ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

A Road Map on Security Deliverables for Mobile Cloud Application

D.Pratiba[1], Manjunath A.E[2], Dr.N.K.Srinath[3], Dr.G.Shobha[4] , Dr.Siddaraja[5]

Asst. Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India[1]

Asst. Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India[2]

Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India[3]

Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India[4]

Professor, Department of Computer Science and Engineering, Dr.AIT, Bangalore, India[5]

Abstract: Mobile phones are one of the greatest achievements of mankind. It is gaining its importance in every walk of life, irrespective of any status. At the same time, Mobile Cloud Computing (MCC) is also gaining its popularity among its users. It has brought in a great revolution in itself. In mobile cloud computing, mobile devices can depend on cloud computing and information storage resources to perform computationally intensive operations such as searching, data mining and multimedia processing. Often the mobile users prefer the latest and the best technology which is cost effective and value for money. Mobile cloud storage enables users to remotely store their data and enjoy the on–demand high quality Cloud applications without the burden of local hardware and software environment. In spite of the hype achieved by mobile cloud computing, the growth the mobile cloud computing subscribers is still below expectations. This study is based on existing literature, highlights the current state of the work proposed to secure mobile cloud computing infrastructure.

Keywords: Cloud Computing, Privacy, Mobile Cloud, Data Security.

I. INTRODUCTION

Cloud computing can be termed as a model of information processing, storage, delivery in which clients can request cloud computing resources as and when they require[1]. The organizations need infrastructure physical devices, services, storage or any networking equipments can be requested from the cloud instead of purchasing.

Cloud service providers have outsourced resources on demand basis [1]. Mobile devices have some significant constraints like ubiquitous wireless infrastructure, longer battery life, less storage capability. Cloud computing provides a ground for a new computing rule called Mobile Cloud Computing (MCC). The mobile devices battery powered have limited processing power, low storage, less security, unpredictable internet connectivity and less energy. The limitations of mobile devices mentioned above are obstacles for computationally intensive and storage demanding applications on a mobile. Computationally intensive and storage demanding jobs should be moved to cloud to improve the capability, capacity and enhance battery time of the mobile devices [2][3].

On the basis of the above discussion, mobile cloud computing can be defined as protocol that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resource by providing wireless access. In order to make offloading beneficial for mobile users, care has to be taken before moving jobs on a cloud server by considering the network conditions and communication overhead [4][5].

The architecture of mobile cloud computing is depicted in Fig. 1.

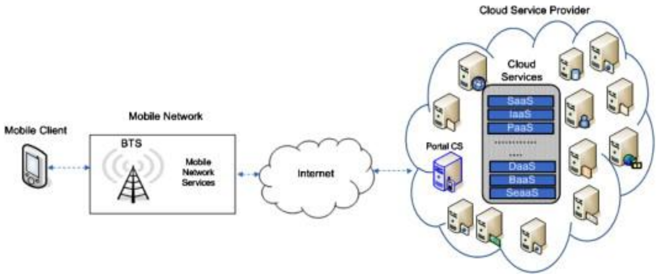

Fig.1. Mobile Cloud Computing architecture

Mobile users communicate with cloud service provider by using mobile applications or by using embedded browser applications.

In order to perform intensive operations like searching, data mining and multimedia processing, mobile devices depend on cloud computing and information storage resource. Users personal data, sensed information and location coordinates and health related information should be processed and stored in a secure manner in order to protect user's privacy in the cloud.

II. SURVEY OF EXISTING SECURITY FRAMEWORKS FOR MOBILE COMPUTING

We present secure framework solutions that have been proposed in the scientific journals and conferences concerning to securing mobile cloud computing in the following section.

A. Energy efficient framework for integrity verification of storage services in mobile cloud computing

Itani et al. [6] proposed an energy efficient framework for mobile devices to ensure the integrity of the mobile user's files/data stored on the cloud server using the methods called incremental cryptography and trusted computing.

The design of the system contains the following three main entities (a)mobile client, (b)cloud service provider, and (c) trusted third party.

Mobile clients utilize cloud resources and service providers provide cloud storage services for mobile users. The responsibility of the cloud service provider are managing, operating and allocating the cloud resources efficiently. Configuration and installing the tamperproof coprocessors are the responsibilities of the trusted third party on the remote cloud.

Multiple registered mobile clients can be associated with each coprocessor and coprocessor distributes secret key (SK) with associated mobile clients and generates a message authentication code for mobile clients. In this framework, authors have discussed about uploading, block insertion, block deletion and integrity verification operations for files in the mobile cloud computing environment.

The mobile client generates an incremental Message Authentication Code ($\mathrm{MAC_f}$) for uploading a file on cloud servers using [6] secret key in equation (1).

$$\mathrm{MAC_f} = \sum_{i=1}^{k} HMAC(Fi, SK) \qquad (1)$$

Where F_i corresponds to the i^{th} part of the file, and $\mathrm{MAC_f}$ represents the sum increment message and k represents total logical partition of the file. The mobile client uploads files on cloud server and stores $\mathrm{MAC_f}$ on local storage.

Mobile clients have the permission to do operations like insert, delete and update operations on uploaded files. Files are transferred to the mobile client as well as to the trusted coprocessor by the cloud servers.

Experimental results of the proposed framework saves processing and energy on the mobile device as compared to conventional techniques. This energy efficient framework moves most of the integrity verification jobs to cloud service providers and to the trusted third party in order to minimize the processing overhead on the mobile users when the mobile user instructs cloud provider to redirect the stored files to the coprocessor. For integrity verification, the coprocessor calculates an incremental MAC on received files.

The proposed framework fails to notice the privacy of uploaded files. Coprocessor in the proposed framework can handle only a specific number of mobile users. If the number of mobile users increases, the proposed framework may result in performance degradation.

B. A framework for secure data service in mobile cloud computing

Jia et al.[7] proposed a secure data service that outsources data and security management to cloud in trusted mode.

The proposed secure data service framework permits mobile users to move data and computing overhead to cloud without disclosing any information. The following are the three entities involved in the proposed framework: (a) data sharer, (b) data owner (c) cloud service provider.

Data owner gives access privileges to data sharers and shares files. Both data owner and data sharer uses cloud storage service to store and retrieve files. In order to achieve secure data service, the proxy re-encryption and identity based encryption are used.

A semi trusted proxy transforms cipher text encrypted with A's public key into another cipher text that is encrypted with B's public key in proxy re-encryption scheme. The proposed secure data service framework provides data privacy and fine grained access with minimum cost of updating access policy and communication. It has removed security management overhead from the mobile users but mobile users have to perform some cryptographic operations before uploading file(s) on cloud.

The cryptographic operations consume more amount of energy. This issue needs to be considered while implementing a secure framework for mobile cloud computing. The cloud is responsible for performing the security management and re-encryption on behalf of the mobile user.

In the proposed framework, the outsourcing of security management and re-encryption increase the amount of utilization of cloud resources. The excessive use of cloud resources results in an overcharge to mobile user. There is a need for strong analysis that shows tradeoff between resources consumption on cloud and energy consumption on mobile device while using the secure data service.

C. A framework for secure storage services in mobile cloud computing

Hsueh et al.[8] proposed a framework for smart phones to maintain the mobile user's files stored on cloud server(s) in a secure manner.

In the proposed secure framework, authors also introduced a mechanism to authenticate the owner of the uploaded file on cloud. The proposed framework consists of following four modules: (a)mobile device, (b)cloud service provider, (c) certification authority, (d) telecommunication module.

Authentication of mobile devices is done by certification authority. The telecommunication module generates and keeps tracks of mobile device passwords and related information to use cloud services. In order to use cloud services, the mobile user has to register with the telecommunication module through certification authority.

The telecommunication module issues a password for mobile users to use cloud resources on successful registration. In the proposed framework, the mobile user encrypts the files using asymmetric encryption techniques. The encrypted files are stored on cloud servers along with mobile user attributes like user name, signature and password. The encrypted files along with user credentials may be stored on a cloud server hosted by adversary. Later adversary can utilize credentials to impersonate the user.

The proposed scheme neglects the processing and storage limitations of the device. The cryptographic encryption and decryption and even hash function on an entire file are performed on mobile device.

D. A security framework for efficient and secure data storage services in mobile cloud computing

Zhou and Huang [9] proposed a security framework called privacy preserving cipher policy Attribute-Based-Encryption (PP-CP-ABE) for lightweight mobile devices. The proposed attribute based data storage system that provides cryptographic access control to overcome the communication and storage overhead for data management on mobile devices and as well as on cloud.

The architecture of the proposed scheme consists of following four components (a) data owner, (b) encryption service provider, (c) decryption service provider, (d) storage service provider. The data owner can be sensor or mobile device that can request to store and retrieve data from cloud. The files of data owner are encrypted by encryption service provider (ESP) without having knowledge about the security keys.

Without getting any information about data contents, the decryption service provider (DSP) decrypts the file for data owner. The trusted authority is responsible for generating and distributing keys among data owners. The PP-CP-ABE is based on bilinear mapping, access policy tree, and secret sharing scheme.

In cipher text policy attribute-based encryption scheme, the cipher text grows linearly with an increase in number of cipher text attributes. The increase in cipher text involves more pairing evaluation and decrypting the cipher text. The problems in the PP-CP-ABE are inherited in cipher text policy attribute-based encryption scheme.

There is a need for better encryption scheme that has a fixed cipher text regardless of cipher text attributes.

E. MobiCloud: Building secure cloud framework for mobile computing and communication.

Huan et al. [10] proposed a new mobile cloud computing framework that improves the functionality of the Mobile Ad-hoc Network (MANET) in terms of risk management, trust management, and secure routing and it also provides conventional computation services. In the proposed framework, the new service oriented model considers each mobile node as a service node.

Depending upon the capability of the node, a service node can provide or consume services. The services can be storage, computation services or sensing services. In order to overcome the uncertainty caused by the mobility, one or more Extended Semi Shadow Images (ESSI) is virtualized on cloud.

The ESSI and mobile clients interact with each other through secure connections like SSL, IPSec etc. In this framework private keys are generated from descriptive terms. This new private keys generation mechanism requires less processing time to manage the security policies. In this model, trust management server module is responsible for user centric identity management through the attribute based identity management scheme.

The attribute based identity management scheme defines Point Of Network Presence (PONP). PONP is a combination of type, value and attributes. The type consists of following components: (a) identity issues, (b) private key issues and (c) validation period. The PONP may have multiple attributes and each attribute is a combination of type and value.

In order to define publicly known native identities for the device, the trust management server module may use multiple attributes. This architecture is useful for mobile Ad-hoc networks for security, risk assessment, location based services, network status monitoring and context aware routing. The MobiCloud architecture has not considered the trustworthiness of the cloud node and mobile users must trust cloud service providers in order to secure their data in cloud.

There should be secure mechanism to store mobile user information on cloud servers in a secure manner.

F. Secure data processing framework for mobile cloud computing

The MobiCloud architecture proposed in[10] did not consider the privacy and security of user's data stored on cloud. Huang et al. [11] proposed a secure data processing model for MobiCloud that provides enhanced security and privacy protection for mobile users with help of multi-tenant secure data management, trust management, and a ESSI data processing model.

The proposed model consists of following three domains: (a) cloud public service and sensing domain, (b) cloud trusted domain, (c) cloud mobile and sensing domain. The copy of each mobile device called ESSI is running under the supervision of the cloud trusted domain. The ESSI not only improves the processing and storage capabilities of the device but also provides enhanced security and privacy protection.

Strict security policies are implemented in the cloud trusted domain through a distributed firewall system for the inspection of incoming and outgoing malicious packets in order to avoid data leakage. The detail of the model is shown in Fig. 3.

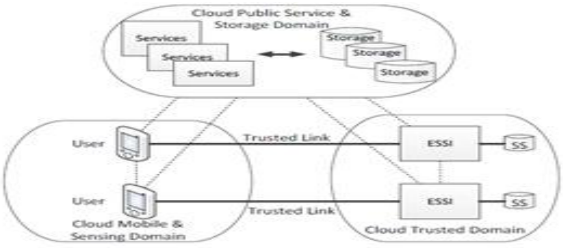

Fig. 3. Reference model for mobile cloud [11].

The proposed multi-tenant data management system divides the data into the following two categories: (a) critical data (b) non critical data or normal data. Critical data is encrypted with a user generated key and normal data is encrypted with a cloud generated key. Incoming data flow received by the ESSI is classified as critical or normal data. If data is found to be critical, the Encryption Decryption and verification (EDV) module is used to encrypt data and store in the secure storage of ESSI. The normal data is stored on cloud through a masking procedure.

The masking procedure removes the private information to preserve anonymity depending on user preference. The presented approach has a number of advantages over the traditional approaches, e.g. Scalability, user critical data is not stored on cloud storage and computation is distributed between ESSI and a mobile device, and no single point of failure.

This proposed framework provides enhanced security and privacy protection for mobile users with the help of multi-tenant secure data management, trust management, and ESSI data processing model. To provide strong security services to user, the storage domain module and cloud trusted domain module are physically isolated if the cloud trusted domain module is hosted by a trusted third party, there is an issue of scalability.

III. CONCLUSION

Based on the investigations made at various levels, some security measures have to be adopted for the protection of mobile cloud computing environment. Most of the discussed security frameworks move processor jobs on cloud due to resource constraints of mobile devices.

Mobile service providers have to address the issues relating to data security, network security, data segregation, data access, authentication, authorization, data locality, data integrity, web application security, data confidentiality, and data breach issues and various other factors. It is also bounded duty of the service providers to meet the required challenges in mobile cloud computing in order to guarantee user privacy and the provision of mobile application security that uses cloud resources.

To achieve a secure mobile cloud computing environment, security threats needs to be studied and addressed accordingly.

IV. REFERENCES

1] Peter Mell and Tim Gracnce, "the NIST Definition of Cloud Computing'. October 7, 2009, version 15, National Institute of Standards and Technology (NIST).

2] E.Y. Chen, M. Ithoh, Virtual smartphone over IP, in: proc. IEE Int. Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM '10 Montreal,QC Canada, June 2010.

3] B.P. Rimal, E. Choi, I. Lumb, A taxonomy and survey of cloud computing systems, in: Proc. 5th Int.Joint Conference of INC, IMS and IDC, NCM '09,Seoul, Korea, NOV.2009.

4] H. Canepa, D. Lee, A virtual cloud computing provider for mobile devices, in:Proc. 1st ACM workshop on Mobile cloud Computing and Services Social Networks and Beyond, MCS'10,San Francisco, USA, June 2010.

5] K. Kumar, Y.H Lu,Cloud computing for mobile users: can offloading computation save energy? IEEE Journal Computer 43 (4) (2010) 51-56.

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, December.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 W KSHPS, Shanghai, China, April .2011.

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

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

10] D. Huan, X, Zhang, M. Kang, J. Luo, MobiCloud: building secure cloud framework for mobile computing and communication, in:Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering,SOSE'10, Nanjing, China, June 2010.

11] D. Huang, Z. Zhou, L. Xu, T. Xing, Y.Zhomg, Secure data processing framework for mobile cloud computing, in:Proc. IEEE INFOCOM Workshop on cloud computing, INFOCOM'11,Shanghai, China, June 2011.