RESEARCH ARTICLE OPEN ACCESS

Hierarchical Identity Based Encryption for Mobile Cloud Computing Using Lightweight Data Sharing Scheme

*Boobalan. P, **Anand.B, ***Gunalini.B, ****Ilakkiya. P

*(Associate Professor, Information Technology, Pondicherry Engineering College, Pondicherry)
** (Information Technology, Pondicherry Engineering College, Pondicherry)
*** (Information Technology, Pondicherry Engineering College, Pondicherry)
**** (Information Technology, Pondicherry Engineering College, Pondicherry)

----------**********----------

Abstract:

With the event of cloud computing and therefore the quality of sensible mobile devices, folk's area unit step by step obtaining aware of a replacement era of information sharing within which the information isstored on the cloud and therefore the mobile devices area unit accustomed store/retrieve the information from the cloud. Typically, mobile devices solely have restricted space for storing and computing power. In this paper, we describe the Lightweight Data Sharing Scheme (LDSS) system design. First, we give the overview of LDSS, and then we present LDSSHierarchical Identity Based Encryption(HIBE) algorithm and system operations, which are the base of the LDSS algorithm. Finally, we describe LDSS in details. In LDSS, the proxy encryption server and proxy decryption server are introduced to assist users to encrypt and decrypt data so that user-side overhead can be minimized. In essence, proxy servers are machines within the cloud. Thus, we have a tendency to take into account that they're honest however curious even as the Cloud Service Provider (CSP).

Keywords **—HIBE, MOBILE COULD COMPUTING, DATA ENCRYPTION, LDSS,CSP.**

----------**********----------

I. INTRODUCTION

Versatile processing is human– PC collaboration by that a compact PC is required to be transported all through old use that takes into account transmission of learning, voice and video. Mobile computing takes present in mobile communication, mobile hardware, and mobile software. The advancement of distributed computing and the ubiquity of shrewd cell phones, individuals are bit by bit getting acclimated with another period of information sharing model in which the information is put away on the cloud what's more, the handsets are utilized to store/recover the data from the cloud. Commonly, cell phones just have constrained storage room and figuring power. On the contrary, the cloud has massive amount of resources. In such a condition, to accomplish the tasteful execution, it is fundamental to utilize the assets gave in the cloud dedicated co-operation (CSP) to stock and offer the information. These days, different cloud

versatile claims have been generally utilized. In these applications, individuals (information proprietors) can transfer their photographs, recordings, reports and different documents on the cloud and share these data with different people (data customers) and they get a boost out of the opportunity to share. CSPs additionally give information usefulness to data managers to access. Since individual information documents are touchy;information proprietors are permitted to pick whether to make their information records open or must be imparted to particular information clients. Plainly, information protection of the individual sensitive information may be a major worry for a few information proprietors.

II. EXISTING SYSTEM

In existing system the lightweight data sharing scheme (LDSS) for mobile cloud computing adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to form it appropriate for mobile cloud environments.LDSS moves an outsized portion of the machineintensive access management tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to scale back the user revocation price, it introduces attribute description fields to implement lazy-revocation that could be a thorny issue in programmingwhich is based on the CP-ABE systems.Furthermore, to reduce the user revocation cost; it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems.

III. DISADVANTAGES OF EXISTING SYSTEM

The user feels complex to search the encrypted data in cloud. Because the data owner uploads the data in encrypted form without the user's knowledge hence the user feels it difficult to search.Multi-user cannot access the file at same time, access can be provided only to single user.Non-efficiency and non-existence of attribute revocation mechanism.

IV. PROPOSED SYSTEM

In the proposed system, a lightweight data sharing schemeis used for mobile cloud computing. It adopts the Hierarchical Identity Base Encryption scheme that can be used to perform search on encrypted data, forward secure encryption, fully private communication, limited delegation and damage control. In specific, email addresses and dates may be public keys. It is the system which allows any party to generate a public key from a known identity value such as an ASCII string, or any numbers etc. A trusted third party or data owner called the Private Key Generator (PKG) generates the corresponding private keys. LDSS moves a large portion of the computational intensive access control tree transformation in IBE from mobile devices to external proxy servers.

V. ADVANTAGES OF PROPOSED SYSTEM

The advantages of this project are the user sent the data efficiently with secured multi keyword searching scheme. Not only single user, multi user can access the file at same time without any distractions.HIBE can simplify system that

manages a large number of public keys rather than sorting database of public keys.

VI. IMPLEMENTATION

The data owner outsources the data to the cloud for convenient and reliable data access to the corresponding search users. After that, the data owner sends the encrypted documents and the corresponding indexes to the cloud, and sends the symmetric key and secret key provided by Identity based encryption. The cloud server associate intermediate entity that stores the encrypted documents and corresponding indexes that square measure received from the information owner, and provides data access and search servicesto search users. The search user receives each the key and even key from the information owner. According to the search keywords, the search user uses the secret key to generate trapdoor and sends it to the cloud server. The data user receives the matching document collectionfrom the cloud server and decrypts them with the even key.

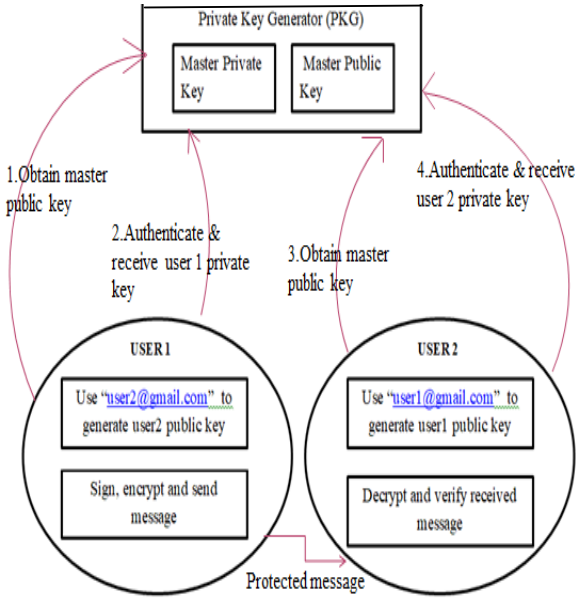

Fig.PRIMARY KEY GENERATOR DIAGRAM

VII. MODULE DESCRIPTION

The LDSS scheme is designed for data sharing in the mobile cloud. The whole process of LDSS includes system initialization and network formation of data user and data owner, generation of attribute key for data user, decryption of cipher text, asynchronous preprocessing of attribute revocation, document updating by lazy revocation and self - destruction scheme. It also has to support attribute revocation and file update operations.

1. DATA OWNER / DATA USER NETWORK FORMATION

Data owner encrypt the plain text into encrypted format and upload it to the cloud. The encryption is done by using a password. By using this password anyone can decrypt the text. The user will upload the password and also include the encrypted data.

The trusted authority id responsible is for passing the password to the requested user. To improve the search potency, the information owner generates some keywords for every outsourced document. The corresponding index is then created according to the keywords and a secret key. After that, the data owner sends the encrypted documents and the corresponding indexes to the cloud, and sends the symmetric key and secret key provided by Identity based encryption.

2.GENERATION OF ATTRIBUTE KEYS FOR DATA USER

Any user can view the file uploaded in the server all the files are in encrypted format. Users can't view the files without knowing the password. To view the file, first user needs torequest the password to Trusted Authority (TA). The Authority checks the user and provides the password if the user is valid. TA compares the attribute description field in the attribute key with the attribute description field stored in the database. For each inconsistent bit in the description field, if it is 1 on data user's side and 0 on TA's side, it indicates that Data User (DU) attribute has been revoked, and then TA does nothing on this bit. If it is a reversed scenario, which indicates that DU has been assigned a new attribute, then TA generates the corresponding attribute key for DU.TA checks the version of every attribute key of DU. If it's not the same with the current version, then TA updates the corresponding attribute key for DU.

3.DECRYPTION OF CIPHER TEXT

Data user sends a request for data to the cloud.Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses the request, otherwise itsends the ciphertext to DU. DU receives the ciphertext, which includes ciphertext of data files and ciphertext of the symmetric key. Then DU executes the decryption function to decrypt theCipher text of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the cipher text of data files.

4. ASYNCHRONOUS PREPROCESSING OF ATTRIBUTE REVOCATION

Data owner can revoke attributes from Data user. DO informs TA and the cloud that one attribute has been revoked from a specific DU. TA and the cloud update the information of DU in the database.DO marks the corresponding bit of the attribute description field of data files. This strategy implements the asynchronous processing of attribute revocation and attribute keys update operations. When DO want to revoke one attribute from a DU, TA only updates the database and doesn't update attribute keys for DU simultaneously.

5.DOCUMENT UPDATION BY LAZY REVOCATION

As a result of lazy re-encryption, when DO revokes one attribute from a DU, the revoked attribute is not updated. When the data file is updated, if it has one attribute that has been revoked, this attribute should be updated. DO checks if there is any bit in the description field of data files. DO inform TA which attributes should be updated. TA chooses a new value for every attribute to replace the original one, and updates the description field of DO in DO-

Primary key (PK) or Master key(MK) table, changing the corresponding attribute description bit to the new value. TA sends a new PK to DO, and DO uses the new PK to encrypt data files.

6. SELF DESTRUCTION SCHEME

Every cipher text is labelled with a time interval while private key is associated with a time instant.When the user gets far from the organization then the revocation takes place and key gets updated to producesecurity. The suicidal themeis enforced to delete the files mechanically when completion of your time span.In the Self Destruction Scheme (SDS) scheme, a data is encrypted into a cipher text, which is then associated and extracted to make it incomplete to resist against the traditional cryptanalysis and the brute-force attack. Then, both the decryption key and the extracted cipher text are distributed into a distributed hash table (DHT) network to implement self-destruction after the update period of the DHT network.The main idea of the above-mentioned schemes is that they respectively combine different cryptographic techniques with the DHT network to provide fine-grained data access control during the lifecycle of the protected data and to implement data self-destruction after expiration.

.

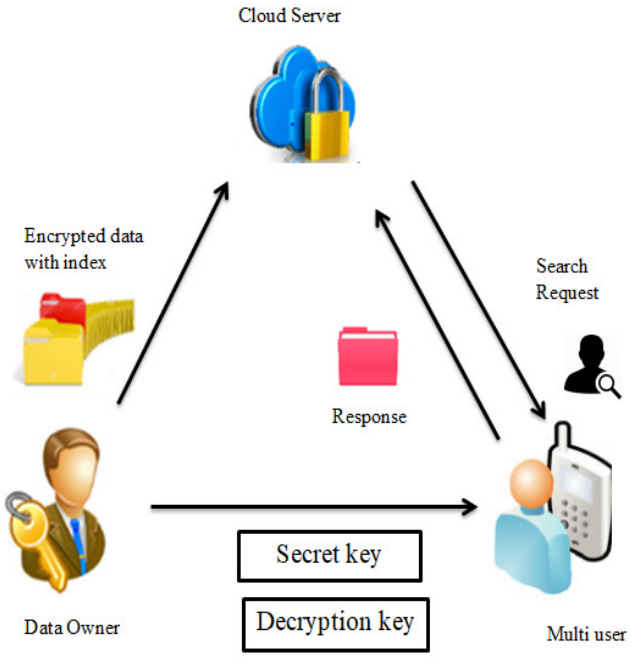

Fig.ARCHITECTURE DIAGRAM OF HIBE

VII. CONCLUSION

However, ancient ABE isn't appropriate for mobile cloud as a result of its computationally intensive and mobile devices solely have restricted resources. Focus on the issue of data access control in the cloud.Theyare principally for non-mobile devices and can't be applied for knowledge sharing in mobile cloud setting. Regarding to data privacy in mobile cloud, some works have been done in this field. In this paper, we tend to propose LDSS to handle this issue. It introduces a novel LDSS- IBE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud.

VIII. REFERENCE

[1] RuixuanLi ,Chenglin Shen, Heng He, XiwuGu, Zhiyong Xu, and Cheng-Zhong Xu, *"A Lightweight Secure Data Sharing Schemefor Mobile Cloud Computing"*. IEEE(2018).

[2] Yu Jin, Chuan Tian, Heng He and Fan Wang.*"A Survey of Security and Privacy Challenges in Cloud Computing."*IEEE Fifth International Conference on Big Data and Cloud Computing.

The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. Hierarchical access control has good performance in reducing the overhead of key distribution in cipher text access control. All the above works will

[3] Princy P. James, Renuka Ajay Sonone, Naveen Ghorpade, Reddy Kumar.*"An Efficient Lightweight Secure DataSharing Scheme for Mobile CloudComputing"* in International Journal of Innovative Research in Science, Engineering and Technology,(2018).

[4] Madhavi Langute , H. A. Hingoliwala, "*Survey: Identity- Based Encryption in Cloud Computing*" International Journal of Science and Research (IJSR),(2018).

