IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10721

SECURING PRIVACY FOR REMOTE DATA IN A CLOUD STORAGE

Chiranjeevi P[1], Dharani NV[2]

Department of MCA, Dr.Ambedkar Institute of Technology, Bengaluru, India[1]

Assistant Professor, MCA, Dr.Ambedkar Institute of Technology, Bengaluru, India[2]

Abstract: The cloud data storage service plays a major role in a day to day life. Many scientists have noticed about secure search over encrypted information. The main target of this service is to promise the secrecy of the information stored in the cloud server. However, the huge data stored in a cloud are protected using various privacy and security algorithm. In this regard, to handle the security concerns, it is desirable to deploy sensitive information in encrypted structure. Encrypted information storage protects the information against illegal access. It includes much basic and fundamental functionality such as the search on the information. The searching Handled by keywords is made by two to more keywords to be added. In this proposed project, we have used one of the privacy and preserving encrypted multi-sharing mechanism to achieve the searching.

The merit of re-encryption with unnamed method in which an encrypted can be shared multiple times without revealing both the knowledge of elementary message & the uniformity data of cipher text senders/receivers.

Keywords: privacy, security, re-encryption, cloud computing.

I. INTRODUCTION

In recent years and research, Information storage in an organization and storage medium. It’s very necessary, there are various storage devices to store data. Hard drives are the one of most commonly used. But data in the organization has to be maintained for a longer phase. Hard drives and other storage devices are not safer for a longer interval, cloud is the solution. Storing the data in the cloud is the safest place for keeping the files and data for future use. But, how safe are the files is very important. Cloud providers will have easy access to the data of their clients.

In order to keep files safe from intruders, the data can be encrypted.

II. LITERATURE SURVEY

Many scientists have noticed about secure search over encrypted information. Song et al [1], was one to solve the issue of secure search over encrypted information.

They have suggest the some pattern of searchable encryption, which is a JCE primitive that enable users to act upon a keyword-based search mechanism on encrypted information, just as on plaintext information. Keyword-based search mechanism over encrypted cloud information is first defined [2]. This study does not only shrink the computation and storage rate for keyword based search mechanism over some encrypted cloud information, but it also enriches the cluster of search function, including ranking based multi keyword search mechanism, fuzzy keyword based search mechanism and similarity searching mechanism.

The data and information which is stored in the cloud is becoming more popular now a day’s and the usage of these services are rapidly increasing. This service’s is increased due to the presentation of new networking technologies. In that case we can notify that data is the main component of the clouds services. And there is many other services are there that is having elevated intention to utilize the faster networks.

Now it’s very important to have secure tools for the cloud service. The huge amount of data is required to manage the different features of facts. The sized of the data impact on the price of the clouds service. The level of storing is raised according to the value of the data stored.

Disadvantages:

- The security is low.
- The performance and efficiency is less.
- There is chance of leakage of data.

DOI 10.17148/IJARCCE.2021.10721

III. PROPOSED SYSTEMS

In this proposed paper, we aim to suggest a ranking based multi keyword search mechanism over encrypted information with the following properties:

1. **Public-Key Cryptography**
2. **Administrator**

Public-Key Cryptography

In this proposed project, the public-key cryptography includes two types.

i. **Public Key**
ii. **Private Key**

Public Key is used for encryption of data while uploading file to cloud server and decryption while downloading data. There the data owner uses the public key to carry out the encryption, but when it comes to private key it is kept private from the user or receiver.

This type of cryptography is also called as “asymmetric key algorithm.”

Administrator

In this proposed project, Administrator allows new data owners to register for this technique without affecting other owners or users, i.e., the propose project helps data owner scalability in a plug-and-play model.

***Achievements*:** We study a new concept, **PRMSM**. We summarize the definition and security model. In the security model, we allow the data owners to register without affecting other registered data owners. Once administrator approver’s the owner. He/she will receive the username and password to this registered email id. Once data owner login is successful. Owner can upload the file or data along with file name and keywords. Once the file is successfully uploaded to a cloud server encrypted files can't be read until it has been converted into plaintext (decrypted) with a decryption key. It will be encrypted with some encryption algorithm **JCE** (Java Cryptography Extension) and different keys for different data owners in cloud storage. So that it prevent from leakage of the information in cloud storage and illegal access of the stored information.Further coming to users. Once administrator approver’s the user. The registered data user will receive the username and password to this registered mail id. In this scheme only verified data users can act upon some accurate searches, he can search using specified keywords or a file name. Once the legal user act upon his search. The secret key on the administrator region will be changed, there will be contradictory secret keys between the administrator and the legal users. Therefore, the user and administrator will soon identify this illegal activity, when user done with a required accurate search, the request for the document download permission will be sent by the respective owner.If user is cancelled by an administrator, user can not longer act upon correct searches over the encrypted cloud files or information.When owner approver’s the request sent by a user’s, conditional data sharing, the requested user will receive a decryption key to this registered a mail id. Using that decryption key the user can download and decrypt the document or file.
So that it prevent from illegal access and leakage of the information which are stored in the cloud server storage.

IV. SYSTEM REQUIREMENT

In the primary block, we have developed the Scheme Model to put into practice our proposed system. Our scheme model involves Administrators, Users, Data Owners, and Cloud Service Providers.

A. Administrator

An administrator grant sign-in credentials to both owners and Users. Initially, the new end-users need to register themselves by providing necessary details and the Administrator approves each end-users request. The individual sign-in credentials will be sent to the registered Email ID of the both Data owner and users.

B. Data-User

In the Users sub-block, each user has to sign on with the individual sign-on credentials granted by the administrator in the system. The user prospects their profile. The user can act upon some accurate searches, he can search using specified keywords or a file name. Once the legal user act upon his search. The secret key on the administrator region will be changed; there will be contradictory secret keys between the administrator and the legal users. If the user needs

DOI 10.17148/IJARCCE.2021.10721

to download the file. He needs to obtain a decrypt key enclosed with its impute entitled by the matching impute data owners, i.e., the scheme should carry owner adaptability in a plug-and-play model.

C. Data-Owner

In the Owner's sub-block, the proposed scheme should accept new owners to register themselves by providing necessary detail in this proposed system without affecting other owners.

D. Cloud Service Provider

In the Cloud service provider sub-block of the scheme model, the owner uploads the encrypted data to the cloud server storage through the Administrator.

Owners do not rely on the cloud server to do information access control. But, access controls occur inside the Java cryptography Extension. That is only when the user's imputed satisfying the access protocol. The user can decrypt the encrypted file using some decryption key. Thus, users with different impute can decrypt several keys and thus obtain different granularities of information from the same data or information.

E. End-users Verification.

To keep away from cyber-riders from acting to be legal data users performing some searches. Users must be verified before the administration server re-encrypts keys for data users. Our scheme follows some techniques. First, the information requested is to send a request to respected owners and owners to share a decryption key. Second, the requester decrypts the information using the decryption key.

F. Unauthorized Search mechanism Detection.

In our scheme, the verification process is protected by public-key cryptography. We assume that an attacker has successfully attacked the decryption key. Then he has to set up the verification information; if the attacker has not successfully on the data, e.g., the request counter, the last request time, he cannot set up the correct verification information.

Therefore this illegal activity will soon be detected by the administrator server.

V. SYSTEM USE CASE DIAGRAM:

A use case graph is to-be realized the behavior of project. The goal behinds this graph chart is to display the whole capacity of a project for which on screens charter is to be display. It demonstrates assignment among the client and the capacities and their relationships as shown in figure 1.

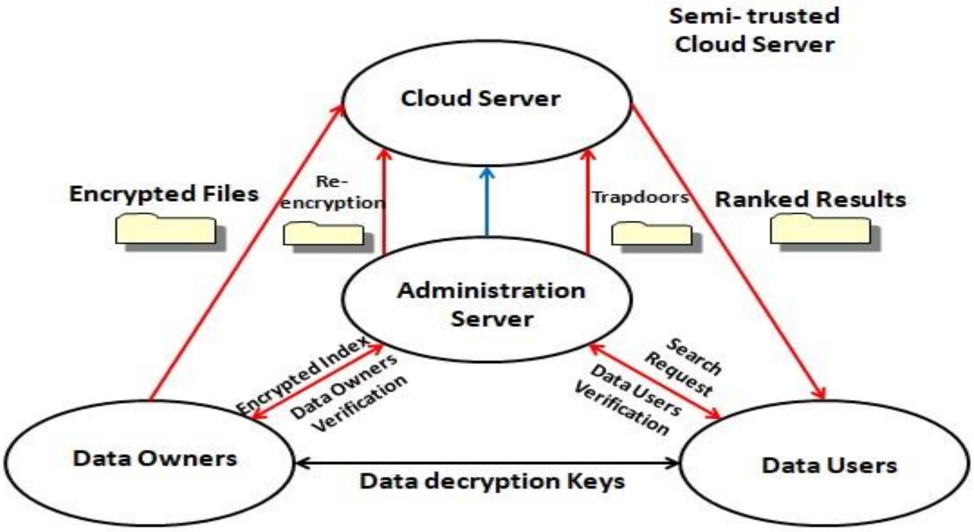

Fig 1: Use case diagram for the proposed system.

DOI 10.17148/IJARCCE.2021.10721

VI. CONCLUSION

This proposed project grants to providing security to the information stored in the cloud computing, by encrypting the information before uploading it into the cloud computing. As encryption technique consumes more processing overhead, many clouds computing service providers will have basic encryption applied only on few data or information fields. If cloud computing service providers can encrypt information, then cloud computing service can providers can decrypt encrypted data. To keep the cost low and maintain highly sensitive data, it would be better to encrypt the data before uploading. In this project, we encrypt information using symmetric key encryption where private keys to the document will be stored in the local database. The system generates an odd key for accessing multiple files or stored documents.

This Access key is stored in the cloud storage is which further helps to retrieve or access private keys that are stored in the local database. As an odd key is stored in the cloud storage for multiple files or documents, flexibility will be increased for sharing n number of files, the cost for key management will be minimized.

In the future, Access key generation can be increased. If the Access key itself decrypts the files or documents requested, it would minimize the maintenance of private keys in the local database. Document Modification techniques without downloading the document can be improved. The encryption

Technique can be increased further.

VII. REFERENCE

[1] G. Ateniese, K.Fu, M. Green and S. Hohenberger. Improved proxy re-encryption scheme with applications to secure distributed storage. ACM TISSEC, 2006.

[2] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption, 2004.

[3] R. Canetti and S.Hohenberger chosen-ciphertext secure proxy re-encryption. ACM, 2007.

[4] G. Ateniese, K. Benson, and S. Hohenberger. Key-private proxy re-encryption, 2009.