A Security Access Control Mechanism for Outsourced Data in Mobile Cloud Computing Environment

Pratika Singh
Pranveer Singh Institute of Technology
Kanpur, U.P. (208020)
Dr. A.P.J. Abdul Kalam Technical University,
Lucknow, U.P.

Dr.HarshDev
Pranveer Singh Institute of Technology
Kanpur, U.P. (208020)
Dr. A.P.J. Abdul Kalam Technical University,
Lucknow, U.P.

ABSTRACT- ***"Mobile Cloud Computing"(MCC), is basically a cloud environment in which mobile users are acts like a client and cloud server at the back end which allows users to save and access their huge data with different mobile devices(such as tablets, smart phones, PDAs, etc.) in a diversified manner. Although Mobile cloud acts as an inventory of user's data and resolves the storage and processing issue but also it opens the door for the threat of data security. The present solutions has their drawback such as less flexibility, scalability and overloaded key distribution computation. And also some solutions are not applicable in mobile cloud environment. So we propose an "Access Control mechanism" which is not only lightweight with minimum computation overhead but also less expensive in nature and gives access right for data sharing. We are using out of band mobile authentication for data sharing which enables dynamic scalability, client side encryption and decryption and lesser overhead as compared to existing solution. The security encryption algorithm, sharing access right and use of out of band mobile authentication is highly analysed and proves its applicability with higher efficiency.***

Keywords – Mobile Cloud Computing, out of band Mobile authentication, Access Control Mechanism

I. INTRODUCTION

Growth of Mobile devices and then the fast development of mobile application has directed to the development of technology such as Mobile Cloud Computing. The MCC is a blend of mobile and cloud computing. Different researchers have define this new technology differently .Mobile Cloud computing forum defines Mobile cloud computing as "Mobile cloud computing refers to an infrastructure where both the data storage and data processing happing outside of the mobile devices"[1].

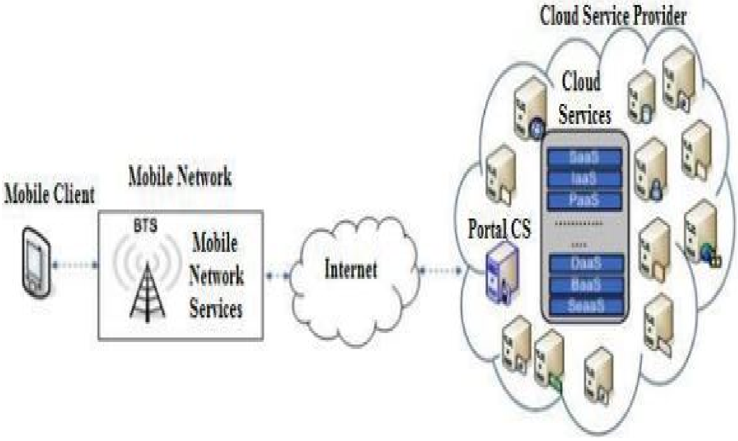

Fig. 1.*MCC architecture depicting portal and back-end cloud servers [2]*

Altogether, MCC utilizes the capabilities of Cloud computing, Mobile computing and the wireless infrastructure, and provides vast storage for a mobile user plus "always-on" connectivity for their personal and corporate data. As far as MCC architecture is concern it is shown in fig.1 as there are two servers in the cloud, the first gateway cloud servers that take requests from the mobile clients and depending upon the services demanded use the second back-end servers to serve the request.The traditional boundaries of Mobile computing are stunned by the virtualization and scalability of the cloud resources. Merging the two environments i.e. Cloud computing and Mobile computing, MCC has the following advantages.

1. Improved battery lifetime: Running long and powerful applications in the battery-controlled mobile devices is very problematic as it will rapidly drain out the battery. So, if these applications are totally or partially execute on the cloud, it will extend the battery lifetime.

2. Reliability: In the meantime data is kept and backed up on n-number of servers, any disaster can be controlled easily and the mobile device will have less chance of losing their data.

3. Processing & Storage: A huge amount of data can be processed and stored regardless of the resource restrictions of the mobile devices.

4. Meet unpredictable user demands: Service providers can simply develop their resources and facilities to meet the requirements of the users.

With these advantages Portable Distributed computing additionally has some difficult issues security and protection of client's information on the cloud. This is on the grounds that, the cloud servers, which house client's delicate information are observed and controlled by the suppliers and thus expands the danger of misuse. Once it involves sharing, data house owners need solely approved individuals to possess access to their information to take care of its integrity and privacy. Hence, the first necessities of any cloud storage square measure to produce security, privacy, confidentiality and fine-grained access management, flexibility in information sharing and answerability.

In this paper our aim is to supply fine-grained access management, dynamic measurability, confidentiality and integrity at a similar time within the MCC surroundings. For this, we've got analyzed the present approaches that have enforced the assorted access management mechanisms and pointed their flaws. Then, we've got projected a unique approach to understand fine-grainedness to user's information within the cloud that is achieved by OOB mobile authentication. This approach assumes the mobile device and therefore the cloud server storage to be semi-trusted and its benefits embrace dynamic measurability, low over head, and acceptable authentication to realize fine-grained access management, the theme is resilient to any information abuse on mobile devices. We've got established that this theme is secure below the assorted security necessities of the cloud and device storage.

This paper is prepared as follows. In section 2, we discuss previously done research work in this area, with analysis of strength and weakness. In section 3, we focused on possible attack on confidential data. In section 4, a brief overview of the proposed system, its features, working and architecture is discussed. Finally in section 5, we concluded our research Paper.

I. RELATED WORK

As MCC takes the advantages of cloud computing, it does also inherit the security issues that arise in cloud computing. But the frameworks designed for the cloud computing environment cannot be applied directly in the MCC environment, since mobile devices have additional limitation of resources. Thus, the frameworks needed for MCC should not just be lightweight but also requires minimum computation and processing overhead.

The numerous issues relating to MCC include:

Firstly secure migration of mobile applications on the cloud i.e. a ***secure communication (transport) channel.***

Secondly, ***security, privacy, and integrity*** of the applications stored on the cloud, their authentication and access control, as to who is authorized to access the user's data. Then, how so many users are managed, if any shared key is provided individually then a mechanism for ***key management*** is required.

Thirdly, not only security of data on cloud is essential but also the applications on the mobile device should be protected. Thus, security in MCC is related to both ***security of data in the cloud and security of applications in the device***. Although, the smart phones now a day shave security features like the Google Drive Policy Application [3] through which users can remotely clear or lock information stored in a stolen or lost mobile device, but to overcome a number of other threats various approaches/methods have been presented.

In [2] the authors have given the evaluation criteria for the security frameworks of MCC. In their survey paper which covered almost all the proposed work till now in the field of MCC including both data manipulation on device and cloud servers. Their survey classifies current security frameworks for MCC into two categories:

(a) Frameworks for securing data in the cloud
(b) Frameworks for securing application installed or updated in the device.

A number of proposals to protect data have been made in the recent years such as [4, 5, 6,7, and 9].Specifically, [6] and [9] focus on the data integrity issue. In [6] Itani Wetal. proposed an energy-efficient protocol to ensure the integrity of data in MCC. The incremental cryptography primitives [7], [8] and the trusted computing model which is based on the cryptographic co-processor applications of the Dyad project [10] is used. Techniques such as identity-based encryption (IBE) [12], Proxy-re-encryption (PRE) [11], various extensions of on attribute based-encryption (ABE) such as [13, 14] have been realized to provide confidentiality and access control to cloud data.

In [15] Zhou and Zhibin have extended the Ciphter text Policy Attribute-Based Encryption (CP-ABE) [13] and called it Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) scheme. The CP-ABE based schemes [13, 14, 15] which provide confidentiality and better access control, facilitate key-management in an efficient manner have some weaknesses and open research challenges which have been overcome by the authors.

In [16] also, the authors have proposed an ABE extension, key policy-attribute based encryption scheme (KP-ABE), for secure data outsourcing in the cloud servers. However, we argue that in a dynamic mobile cloud, the ABE based approach is not efficient in the MCC due to reasons stated in the section above.

In [17] authors proposed a secure data service mechanism (SDSM) for MCC which out sources both data and security mechanism to the cloud and uses Identity based proxy re-encryption (IBE) [18], [19]where a semi-trusted proxy transforms the data encrypted with owner’s public-key into the one encrypted with sharer’s public key. The IBE is based on bilinear mapping. The proxy-re-encryption scheme used consists of six algorithms i.e. Setup, KeyGen, Encrypt, RKGen, Re-Encrypt, and Decrypt. As discussed above, data in the cloud is stored using cryptographic approaches which transform the plain text into cipher-texts. This protects the data from intruders and to some extent ensures that only authorized people get access to the data.

II. PROPOSED FRAMEWORK

We propose a lightweight access control mechanism where the mobile users outsource data with minimal security management overhead. The basic idea of the proposed framework is to provide maximum security to the data, maintaining integrity, realizing confidentiality and fine-grained access control by using OTP- mobile authentication for data sharing rather than regular communication means such as e-mail. To realize this, we have used simple hash functions and exclusive-or operations for key generation and password storage, followed by symmetric encryption algorithm to encrypt data before uploading. This protects data from leaking since key is generated using user’s file name and file size. Furthermore, server side application running in the cloud servers allow viewing and downloading of data after the user enters the OTP sent on the mobile number provided by the sharer. This facilitates for dynamic sharing and improved scalability unlike [57] where sharer attributes are pre-determined and thus suitable only for static and small-scale networks.

IN OUR FRAMEWORK,

1. *We have considered the shortcomings and disadvantages of the existing approaches where most of them assume the cloud servers and mobile devices to be in the same trust domain, the vulnerability of mobile devices (in case they are lost or stolen) has been ignored, & there is heavy communication overheads in key distribution and data management.*
2. *We have worked towards maintaining integrity of the file while uploading and downloading, reducing communication and computation overheads, providing appropriate authentication of the sharers before granting access rights, lost and stolen mobile devices have also been considered.*
3. *A new technique for fine-grained access control, which includes, client-side encryption (where data is encrypted before uploading), OTP based authentication for sharers (before giving access of data), no key distribution mechanism required thus reducing the communication overhead, use of hash and concatenation operators thus reducing computation overhead.*

II.1 SYSTEM MODEL

The MCC environment comprises of the cloud server, the data owners (DO) and the data sharers (DS). The cloud servers store the data uploaded by the DO. This data is downloaded either by the DO or DS. The DO and DS use their mobile devices to have access to the internet where their data is located.

© 2014- 16, IJIRAE- All Rights Reserved

The cloud servers not only provide storage but enforce access control policies on the stored data. In our access control mechanism, the DO forwards the encrypted file to the cloud servers. The DS who wish to access the file are firstly authenticated by sending an OTP via SMS on their registered mobile number. On verification, authorized sharers are allowed to access the file with appropriate rights (read-only, write-only, read-write, print, download, etc.).

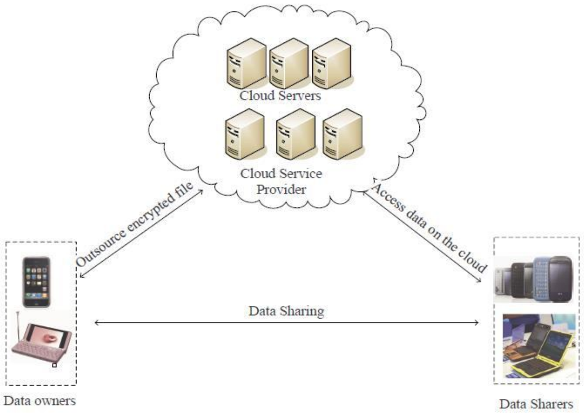

Fig.2. Network model for our protocol

II.2 TRUST MODEL

We make the following assumptions in the functioning of our technique for access control.

1. The cloud servers are semi-trusted. They are assumed to perform the access control properly, but cannot be completely trusted, hence the encryption and decryption in our proposed system is performed at the client-side
2. The Mobile devices are also semi-trusted. We assume the computations to be faithful but distrust the storage, as it is prone to attacks by malicious software's or attackers. In case they are lost or stolen, the user's privacy is at stake. Hence, in our authentication phase where an OTP is sent via sms on the device, the sharer needs to enter both the OTP and a secret key provided during registration(which is just like an ATM pin that a bank provides and known only to the user).
3. The links between the mobile devices and the cloud servers are assumed to provide safe upload and download ensuring integrity and privacy of user's data. This is because of the IP layer protocols such as IP sec.

II. 3 FEATURES

Before we discuss the working and algorithms of our protocol, we give a small overview of the features of this protocol. The protocol although employs the existing symmetric algorithm (such as DES) for encryption and decryption but the authentication mechanism prior to granting access rights, reduced server dependency, fine-grained access control, and inherent authorization revocation makes it most suitable for the MCC environment. The protocol has the following merits:

1. *Safe upload and download: Since encryption and decryption occurs at the client-side, the storing and retrieving is done in the form of cipher-text, thus it becomes secure preserving the data integrity.*
2. *Stronger and better access control: Only authorized sharers get to access the data. Unauthorized users get to know nothing about the data content.*
3. *Dynamic Scalability: In MCC, where users are mobile, attributes cannot be fixed for decryption rights since they change in with the user's location. In our mechanism, lower cost of communication, flexible in operation makes it suitable for MCC*
4. *Lightweight with less computation and communication overhead: Simple hash functions and ex-or operations in key creation are used. No key forwarding mechanism required.*
5. *Mobile OOB Authentication For authorization rights OOB channel, as the name suggests basically refers to communicating via a channel outside the previously established channel. For e.g. If two users are interacting and sharing data via emails then for security reasons they can send their important information (such as a secret key) via a phone call or message. OOB authentication is used by most banking services now a days to verify user's identity through a separate channel. This includes sending One-time passwords, pin, etc.*

III. WORKING AND ARCHITECTURE

1. Client-side Application

The application will be a web application which will be rendered to both the mobile and desktop users.

*a. The user first needs to create an account by **signing up** to the application and entering **username** and a **password**.*
b. The user will be automatically allocated space to store and share data.
c. Space for personal (individual) usage of data and shared data will be separate.
d. Different groups with different rights shall be created in the shared space.
e. Users can login both from mobile and desktops as it will be a generic app.
f. All options for sharing, storing and synchronization will be available.

2. Server-side Application

a. This application running in the portal cloud server, will be the one with which the client side application will interact.
b. Through this application data will be stored in the back-end i.e. storage assigned by RED HAT.

3. Storage and Platform Open shift by Red Hat (by Linux) which will provide us the required space on subscription basis and a range of platforms to choose from in the cloud app development.

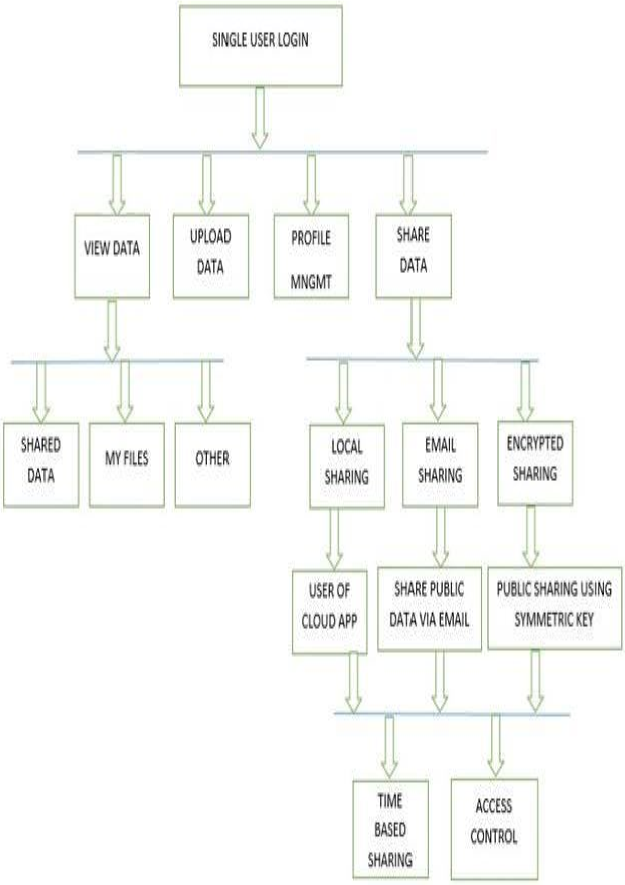

Fig.3. Flow of Working

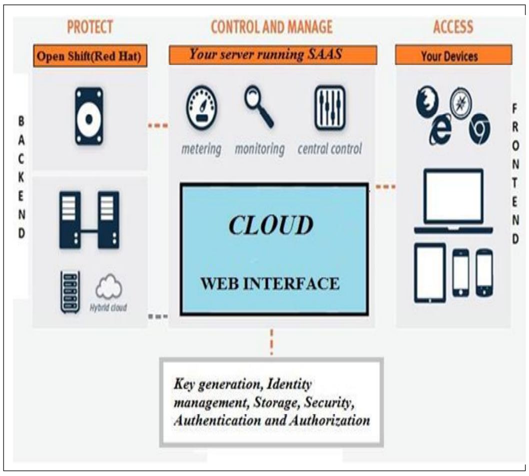

Fig.4. Proposed Architecture

IV. RESULT& DISCUSSION

Considering both the perspectives i.e. vulnerability of the mobile device being exposed to malicious attackers/software's and securing data in the cloud, the application is aimed to provide security, integrity, confidentiality, appropriate authentication and authorization and fine-grained access control to user's data. To examine each of these parameters we have given a detailed justification of how these features are realized in this approach.

There are various flaws found in traditional applications and our proposed modeler solved them and provide better and efficient solution.

Feature	Proposed Model	Box	Drop Box	Google Drive
Client Side Data Encryption	Yes	No	No	No
Channel Encryption	Yes	Yes	Yes	Yes
Fine Grained Access Control	Yes	Yes	Limited	Limited
End to End Data Sharing	Yes	No	No	No
Automatic Backup	Yes	No	No	No
Log Creation	Yes	No	No	No

Table 1. Comparison of our proposed cloud model with other clouds

V. CONCLUSION

This research work aims to provide fine-grained access control, dynamic scalability, confidentiality and integrity at the same time in the MCC environment. Firstly, we have analyzed the current approaches that have implemented the various access control mechanisms and pointed their flaws. Then we have proposed a novel approach to realize fine-grained ness to user's data in the cloud which is achieved by OOB mobile authentication. This approach assumes the mobile device and the cloud server storage to be semi-trusted and its advantages include dynamic scalability, low overhead, and appropriate authentication to achieve fine-grained access control, the scheme is resilient to any data abuse on mobile devices. We have proved that this scheme is secure under the various security requirements of the cloud and device storage.

VI. REFERENCES

[1] http://www.mobilecloudcomputingforum.com/
[2] Khan, Abdul Nasir, et al. "Towards secure mobile cloud computing: a survey." Future Generation Computer Systems 29.5 (2013): 1278-1299.
[3] Device policy for Android: Overview for users.[Online]Available:http://www.google.com/support/mobile/bin/answer.py?hl=en&answer=190930.
[4] Zhang, Xinwen, et al. "Securing elastic applications on mobile devices for cloud computing." Proceedings of the 2009 ACM workshop on Cloud computing security.ACM, 2009.

[5] Pautasso, O. Zimmermann, and F. Leymann. Restful web services vs. big web services: Making the right architectural decision. In Proc. of WWW, 2008.

[6] Itani W, Kayssi A, Chehab A. Energy-efficient incremental integrity for securing storage in mobile cloud computing, In International Conference on Energy Aware Computing (ICEAC), January 2011.

[7] M. Bellare, O. Goldreich, and S. Goldwasser, Proc. 27th Symposium on the Theory of Computing, pp. 45-56,1995.

[8] M. Bellare, O. Goldreich, and S. Goldwasser, Crypto ’94, Vol 839, Springer-Verlag, pp.216-233, 1994.

[9] Boneh, Dan, and Brent Waters. “Conjunctive, subset, and range queries on encrypted data,” Theory of cryptography. Springer Berlin Heidelberg, 2007.535-554.

[10] M. Bellare, O. Goldreich, and S. Goldwasser, Crypto ’94, Vol 839, Springer-Verlag, pp.216-233, 1994.C J. D. Tygar and B. Yee, In Proc. of IP Workshop, 1994.

[11] B. J. Shao and Z. Cao, “Cca-secure proxy re-encryption without pairings,” in Public Key Cryptography, 2009, pp.357-376.

[12] Green, Matthew, and Giuseppe Ateniese. "Identity-based proxy re-encryption."Applied Cryptography and Network Security.Springer Berlin Heidelberg, 2007.

[13] Bethencourt, John. "Intro to Bilinear Maps."Computer Sciences Department, Carnegie Mellon University. http://www. cs. berkeley. edu/" bethenco/bilinear_ maps. pdf. Version: März(2006).

[14] Chow, Richard, et al. "Authentication in the clouds: a framework and its application to mobile users." Proceedings of the 2010 ACM workshop on Cloud computing security workshop.ACM, 2010.

[15] Zhou, Zhibin, and Dijiang Huang. “Efficient and secure data storage operations for mobile cloud computing”, Proceedings of the 8th International Conference on Network and Service Management. International Federation for Information Processing, October 2012, 37-45

[16] Katz, Jonathan, AmitSahai, and Brent Waters. “Predicate encryption supporting disjunctions, polynomial equations, and inner products,” Advances in Cryptology– EUROCRYPT 2008. Springer Berlin Heidelberg, 2008.146-162.

[17] Jia W., Zhu, H., Cao, Z., Wei, L., & Lin, X. “SDSM: a secure data service mechanism in mobile cloud computing,” Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011, 1060-1065.

[18] Shao, Jun, and Zhenfu Cao. “CCA-secure proxy re-encryption without pairings”, Public Key Cryptography–PKC 2009. Springer Berlin Heidelberg, 2009, 357-376.

[19] Green, Matthew, and Giuseppe Ateniese. “Identity-based proxy re-encryption,” Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2007, pp. 288-306.

© 2014- 16, IJIRAE- All Rights Reserved