Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

AN APPROACH TO SAFEGUARD PRIVACY AND INTEGRITY OF DATA STORAGE IN MOBILE CLOUD COMPUTING

Priyanka varma, Hardik Upadhyay
M. Tech Student, Department of Computer Engineering, MEC, Basna
Department of Computer Engineering, GPERI, Mehsana

.

Abstract- *Mobile cloud computing is a combination of mobile computing and cloud computing that provides a platform for mobile users to offload heavy tasks and data on the cloud, thus, helping them to overcome the limitations of their mobile devices, where data processing and storage can happen away from mobile device Although, cloud storage brings convenience to mobile users, at the same time brings the certain risk to the security of their data as the user will have to surrender the control of their data. Due to storing data on cloud there is an issue of data security, integrity and confidentiality. To ensure the security of user's data in the cloud we propose an effective mechanism for data integrity and confidentiality. The enhanced mechanism provide flexible security using different algorithms with key variation (depending on sensitivity of file), Hash function (dynamic verification), CRCs for checking network transmission error and Group policy providing low cost, less communication overhead and better security to the data stored on the mobile cloud.*

Index Terms— *Mobile Cloud Computing, Security, Data Storage Correctness, Integrity, Flexibility, Group Policy*

I. INTRODUCTION

Mobile devices are becoming the essential part of communication in today's world of communication. Mobile users are greatly experienced of the services of mobile applications (e.g. iphone apps, google apps etc.) which run on devices or remote servers with the powerful proceedings of mcc as a powerful trend in the development of IT technology as well as commerce and industry fields. But, the mobile devices are facing many challenges related to resources as well as the communication.
Cloud computing (CC) refers to the next generation's computing infrastructure cc offers the advantage and provide its users to use the platform (e.g. operating system and middleware services), software (e.g. application programs) provided by cloud providers at reasonable cost and infrastructure (e.g. network, servers, storages) with the commencement of mobile applications as well as the support for CC for a variety of services to its mobile users, mobile cloud computing (MCC) can be defined in simple terms as an integration of cloud computing into the mobile environment.
Most applications built for smart phones require intensive computing power and software platform support for application execution. Many low-end but browser-enabled mobile phones are unable to support such applications with the advent in mobile cloud computing, the resources in terms of computing storage and platform support required to execute these application are available through the cloud and in theory, a greater number of devices can be supported.
We need to transfer applications processing from the mobile devices to the cloud. The centralized applications are there after accessed over the wireless connection based on a thin client or the web browser on all the mobile devices. MCC is the combination of mobile web together with the cloud computing and is the tool to access the web services and application on internet. Briefly, MCC provides mobile users with data processing as well as storage services in cloud.
Due to storing data on cloud there is an issue of data security and confidentiality. To provide security to the user's data one can encrypt the file and send it to cloud. Also integrity is another major challenge in outsourcing data to the cloud. Once user upload the data to the cloud it is no longer resides in mobile devices. At cloud side data may get corrupted because of several reasons. So, beside encrypting the data one should also calculate the hash of the file before uploading to storage service provider. In this paper, we design an approach to safeguard and provide better security using Cryptography and Hash function to ensure integrity and privacy of user's data on mobile cloud with less computing cost and communication overhead and providing security flexibility.
The rest of the paper is organized as follows. Section 2 illustrates Survey on various security proposals on storage correctness approaches available with their pros and cons. Section 3 contains overall comparison among all these approaches followed by Proposed model in Section 4. Section 5 comprises of experimental analysis followed by conclusion in section 6. Last section contains the list of references used.

II. SURVEY ON VARIOUS SECURITY PROPOSOLS FOR

DATA STORAGE CORRECTNESS

Md Whaiduzzaman, Abdullah Gani in [1], has proposed trusted third party for security ranking. An automated software scripting model is used by penetration testing for TTP to run on CSP side. TTP must maintain trust, reliability and should have enough resources.

Authors of [2] Preeti Garg and Dr. Vineet Shanna have used RSA and hash function with other encryption and decryption processes to provide security to the user's data. TPA provides integrity check and perform computational intensive tasks All the computations and verification are offloaded to TPA and there is no mechanism provided to verify TPA.

Criteria Group →	Integrity oriented measures			Confidentiality oriented measures			Others					
Individual Criteria → Cloud Providers ↓	Verification Cost(Time)	Verified by CSP ?	Algorithms used ?	Encryption (Data at rest)	Encryption (Data in transition)	Flexible security options	TPA?	Access rights mechanism	Searching Mechanism ?	Implementation result ??	Network transmission error??	Group Policy?
[1]	more	x	√	x	x	x	√	x	√	√	x	x
[2]	more	√	√	√	√	x	√	x	x	√	x	x
[5]	Less	x	√	√	√	x	x	x	x	x	x	x
[7]	Less	√	√	√	x	x	x	x	x	√	x	x
[8]	more	√	x	√	x	x	√	√	x	√	x	x

Abir Awad and Adrian Matthews of [3] developed a mechanism for automatic ranking in order to alleviate the task for the mobile user and make the scheme more user friendly. In the research work, they have designed a new automated ranked fuzzy keyword search method

that allows a secure storage and search of the data on the cloud. A content based index is a secure searchable encryption scheme that allows the user to store their files on cloud in a secure way and then perform a secure query and fuzzy search. There is a need for improvement of retrieval performance of the whole scheme.

CAO Wanpeng and BI Wei of [5] introduced

Adaptive and Dynamic data encryption method to make the data encryption safer. The encryption algorithm selection strategy is confirmed from phone's character such as hardware, personalization information and a pseudo-random number. It possess higher complexity and strength can be increased by adding them into the encryption algorithm library.

III. COMPARISON OF VARIOUS RESEARCH SCHEMES

The table.1. shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique used with the benefits that researcher gets as well as the limitations found in schemes.

IV. PROPOSED MODEL

Confidentiality and integrity are the two of the main goals to be achieved in Security Data storage model for Mobile Cloud Computing. Both the operations in our model are achieved as mentioned beneath :

(A) Encryption Process: Encryption is performed before the file is uploaded on the cloud to provide confidentiality to the data. It is performed at CDO's site or CDU's site, they can choose encryption algorithm along with appropriate key. Here

flexibility for algorithm is provided to the data owner according to their respective files. Different symmetric key encryption and asymmetric key encryption may be used here. The keys are to be stored and maintained by the data owner, per file, locally.

(B) Dynamic Verification: This is the process in which, for providing high security owner gets the list of its files from CSP. Owner chooses the file and send request for random bits, then CSP finds those random bits of the same file and sends back to the client. The client needs to fetch same bits from the local file and compares it. In case of moderate security user gets the list of its file from CSP, it chooses the file and send request for getting hash, then CSP calculate hash and sends back to the client. Client compare the hash for that file and if it is same then the file is not been modified.
For checking the integrity of data client request for random bits verification which leads to reduction of time required by CSP and client by getting some data only.

(C) Group Policy: In this policy user (owner) defines rules for its own files for other users. As per this policy user can also get list of files from cloud server and list of user as well. By doing this owner chooses file and list of users from cloud then assigns (read/write) rights to the user.

This policy is beneficial for two reasons:

I. Each user does not need to request separately for owner's file.

II. It also reduces the intra communication request hence it reduces request traffic on cloud server.

(D) Network transmission error: The RC232 embedded RF Protocol is used in a range of products from Radiocrafts. The Protocol handles host communication, data buffering, addressing and broadcasting and error check. It support point-to-point, point-to-multipoint and peer-to-peer network topologies.

Other than above the Model is also provides following security goals:

(a) Correctness of the stored data: Data on to the cloud cannot be altered or modified by the user who doesn't having rights to access the data.

(b) Different levels of encryption: Based on sensitivity, users' data can be divided into three Categories :
(1) Not sensitive (fully trusted model)
(2) Highly sensitive data (not trusted model) (3)Moderately sensitive data (partial cryptographic primitives). So, Based on this Sensitivity level, Aim is to provide different encryption schemes.

(c) Lightweight: Implementation point of view the model must consume low computation cost at client side as well low communication overhead.

(d) Duplicate copy of original data should not be generated.

(e) No assumption of file type or file properties.

As well while wish to achieve above the model cannot be compromised with other standard security goals like Availability, reliability, efficient retrieval and data sharing Etc.

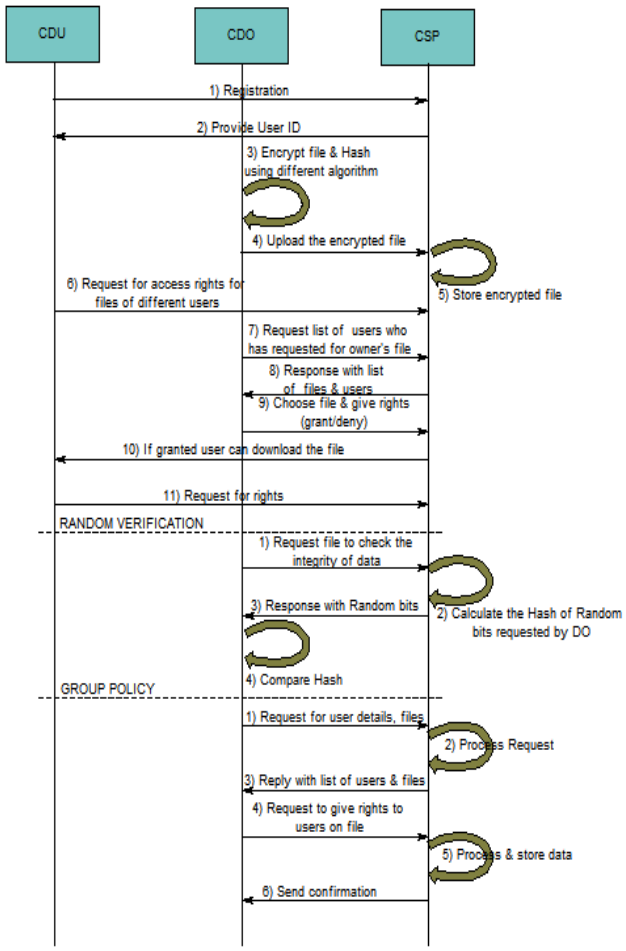


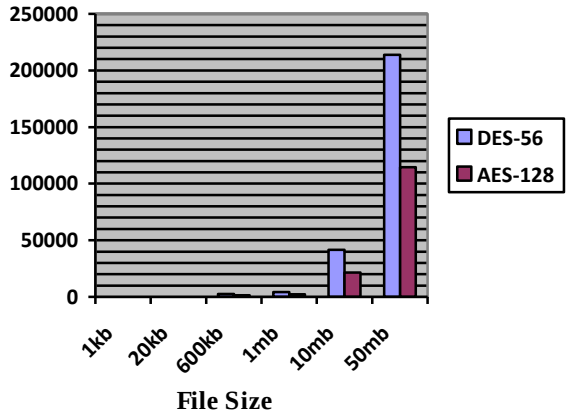
Fig. 1.Intraction among data owner, cloud provider and users

V. EXPERIMENTAL ANALYSIS

Experimental result for Encryption algorithm AES and DES are shown in Table.2 by giving different file size as an input and record computation cost. Figure.2 shows a chart for File size V/S computation cost.

File Size	DES-56	AES-128
1kb	2.613425	11.256
20kb	10.575115	43.854
600kb	2595.752	1384.655
1mb	4345.451	2156.310
10mb	41581.973	21624.54
50mb	213689	114572

Table. 2 Computation Cost (Encryption)



From above we can say that DES provides highest speed but it is not so secure. In contrast AES does not provide high speed but it provide more security. As far as the security is concern we should prefer AES or RSA.

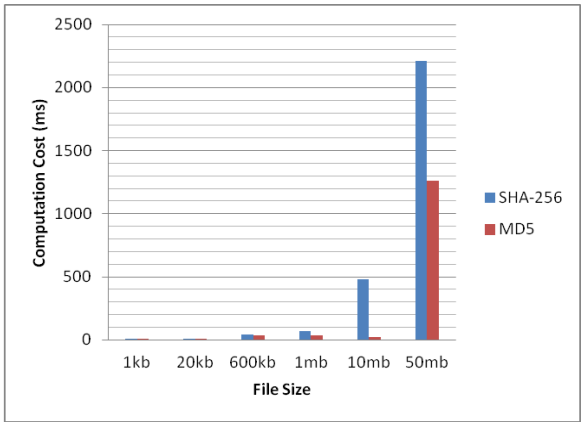


Fig.3 File size V/S computation cost

From above graph we can say that MD5 works faster than SHA-256 but as far as security is concern user should prefer SHA-256.

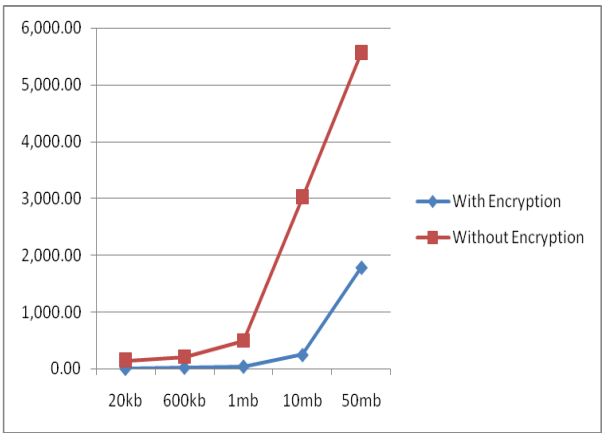


Fig.4 Time consumption for encryption and non encryption of a file

The above graph shows the time consumption for encrypted verses non encrypted files of user. As the size of the users file increases the time for encryption also increases.

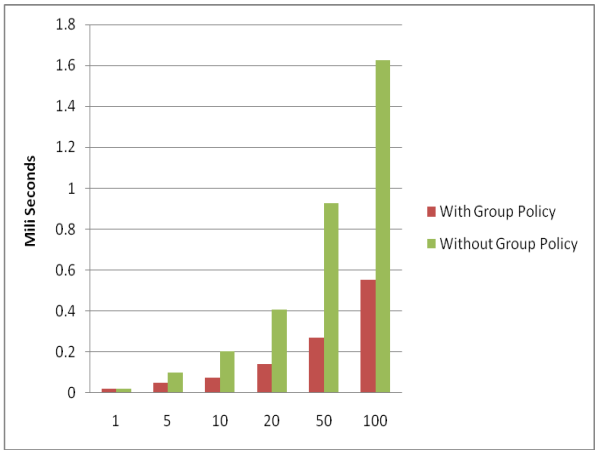


Fig.5 Number of request made by user in unit time (ms)

Here on Horizontal Axis we have shown the number of request per unit time. If we consider with group policy then the user can provide group access to all the files within short period of time. While in case of without group policy every time the owner needs to check and provide rights to individual users which consumes more time. Thus, group policy reduces the communication overhead and computation cost.

The proposed model provides its user with an environment where the user can select the algorithm according to sensitivity of its files. It enhances the data Confidentiality and security by using different encryption and encoding algorithms with different size of keys. Group policy reduces the communication overhead and cost whereas dynamic verification consumes less time and processing for integrity check and provides more security to the users file on cloud. It can also check for the network transmission error occurred during transmission of data from user to cloud and vice versa.

VI. CONCLUSION

This proposed model presented a set of security rules to secure the data files of a data owner in the Cloud environment. In my proposed scheme, the combined approach of access control and cryptography is used to protect the outsourced data. We use the access control mechanism along with public key encryption. A model is proposed for the users to access the outsourced data efficiently and securely from Cloud service providers' infrastructure. It provides the user with the security flexibility, reliability, low computation cost and less communication overhead. It also check the network transmission error if occur during transmission of data. The public key, hash, and private key ciphers that are proposed between Cloud service provider, data owner, and user ensure an isolated and secure execution environment at the Cloud.

VII. REFERENCES

[1] Md Whaiduzzaman, Abdullah Gani, Measuring Security for Cloud Service Provider : A Third Party Approach, 2013 International Conference on Electrical Information and Communication Technology (EICT), 2013

[2] Preeti Garg, Dr. Vineet Shanna, An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function, Internationai Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE, 2014, pg 334-339

[3] Abir Awad, Adrian Matthews, Brian Lee, Secure Cloud Storage and Search Scheme forMobile Devices, 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014, pg 144-150

[4] Amar R.Buchade, Rajesh Ingle, Key Management for Cloud Data Storage: Methods and Comparisons, IEEE, 2014 ,pg 263-270

[5] CAO Wanpeng, BI Wei, Adaptive and Dynamic Mobile Phone Data Encryption Method, Network Technology and Application, China Communications January 2014, pg 103-109

[6] Xueli Huang and Xiaojiang Du, Achieving Big Data Privacy via Hybrid Cloud, 2014 IEEE INFOCOM Workshops: 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data, 2014 pg 512-517

[7] Manisha Jindal, MayankDave, Data Security Protocol for Cloudlet based Architecture, EEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014
[8] Harsh Yadav and Mayank Dave, Secure Data Storage Operations with Verifiable Outsourced Decryption for Mobile Cloud Computing: IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India
[9]Sapna Malik and MM Chaturvedi " Privacy and security in mobile cloud computing: Review" International Journal of Computer Applications (0975 – 8887) Volume 80 – No 11, October 2013
[10] Han Qi and Abdullah Gani," Research on mobile cloud computing: Review, trend and perspectives", in DICTAP, by IEEE, 2012
[11]http://en.wikipedia.org/wiki/Mobile_cloud_computing.
[12] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, A survey of mobile cloud computing: architecture, applications, and approaches, Wireless Communications and Mobile Computing,WileyOnlineLibrary, http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/full,2011
[13] Itani W, Kayssi A, Chehab An Energy-efficient incremental integrity for securing storage in mobile cloud computing, In International Conference on Energy Aware Computing (ICEAC), January 2011
[14] Ou S, Yang K, Liotta A, Hu L. Performance analysis of offloading systems in mobile wireless environments, In Proceedings of the IEEE International Conference on Communications (ICC), 2007; 1821
[15] Chow R, Jakobsson M, Masuoka R, et al. Authentication in the clouds: a framework and its application to mobile users, In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), 2010; 1–6.

