International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

An Efficient Data Sharing and Retrieval Method for Cloud Computing

Santosh Chinchali, Shivakumar Honawad

Abstract*: now a days mobile devices can use cloud for data Access and manipulation without knowing overhead of local data management this may lead to leakage of sensitive data. Major disadvantage is to provide security for the user data , so this leads to concern for the user to access cloud computing. Lot of Research work carried out to provide security to user data over cloud computing, However these solutions are not resolve issues of mobile cloud computing due to constrained resource in mobile devices[2]. To overcome these issues, proposed methodology efficient data sharing and retrieval method, provide secure access control terminology using attribute based encryption in cloud platforms, as well as by using lazy-revocation technique will reduce user revocation cost

***Keywords* :,access,cloud, security,revocation.**

I. INTRODUCTION

THE popularity of cloud computing and mobility devices, users accessing data from cloud using smart data sharing technique to store their personal/sensitive data or retrieve the data from the cloud. These are constrained devices because of limited information/data storage capacity and computational resources in comparison with cloud has more number of resources. In order, to improve the performance it is better to use the functionality facilitates by the Cloud services .

now a days people can store their data in different forms such multimedia documents, text document, pdf and different format files to the cloud and share these files to different individual. Cloud service provider facilitates data management methods for authorized owner. Moreover these data are private and sensitive data owner can made available to access public or any specific people.

The privilege provided by cloud service provide is not upto the mark. When people store data on to the cloud CSP can make use of this data for commercial purpose[2]. and if data owner wants to share their encrypted data to the specific people, then data owner have to provide password to all to those whom he allow to access, which is not convenient. or else simplify the sharing method,

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Santosh S.Chinchalli*, Department of Information Science and Enginnering, V.P.Dr P.G.Halakatti College of Engineering and Technology Vijayapura, India. Email: santoshchinchalli@gmail.com
Shivakumar K. Honawad, Department of Information Science and Enginnering, V.P.Dr P.G.Halakatti College of Engineering and Technology Vijayapura, India. Email: shivakumar.honawad@gmail.com

the data owner can make group of users of people of he want to share password. However, in this approach also password management is a big concern.

To rectify these mentioned issues, owner information/data must be encrypted before sending it to cloud. The data encryption brings new challenges into picture that addressing efficient data retrieval control mechanism on ciphertext decryption to restrict only specific users can able to access data. Also system must provide different features for data owners to handle effective privilege management policy. By these features they can easily grant/revoke privileges of data users. There are continues lot of researches conducted on data access control based on ciphertext. In this approach can divide the task into different categories such as encrypted data access control, sequential retrieval, access control based on fully homomorphic encryption and access control based on attribute-base decryption, this method contain complex computation as well large amount of storage is required , these features are not well suited to constrained device such as mobile devices. As per the experiment results, attribute based encryption operations consume more time on handheld devices compare to laptop/desktop computers.

It will take wast amount of time to execute on mobile device than desktop computer . This remarks that a encryption process which is taking few minutes in desktop will take multiple of 10 minutes on mobile device. Also current system does not reflect effective user privilege management policy. So attribute based encryption operation can yield in higher revocation cost and it is suitable for mobile devices as well that is this will helps to resolve problem data sharing method in mobile cloud application by providing efficient access control policy over ciphertext.

To overcome the latency on mobile devices, this method uses third party servers for encryption and decryption. The attribute based encryption operations are executed on servers to reduce the latency on these devices. To provide privacy to owner data decryption key format is modified while sharing between proxy servers in order to provide maintains privacy over key sharing.

To reduce the user revocation problem, by introducing lazy re-encryption and decryption. Revocation cost is reduced.

Implementing a data sharing scheme based on light weight data sharing. The experiment results show that, this will reduce the computational overhead on mobile devices. Also this will reduces the revocation cost on users.

II. EXISTING SYSTEM

The problem identified with existing system is the data privacy and data security.

When the owner upload data file on to the cloud, it is no where control by data owner. Cloud service provider perform the data handling functionality for data owner efficiently, but it is not very convenient because, this data can used for data mining . in case data owner needs to share data with certain user then need provide the password if further need to send to many then password has to be provided to all in order to overcome this issue data owner can make group of user whom he want to share the data. but this is not an convenient method and password management become major issue. These issues can be addressed by encrypting the data files before sending on to the cloud, thus the data is secure compare to the cloud services. Challenges to resolved is here is to provide secure access control mechanism on ciphertext decryption so that only the specified user can access the data file.

III. PROPOSED WORK

This section illustrates efficient data sharing scheme system design. Overview ,algorithm.

3.1.Overview

The proposed efficient data sharing and retrival in mobile cloud. It has different parts as described below.

(1) The owner share the data to the mobile cloud and can be shared to certain specified users. different access permission policies are to be handled by the owner.

(2) The data stored on to the cloud can be retrieved by the owner.

(3) The functions like key generation and distributing attribute keys are performed by third party authorization.

(4) The data encryption operations for data owner are provided by ESP.

(5) The data decryption operations for data user are provided by DSP.

(6) The data sent by the data owner is stored in cloud service and it executes the operations requested by the owner. It will instantly search for the data stored by the owner.

As the figure below illustrates, the owner uploads the files to the cloud in the encrypted form Because the cloud is not that safer, The access control policies are defined by the data owner.In this data sharing scheme, the symmetric encryption mechanism is used to encrypt all the data and the attribute based encryption is used for data encryption. The ciphertext of the symmetric key contains the access control policy within itself. The data user can decrypt the encrypted data and access symmetric key only. The Service Provider such as Encryption and are used to reduce the overhead on the client side devices. But these are not that trust-worthy. In this paper, data sharing ing scheme in association with attribute based retrieval algorithm make sure that the data is secured and the data privacy has to be maintained.

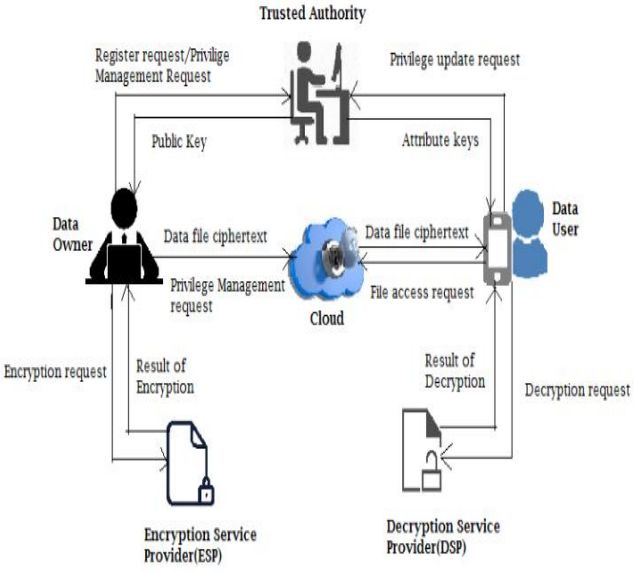

Fig. 1. Efficient data sharing scheme framework.

3.2.Algorithm

Step 1: master key will be generated and based on the value set of the data owner and version attribute, public key will be generated.

Step 2 : attribute keys for data user will be generated by using user attribute /value set and master key..

Step 3 : the ciphertext will be generated using different key such as public key , symmetric key .

Step4 : by using the attribute keys and the access control tree , ciphertext is decrypted.

IV. IMPLEMENTATION

Implementation of data sharing scheme involves various operations such as initialization of system, file encryption, authorization of user, file decryption, revocation and documentation updates.

1. Initialization of system

Data owner provide his information to register into the system and request key from third party authorization, this third party authorization run the algorithm generate a public key and master key, then the public key is sent to the owner and master key secured with trusted third party authority[2]. Data owner define its own attribute set and it will be sent to trusted third party and the cloud.

2. File encryption

Data owner send the file for encryption before uploading it to cloud. In encryption module the data will be encrypted by using symmetric cryptographic mechanism with symmetric key mechanism

3.Authorization of user

Data user register into the system by providing the information then send authorization request to Third party authorization. This will generate attribute keys for data user. third party authority compares the attribute description field in the attribute key with the attribute description field stored

in database whether data user's attribute has been revoked or not and it also checks the version of every attribute key of data user to update the attribute keys for user, when owner changes the attribute of user.

4. File decryption

User send the request to cloud to acces the file. Cloud check the credential whether data user meet the requirements and send ciphertext[1]. data user receives the ciphertext data file and symmetric key and request Decryption service provider to executes the decryption function to decrypt the ciphertext of symmetric key. Data user uses symmetric key to retrieve the original data.

5. Revocation

Data owner acknowledge third party authorization and cloud that one attribute has been revoked from specific data user third party authorization .update information in database. Data marks the corresponding bit of attribute description field of data files.

V. RESULT

When data owner sharing data files to the specified users, these file are to be encrypted using symmetric key, then the symmetric key also encrypted by Attribute based encryption. however the size of the data files remain same it is only required to measure the size of the symmetric key. Results represents that data sharing scheme reduces the computational overhead and storage overhead compared to the normal attribute based encryption on client side.

Table 5.1 Computation Overhead Of Basic Operation Of Attribute Based Encryption Methods

Devices	Pairing	Exponentiation	Multiplication
Desktop	18ms	4ms	0.5 ms
Mobile	500ms	150ms	22ms

Table 5.2 Computation Overhead Of Basic Operation Different Attribute Based Encryption

ABEs	PK	MK	SK	CD
BSW[30]	3 $MG0+$ $LG1$	$Mz+$ $LG0$	(2|Au|+1) $MG0$	(2|Ta|+1) $MG0+$ $MG1$
Waters[40]	(|A|+2) $MG0+$ $MG1$	$MG0$	(|Au|+2) $MG0$	(2|Ta|+1) $MG0+$ $MG1$
DS	3 $MG0+$ $LG1$	$MG0$	(|Au|+4) $MG0$	(2|Ta|+3) $MG0+$ $MG1$

PK:Primary Key

A:Number of attributes of owner

MK:Master Key

Au:Number of attributes of user

SK:Symmetric key

CD:Ciphertext Data

Ta:number of nodes in control tree

DS:Data Sharing

MG0,MG1,Mz:Size of an element in G0 ,G1,Zgroup

VI. CONCLUSION

As we know that there are limited resources provided to mobile devices and the traditional algorithm is not fit for mobile cloud. To adress this problem defined method light weight data sharing scheme algorithm to relocate computational overhead on proxy servers from mobile device this will secure data sharing scheme using mobile cloud . This work concludes that the data sharing method provide privacy and data security in mobile cloud as well as data user side, it reduces overhead in mobile cloud by using lazy revocation.

REFERENCES

1. Jing-yi Fu, Qin-long Huang, Zhao-feng MA. Securpersonal data sharing in cloud computing using attribute-based broadcast encryption:Elsevier,2014.
2. Ruixuan LI, chengling shen,Heng he.a light weight secure data sharing sheme for mobile cloud computing: IEEE Transaction on cloud computing. ,vol 6,issue 2,2017.
3. Brakerski Z, Vaikuntanathan V Efficient fully homomorphic encryption from LWE. In : Proceeding of IEEE Symposium on Foundations of computer science California, USA : IEEE press, pp. 97-106, oct. 2011.
4. Qihua Wang, Hongxia Jin. "Data leakage mitigation for discretionary access control in collaboration clouds". The 16th ACM Symposium on access control models and technologies (SACMAT), pp.103-122, Jun. 2011

AUTHORS PROFILE

Santosh S.Chinchalli ,B.E(CSE),M.TECH(CSE), Assistant Professor
Department of Information Science and Enginnering, V.P.DR P.G.Halakatti College of Engineering and TechnologyVijayapura,India.
Web technology and computer networks are most interested subjects with 10 years of teaching experience, research areas: image processing, computer Networks

Shivakumar K. Honawad B.E(ISE),M.TECH(CSE), Assistant Professor
Department of Information Science and Enginnering, V.P.DR P.G.Halakatti College of Engineering and TechnologyVijayapuraIndia.
Automata theory and file structures are most interested subjects with 10 years of teaching experience, research areas: image processing,cloud computing