This full-text paper was peer-reviewed and accepted to be presented at the IEEE ICCSP 2015 conference

Addressing Mobile Cloud Computing Security Issues: A Survey

Pallavi Kulkarni and Rajashri Khanai, *Member*, *IEEE*

***Abstract*—The cloud heralds a new era of computing where application services are provided through the Internet. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. The computing capability of mobile systems is enhanced by Cloud computing. Mobile devices can rely on cloud computing and information storage resource, to perform computationally intensive operations such as searching, data mining, and multimedia processing. Along with traditional computation services it provides, mobile cloud also enhances the operation of traditional ad hoc network by treating mobile devices as service nodes, e.g., sensing services. The sensed information, such as location coordinates, health related information, should be processed and stored in a secure fashion to protect user's privacy in the cloud.**

While the economic ease for cloud computing is compelling, the security challenges it poses are equally striking. The security threats have become obstacles in the rapid adaptability of the mobile cloud computing paradigm. Significant efforts have been devoted in research organizations and academia to build secure mobile cloud computing environments and infrastructures. In spite of the efforts, there are a number of loopholes and challenges that still exist in the security policies of mobile cloud computing. We discuss these issues here, identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

***Index Terms* — Mobile Computing (MC), Mobile Cloud Computing (MCC), Mobile Cloud Security.**

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 [1] – [2]. 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 [3] – [4].

Furthermore, consider applications that require extensive processing – image processing for video games, speech synthesis, natural language processing, augmented reality, wearable computing—all these demand high computational capacities thus restricting the developers in implementing applications for mobile phones. Considering the trends in mobile phone architecture and battery, it is unlikely that these problems will be solved in the future. This is, in fact, not merely a temporary technological deficiency but intrinsic to mobility [5] and a barrier that needs to be overcome in order to realize the full potential of mobile computing.

In recent years, researchers addressed this problem through cloud computing. Cloud computing can be defined as the aggregation of computing as a utility and software as a service [6]where the applications are delivered as services over the Internet and the hardware and systems software in data centers provide those services [7]. Also called 'on demand computing', 'utility computing' or 'pay as you go computing', the concept behind cloud computing is to offload computation to remote resource providers.

The concept of offloading data and computation in cloud computing is used to address the inherent problems in mobile computing by using resource providers other than the mobile device itself to host the execution of mobile applications. Such an infrastructure where data storage and processing could happen outside the mobile device could be termed a 'mobile cloud'. By exploiting the computing and storage capabilities of the mobile cloud, computer intensive applications can be executed on low resource mobile devices [8] – [10].

It is important to ensure secure and reliable data/ multimedia data transmissions between mobile users and the media cloud. Since the data can be transferred and stored in a cloud system through wireless, it becomes vulnerable to unauthorized disclosures, modifications, and replay attacks. A critical question must be answered when the mobile clients upload their data or multimedia to the cloud: Can users trust the cloud?

The remainder of this paper is organized as follows: Section II describes the mobile cloud computing architecture. Section III explains the technical challenges posed by MCC. Section IV briefs about the approaches used. Section V provides survey of existing security frameworks for MCC. Finally future work and conclusion are identified in section VI and VII.

Pallavi Kulkarni is with the DSATM Bangalore, KA, India (e-mail: pallavik15@ gmail.com).

Rajashri Khanai is with JCE Belgaum, KA, India (e-mail: rajashri.khanai@gmail. com).

978-1-4799-8081-9/15/$31.00 © 2015 IEEE

II. MOBILE CLOUD COMPUTING ARCHITECTURE

The Mobile Cloud Computing architecture is shown in the Fig. 1.The main architecture is composed from the components: mobile users, mobile operators, internet service providers (ISP), and cloud service providers [11], respectively.

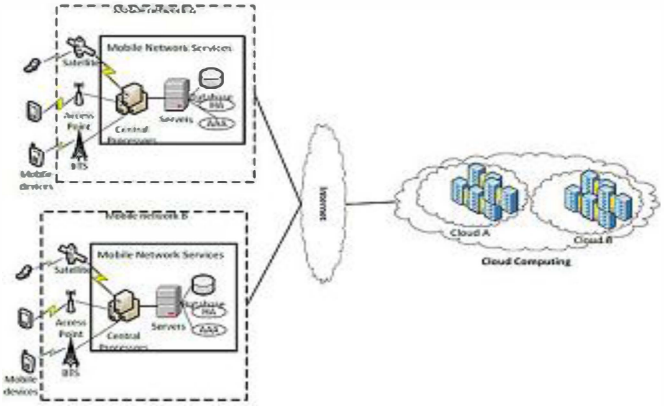

Fig. 1. MCC Architecture

To have an in depth understanding of Mobile Cloud Computing (MCC), it is necessary to get a complete grasp on cloud computing. Cloud computing provides a new computing paradigm that delivers IT as a service. Cloud computing permits customers to utilize cloud services on the fly in pay-as-you-go manner [12, 13] through the Internet. There are various layered architectures available for cloud computing to provide the aforementioned services as a utility [14-15]. One such cloud computing layered architecture is presented in Fig. 2.

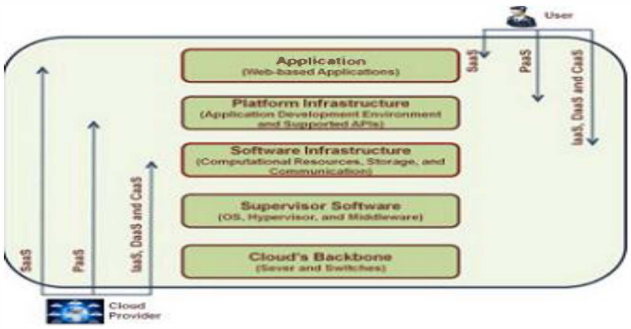

Fig 2. Layered architecture of cloud computing

Cloud's backbone layer consists of physical servers and switches [2]. The cloud service provider is responsible to run, manage and upgrade cloud hardware resources according to the requirements of users. The backbone layer is also responsible to allocate hardware resources to users in an efficient, quick, and smooth way. The supervisor software layer contains the system software to manage the cloud hardware resources. The system software permits application software to run and utilize underlying resources in an efficient way. The operating system manages the computer hardware resources and provides an interface for interaction of user and application software with hardware resources. The hypervisor is system software that allows users to remotely create virtual machines on cloud server(s) at runtime. The virtual machine has user defined hardware specifications and a software stack. The virtualization process improves the availability of the user's hosted services even in case of hardware failure. The virtual machine with the entire software stack can be migrated to another server with negligible unavailability of hosted services. The middleware system software manages the transparent execution and interaction among jobs running on cloud servers. The software infrastructure layer hands over the network resources to upper layers and provides a foundation for a new computing paradigm that delivers IT as a service.

For efficient utilization of resources, multiple virtual machines may be created on each server according to users' demand. The platform infrastructure layer provides an application development platform and a set of Application Programming Interfaces (APIs) for the developers [16].

The developers use APIs to program applications that can interact and utilize the full power of the cloud resources. The topmost application layer allows users to access and use applications installed on a cloud provider's data center through the Internet.

III. SECURITY IDENTIFICATION OF THREATS

To secure an Information System (IS) one has to identify unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Due to its architectural design and characteristics, cloud computing imposes a number of security benefits, which include data and process segmentation, centralization of security, redundancy and high availability. There are numerous challenges existing in the field of MCC, including data replication, consistency, limited scalability, unreliability, unreliable availability of cloud resources, portability, trust, security and privacy [17].

Security in general, is related to the important aspects of confidentiality, integrity and availability; they thus become building blocks to be used in designing secure systems. These important aspects of security, apply to the three broad categories of assets which are necessary to be secured - data, software and hardware resources.

A.Confidentiality and Privacy refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, that leads to an increase in the number of points of access. Delegating data control to the cloud, inversely leads to an increase in the risk of data compromise, as the data becomes accessible to an augmented number of parties.

B. Multitenancy refers to the cloud characteristic of resource sharing. Several aspects of the IS are shared including, memory, programs, networks and data. Although users are isolated at a virtual level, hardware is not separated.

C. Object reusability is an important characteristic of cloud infrastructures, but reusable objects must be carefully controlled lest they create a serious vulnerability.

D. Data remanence is the residual representation of data that have been in some way nominally erased or removed. Data confidentiality could be breached unintentionally, due to data remanence.

E. Integrity A key aspect of Information Security is integrity. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and

hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication.

F. Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. Due to the increased number of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.

G. Availability refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system must have the ability to continue operations even in the possibility of a security breach.

IV. SECURITY THREAT COUNTER MEASURES

As MCC is based on cloud computing, all the security issues are inherited in MCC with the extra limitation of resource constraint mobile devices. There is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. Fig. 3 shows the different security services that may run on different layers to provide a secure MCC environment. The security and privacy protection services can be achieved with the help of secure cloud application services. In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users. 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.

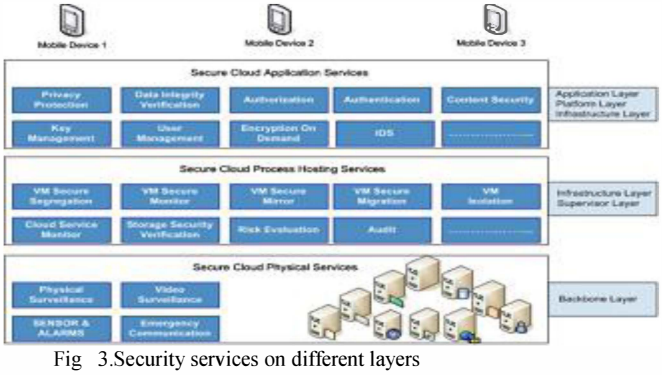

Fig 3.Security services on different layers

V. SURVEY OF EXISTING SECURITY FRAMEWORKS FOR MCC

In this section, we present countermeasure solutions that have been proposed in the scientific journals and conferences pertaining to securing MCC.

A. Paper-1 Cloud computing for mobile users: can offloading computation save energy?

Some types of data cannot be stored in the cloud without considering the privacy and security implications. One possible solution is to encrypt data before storage given in [4]. However, encryption alone will not solve the problem. In one of the scenarios, the data remain encrypted at the cloud storage site. This can prevent unauthorized access even when the storage is breached in the cloud; the cloud vendor cannot access the data either.

In another scenario, the cloud vendor decrypts data to perform operations on that data. For example, in the case of a document, the cloud vendor must know which words are used to check spelling; for a spreadsheet, the cloud application must know the numbers for calculation. This is the general case for cloud services.

Another possible privacy and security solution is to use a technique called steganography. Steganographic techniques can be used to transform the data so that operations can be performed without exposing them.

B. Paper-2 Addressing Cloud Computing Security Issues.

In this paper [3], the authors claim that employing Trusted Third Party services within the cloud, leads to the establishment of the necessary Trust level and provides ideal solutions to preserve the confidentiality, integrity and authenticity of data and communications. In cryptography, a Trusted Third Party (TTP) is an entity which facilitates secure interactions between two parties who both trust this third party. The scope of a TTP within an Information System is to provide end-to-end security services, which are scalable, based on standards and useful across different domains, geographical areas and specialization sectors.

C. Paper-3 Energy efficient framework for integrity verification of storage services in MCC.

Itani et al. [18, 19] proposed an energy efficient framework for mobile devices to ensure the integrity of the mobile users' files/data stored on the cloud server using the concept of incremental cryptography and trusted computing [20,21].

The system design contains three main entities: (a) mobile client, (b) cloud service provider, and (c) trusted third party. The mobile client utilizes the storage services provided by the cloud service provider. The cloud service provider is responsible for managing, operating, and allocating the cloud resources efficiently. The trusted third party is responsible for configuring and installing the tamperproof coprocessors on the remote cloud. Each coprocessor is associated with multiple registered mobile clients. The coprocessor distributes Secret Key (SK) with associated mobile clients and generates a message authentication code on behalf of mobile clients.

D. Paper-4 A framework for secure data service in MCC.

Jia et al. [22] proposed a secure data service that outsources data and security management to cloud in trusted mode. The secure data service allows mobile users to move data and data sharing overhead to cloud without disclosing any information. There are three main entities involved in the proposed network model: (a) data sharer, (b) data owner, and (c) cloud service provider. The data owner shares files and grants access privileges to the data sharer. The data owner and data sharer both utilize the cloud storage service to store and retrieve files. The proxy re-encryption [22] and identity base encryption [23] schemes are used to achieve the secure data service. In the proxy re-encryption scheme, a semi trusted proxy transforms ciphertext encrypted with A's public key into another ciphertext encrypted with B's public key [24]. The identity

based encryption scheme is based on bilinear mapping.

E. Paper-5 A framework for secure storage services in MCC. Hsueh et al. [25] proposed a scheme for smart phones to ensure the security and integrity of mobile users' files stored on cloud server(s).

The authors also introduced an authentication mechanism to authenticate the owner of the uploaded file on cloud. The proposed framework consists of four modules: (a) mobile device, (b) cloud service provider, (c) certification authority, and (d) Telecommunication module. Mobile device utilizes cloud services. The certification authority is responsible for authentication of mobile devices. The telecommunication module generates and keeps track of mobile devices' passwords and related information to use cloud services.

F. Paper-6 A security framework for efficient and secure data storage services in MCC.

Zhou and Huang [26] proposed a privacy preserving framework called Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) for lightweight mobile devices. The proposed scheme offloads the processing and storage intensive encryption and decryption operations on cloud without revealing any information about data contents and security key. The authors also proposed an attribute based data storage system that provides cryptographic access control to overcome the communication and storage overhead for data management on mobile devices as well as on cloud.

G. Paper-7 Lightweight and compromise resilient storage outsourcing in MCC.

Ren et al. [27] proposed three schemes to ensure the confidentiality and integrity of the users' files stored on cloud. Encryption based scheme (EnS), Coding based scheme (CoS) Sharing based scheme (ShS). The files are assumed to be created and operated only on a mobile device. The files may be stored on single or multiple cloud servers. The authors assume the cloud servers as distrusted nodes, the mobile device as semi-trusted in case of storage, and trusted in case of computation. In each scheme, the mobile device is responsible for encryption, decryption, and integrity verification.

H. Paper-8 A public provable data possession scheme for MCC.

Yang et al. [28] extended the public provable data possession scheme proposed in [29] for a resource constrained mobile device that ensures the privacy, confidentiality, and integrity of mobile users' data stored on cloud. The system model consists of three main entities: (a) mobile end-user, (b) trusted third party, and (c) cloud storage service.

The mobile end-user utilizes the cloud storage and may request data storage validation. Trusted Third Party (TTP) provides encryption, decryption, and authentication services for the mobile end-user to overcome the processing burden. The Cloud Storage Service (CSS) contains an enormous amount of storage for mobile end-users. The CSS is also responsible for providing proof of data possession when requested by TTP or the mobile end-user. The proposed scheme uses Diffie–Hellman key exchange [30], bilinear mapping [31], and Merkle Hash Tree (MHT) [32].

I. Paper-9 Security Protection between Users and the Mobile Media Cloud.

In this article [32, 33], authors propose a scalable authentication approach using watermarking, which could be scalable and adapted to the size of a scaled image from the media cloud. Another research challenge in the article is the reduction of wireless transmission errors, which could corrupt the embedded watermark and fail the process of watermark detections. Furthermore, authors propose using a secret sharing scheme to divide multimedia data into multiple pieces and then uploading them to different clouds. In this situation, even the data pieces in one cloud are disclosed, but all of the information cannot be disclosed due to the nature of secret sharing. The secret image sharing scheme is widely applied in visual cryptography. The comparison study is provided in Table 1.

TABLE I
THE COMPARATIVE STUDY

	Basic theory	Data integrity	Authentication	Scalability
Itani et al. [18]	Incremental message authentication code	Yes	No	Moderate
Jia et al. [22]	Proxy re-encryption (PRE) scheme and identity base encryption (IDE) scheme	No	No	Highly scalable
Hsueh et al. [25]	Standard cryptography functions	Yes	Yes	Moderate
Yang et al. [28]	Diffie–Hellman key exchange, bilinear mapping, and merkle hash tree	Yes	Yes	Moderate
Ren et al. [27] (EnS)	Standard cryptography functions	Yes	Yes	Highly scalable
Ren et al. [27] (ShS)	Exclusive-OR	Yes	Yes	Highly scalable
Zhou and Huang [26]	Bilinear pairing, access policy tree, and secret sharing scheme	No	No	Highly scalable

VI. FUTURE WORK

Designing user-oriented system which allows users to protect their data's security and privacy since the cloud itself may not be trusted as it is managed by third parties such as cloud service providers. We propose to utilize encryption and Steganographic techniques for user data and media data respectively along with secret sharing and watermarking to address the challenges. Also exploring the possibility of using neural networks to make the system more robust. The research is open to resist multimedia transmission errors through error correcting codes.

VII. CONCLUSION

The survey critically investigates different security frameworks proposed for the MCC environment. Most of the discussed security frameworks offload processor intensive jobs on cloud due to the resource limitation of mobile devices. Although the offloading increases the processing capability of the mobile device, the mobile user has to pay while using the cloud resources in a pay-as-you go manner.

The most challenging aspects in MCC are guaranteeing user

privacy and the provision of mobile application security that uses cloud resources. To provide a secure MCC environment, service providers need to address issues pertaining to data security, network security, data locality, data integrity, data access, authentication, authorization, data confidentiality, data breach issues, and various other factors. To achieve a secure MCC environment, security threats need to be studied and addressed accordingly.

REFERENCES

[1]. Niroshinie Fernando ∗ , Seng W. Loke ∗ , Wenny Rahayu, "Mobile cloud computing: A survey ", Future Generation Computer Systems ,June 2012.

[2]. Abdul Nasir Khana,∗ , M.L. Mat Kiah a, Samee U. Khanb, Sajjad A. Madanic, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, August 2012.

[3]. Dimitrios Zissis ∗ , Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems Volume 28, Issue 3, March 2012, Pages 583–592

[4]. Karthik Kumar,Yung-Hsiang Lu,"Cloud Computing For Mobile Users:Can Offloading Computation Save Energy"IEEE J,Computer Volume:PP , Issue: 99, 18 March 2010.

[5]. M. Satyanarayanan, Mobile computing, Computer 26 (1993) 81–82.

[6]. W. Vogels, A head in the clouds the power of infrastructure as a service,in: Proceedings of the 1st Workshop on Cloud Computing and Applications,CCA'08.

[7]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D Patterson, A. Rabkin, I. Stoica, Above the clouds: a Berkeley view of cloud computing, Technical Report UCB/EECS-2009-28, 2009.

[8]. Khanai, R. ; Dept. of Electr. & Electron. Eng., Gogte Inst. of Technol., Belgaum, India ; Kulkarni, G.H. ; Torse, D.A."AES-TURBO as a single primitive for land mobile satellite channel"Published in Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on 1-2 March 2014 .

[9]. Khanai, R. ; Dept. of Electr. & Electron. Eng., Gogte Inst. of Technol., 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 .

[10]. Rajashri Khanai, G. H. Kulkarni, "Crypto-Coding as DES-Convolution for Land Mobile Satellite Channel", International Journal of Computer Applications © 2014 by IJCA Journal Volume 86 - Number 18 Year of Publication: 2014 .

[11]. Qian (Andy) Wang , Mobile Cloud Computing, A Thesis Submitted to the College of Graduate Studies and Research In Partial Fulfillment of the Requirements, February 2011.

[12]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee,D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the clouds: a Berkeley view of cloud computing, Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb. 2009.

[13]. R. Ranjan, A. Harwood, R. Buyya, Grid federation: an economy based distributed resource management system for large-scale resource coupling, Technical Report GRIDS-TR-2004-10, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, 2004.

[14]. R. Buyya, R. Ranjan, Federated resource management in grid and cloud computing systems, Future Generation Computer Systems 26 (8) (2006) 1189–1191.

[15]. B. Sotomayor, R.S. Montero, I.M. Lorente, I. Foster, Virtual infrastructure management in private and hybrid clouds, IEEE Internet Computing 13 (5) (2009) 14–22.

[16]. L. Wang, J. Tao, M. Kunze, H. Von, D. Kramer, W. Karl, Scientific cloud computing: early definition and experience, in: Proc. 10th IEEE Int. Conference on High Performance Computing and Communications, HPCC '08, Dalian, China, Sep. 2008.Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[17]. Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[18]. 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.

[19]. M. Bellare, O. Goldreicha, S. Goldwasser, Incremental cryptography: the case of hashing and signing, in: Proc. 14th Annual Int. Cryptology Conference on Advances in Cryptology, Santa Barbara, California, USA, Aug. 1994.

[20]. M. Bellare, O. Goldreich, S. Goldwasser, Incremental cryptography and application to virus protection, in: Proc. 27th Annual ACM Symposium on Theory of Computing, STOC '95, Las Vegas, NV, USA, May 1995.

[21]. M. Bellare, O. Goldreich, S. Goldwasser, Incremental cryptography and application to virus protection, in: Proc. 27th Annual ACM Symposium on Theory of Computing, STOC '95, Las Vegas, NV, USA, May 1995.

[22]. 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.

[23]. J. Shao, Z. Cao, CCA-secure proxy re-encryption without pairings in public key cryptography, in: Proc. 12th Int. Conference on Practice and Theory in Public Key Cryptography, PKC '09, Irvine, CA, USA, Mar. 2009.

[24]. S. Yu, C. Wang, K. Ren, W. Lou, Achieving secure scalable and fine-grained data access control in cloud computing, in: Proc. IEEE INFOCOM, INFOCOM 10, San Diego, CA,USA, Mar. 2010.

[25]. 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.

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

[27]. 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.

[28]. 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.

[29]. Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in: Proc. 14th European Conference on Research in Computer Security, ESORICS '09, Saint Malo, France, Sep. 2009.

[30]. D.A. Carts, A review of the Diffie–Hellman algorithm and its use in secure internet protocols, November 02, 2011.

[31]. D. Boneh, C. Gentry, Aggregate and verifiably encrypted signatures from bilinear maps, in: Proc. 22nd Int. Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT '03, Warsaw, Poland, May 2003.

[32]. Honggang Wang, Shaoen Wu, Min Chen, Huazhong ,Wei Wang, "Security Protection between Users and the Mobile Media Cloud", IEEE Communications Magazine ,Volume 52,issue 3, March 2014

[33]. R.C. Merkle, Protocols for public key cryptosystems, in: Proc. IEEE Symposium on Security and Privacy, Oakland, California, USA, Apr. 1980.