ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2 Issue 11, November 2013

Mobile Data Security on Cloud Computing Using SAAS

Mr. Yogesh Graham[1], Mr Praveen Shende[2]

Abstract— Nowadays a mobile device such as a smart phone is becoming one of the major information processing devices for users. On the other hand, a mobile device is still resource constrained, and some applications, generally, demand more resources than a mobile device can pay for. To overcome this, a mobile device should get resources from an external source. One of such sources present is cloud computing platforms. In Mobile Cloud computing generally front-end consists of users who possess mobile devices and back-end cloud servers. This pattern enables users to access a large volume of storage resources with portable devices in a distributed and cooperative manner. In between the time of uploading and downloading files or data, the privacy and integrity of files need to be guaranteed. The important task Mobile data store into the Cloud storage is in the encrypted form. The Data accessibility also be handled authentication and authorization .

Keywords---Mobile Cloud Computing, Cloud Computing, Mobile data security, privacy .

I. INTRODUCTION

Mobile Cloud Computing (MCC) at its simplest, refers to an infrastructure where both data storage and data processing happen outside of the mobile device, part of the Cloud Computing spectrum consider seamless integration between computer, the web and phone.

Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client.

Mobile Data storage is nothing but local Data storage, for Enhancing performance of whole system , while the battery is being lost or empty .there should be a platform for storing data ,so that user can retrieve his/her personal data without getting lost. Right now in this current era of IT, There is no prevision for recover lost data.

Mobile Data storage is nothing but local Data storage, for Enhancing performance of whole system , while the battery is being lost or empty .there should be a platform for storing data ,so that user can retrieve his/her personal data without getting lost. Right now in this current era of IT,
There is no prevision for recover lost data.

Here our main motto is to store data in cloud system and that too with high security. Lot of vendors are present on World Wide Web which provide facility to store data as personal. As provision is being provided by the vendors they can access our data very easily. And here comes the most crucial point of our project, here we are availing users with data encryption and decryption security. Now user can only access this data not any vendor or third party.

The term "mobile cloud computing" was introduced not long after the concept of "cloud computing" launched in mid-2007. It has been attracting the attentions of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, of mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost, and of researchers as a promising solution for green IT [1]. This section provides an overview of MCC including dentition, architecture, and advantages of MCC.

This Paper is structured as follows. section II, Architectures of Mobile Cloud Computing(MCC). Section III.Related existing work. Section IV. Proposed Scheme. Section V. Conclusion of this work.

II. ARCHITECTURES OF MCC

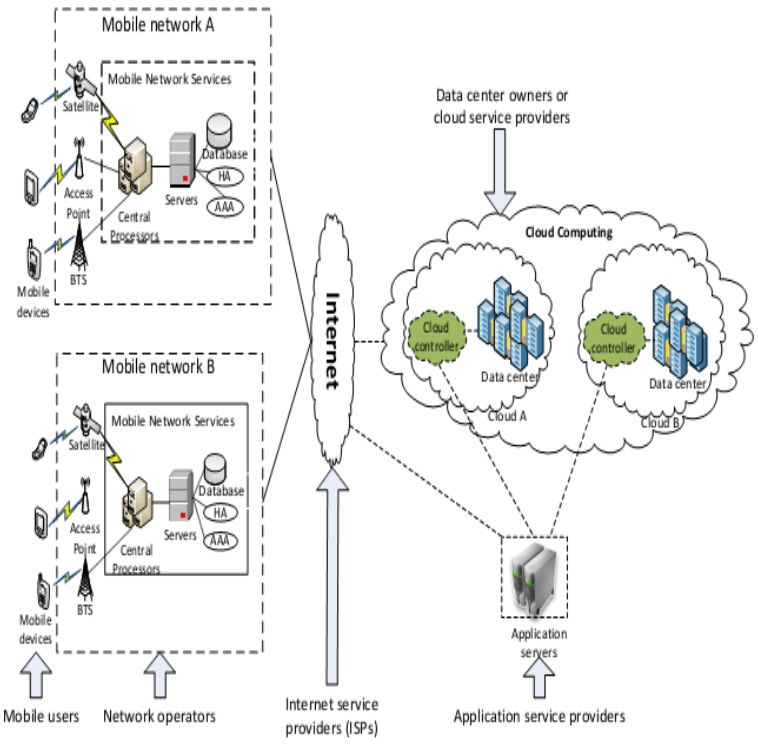

Figure :- Architectures of Mobile Cloud Computing

From the concept of MCC, the general architecture of MCC is shown in Fig. 1. In Fig. 1, mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Mobile users' requests and information (e.g., ID and location) are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers' data stored in databases. After that the subscribers' requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and service-oriented architecture (e.g., web, application, and database servers).

III. RELATED EXISTING WORK

What?offloads the processing and storage intensive encryption and decryption operations on cloud without revealing any information about data contents and security key. [2].

Secure data processing mobile cloud infrastructure is highlighted in Figure 1. The mobile cloud is comprises three main domains: (i) the cloud mobile and sensing domain, (ii) the cloud trusted domain, and (iii) the cloud public service and storage domain. In this framework, each mobile device is virtualized as an ESSI in the cloud trusted domain and each ESSI can be represented as an SN in a particular application (a.k.a., a service domain). The I ntroduced ESSIs can be used to address communication and computation deficiencies of a mobile device, and provide enhanced security and privacy protections. A mobile device and its corresponding ESSI can also act as a service provider or a service broker according to its capability, e.g., available computation and communication capabilities to support a particular communication or sensing service. This approach takes maximum advantage of each mobile node in the system by utilizing cloud computing technologies. In this way, the cloud boundary is extended to the customer device domain. Note that an ESSI can be an exact clone, a partial clone, or an image containing extended functions of the physical device. The networking between a user and its ESSI is through a secure connection, e.g., SSL, IPSec, etc. [3]

The 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 requests 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 checks it for equality with previous MAC stored. If these two MACs are same then integrity of file is verified and the result is transferred to DO.[4]

Liu et al. projected to use hierarchical identity-based encryption algorithm to provide an efficient sharing of the secure storage services in cloud computing. Here the encryption is used just the once and only one copy of the corresponding cipher text needs to be stored. It needs MD having higher computation ability. Wei et al. proposed Sec Cloud. It is an auditing scheme used to secure cloud computing based on probabilistic sampling technique [5].

Park et al. proposed a secure storage BLAST, which is improved by a stream cipher rather than a block cipher with a novel block accessible encryption mechanism based on streaming ciphers [6].

IV. PROPOSED SCHEME

In this paper, Asymmetric key approach is proposed. Asymmetric algorithms use pair of keys, one is used for encryption and the other one for decryption. The decryption key is typically kept secret, therefore called ``private key'' or ``secret key'', while the encryption key is spread to all who might want to send encrypted messages, therefore called ``public key''. Everybody has their own unique public key and is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann.

V. CONCLUSION

In this paper, a system is proposed for protecting the confidentiality and integrity of uploading files or data in mobile storage cloud. My solution enables to securely store and retrieve data into the cloud with minimal cost .In future, I will focus on the following headings: (i) investigate more application scenarios that require data access between mobile and cloud and (ii) investigate the security monitoring, auditing, and illegal intrusion in the mobile cloud system.

REFERENCES

[1] M. Ali, "Green Cloud on the Horizon," in Proceedings of the 1st International Conference on Cloud Computing (CloudCom), pp. 451- 459, December 2009

[2] Zhou and Huang proposed a privacy preserving framework called Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) for lightweight mobile devices. (Z. Zhou, D.Huang, Efficient and secure data storage operations for mobile cloud computing, IACR Cryptology ePrint Archive: 185, 2011)

[3] Anand Surendra Shimpi and R.P.Chander "Secure Framework in Data Processing for Mobile Cloud Computing" for International Journal of Computer Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012

[4] Preeti Garg, Dr. Vineet Sharma "Secure Data Storage in Mobile Cloud Computing" International Journal of Scientific & Engineering Research, Volume 4, Issue 4, April-2013 ISSN 2229-5518

[5] Manjunatha A, Ranabahu A, Sheth A, et al. Power of clouds in your pocket: An efficient approach for cloud mobile hybrid application development. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom10).Indianapolis, IN, USA, 2010: 496-503.

[6] Xu L, Xing T, Zhong Y, et al. Secure data processing framework for mobile cloud computing. In: IEEE INFOCOM 2011 Workshop on Cloud Computing (INFOCOMW11). Shanghai, China, 2011: 711-716

[7] http://en.wikipedia.org/wiki/Mobile_cloud_computing

[9] http://cloudtimes.org/mobile-cloud/

First Author

Mr. Yogesh Graham received the Msc (C.S) From Makhanlal Chaturvedi National University, Bhopal (M.P.) in 2009 And MCA from Punjab Technical University, Jalandhar in 2011 and pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India,. He is now attending the Mtech-CS course in CSIT and her research interest include Mobile Data Security with Cloud Computing and programming language (JAVA, ANDROID, PHP, ASP.NET), Cloud Computing and Web Development.

Second Author

Mr. Praveen Shende, Asst. Prof.,CSE Dept. C.S.I.T. Durg, India, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, His interests are Programming Languages(Java, PHP, Joomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.