ Y1 U Y2 : Cy = gqy(0), Cy′ = H(att(y))qy(0)} where, CT′ is subset of CT.

After receiving SKblind and CT′; DSP performs decryption on the encrypted file and sends it to DO. Now, DO recover the actual message M.

4. PROPOSED SCHEME

The mechanism provided by Zhinbin Zhou and Dijiang Huang works for data confidentiality and access control but could not work well for data integrity, which is also an important security requirement in the cloud. W. Itani, A. Kayssi, A. Chehab provided their mechanism which works for data integrity and is an accepted mechanism. So, our proposed scheme incorporates these two mechanism for providing confidentiality, access control as well as integrity to data. In this proposed scheme Trusted Authority (TA); who provides key to Data Owner (DO), generates an incremental message authentication code (MAC) of the file; provided by DO. Now, when DO request Storage Service Provider (SSP) for a file then after performing access policy, encrypted file is send to Decryption Service Provider (DSP). DSP sends this file to DO as well as to trusted authority. Now TP again generates MAC of this received file and check it for equality with previous MAC stored. If these two MACs are same then integrity of file is verified and result is transferred to DO.

5 CONCLUSION

The concept of cloud computing provides a great opportunity to users to utilize their services by on-demand basis. The requirement of mobility in cloud computing gave birth to Mobile cloud computing. MCC provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will going to use cloud computing on their mobile devices.

There are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In Mobile Cloud Computing data of owner is stored on the cloud, which is not secured.

This paper has provided the description about the basics of Mobile Cloud Computing and issues associated with it. Mainly it discussed about security of data stored in cloud and importance of data security. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality, access control as well as integrity to mobile users.

In future the work can be done on the proposed scheme for providing data confidentiality with data integrity so that Mobile Cloud Computing will be widely accepted.

ACKNOWLEDGMENT

This paper is made possible through the support and institutional facilities provided by the Department of Computer Science & Engineering KIET, Ghaziabad. We convey our sincere thanks to other M.Tech scholars for their rigorous brainstorming sessions to shape up this research paper.

REFERENCES

[1] Portio Research,"Mobile subscribers worldwide," http://www.onbile.com/info/mobile-subscribers-worldwide.

[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wirel. Commun. Mob. Comput. ,2011.

[3] White Paper, Mobile Cloud Computing Solution Brief. AEPONA, 2010.

[4] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Accepted in Wireless Communications and Mobile Computing - Wiley.

[5] Abdul Nasir Khan, M.L. Mat Kiah , Samee U. Khan, Sajjad A. Madani , "Towards secure mobile cloud computing: A survey," Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.08.003, in press.

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

[7] W. Jia, 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.

[8] J. Yang, H. Wang, J. Wang, C. Tan, D. Yu1, "Provable data possession of resource constrained mobile devices in cloud computing," Journal of Networks 6 (7) (2011) 1033–1040.

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

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

[11] W. Ren, L. Yu, R. Gao, F. Xiong, "Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing," Journal of Tsinghua Science and Technology 16 (5) (2011) 520–528.

[12] Niroshinie Fernando, Seng W. Loke , Wenny Rahayu, "Mobile cloud computing: A survey," Future Generation Computer Systems 29 (2013) 84–106.

[13] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review," Journal of Emerging Trends in Computing and Information Sciences, 2012.

[14] C. Doukas, T. Pliakas, and I. Maglogiannis, " Mobile Healthcare Information Management unitizing Cloud Computing and Android OS," in Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBC), pp. 1037 - 1040,October 2010.

[15] K.Govinda, V.Gurunathaprasad, H.Sathishkumar, "Third Party Auditing For Secure Data Storage In Cloud Through Digital Signature Using Rsa " in International Journal Of Advanced Scientific And Technical Research (ISSUE 2, VOLUME 4- August 2012).

[16] P. Cox, "Mobile Cloud Computing: Devices, Trends, Issues, and the Enabling Technologies" in IBM developer Works, March 2011.

[17] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Symp. Research in Computer Security (ESORICS '09), pp. 355-370, 2009