**Algorithm for Multi Keyword Search over Encrypted Data in Cloud Environment**

**ABSTRACT:-**

Cloud Computing offers storage resources as well as network and computing resources to the organizations. This eliminates the high infrastructure cost for the organizations that are using these services as they can now dynamically pay for these services, i.e., pay per use model, which is followed by most of the cloud providers. As the organization does not locally host these resources, these are comparatively far easier to manage and use than the traditional infrastructural resources. As a result of these factors, the popularity of cloud computing is increasing continuously. But this transfer of data and applications to the cloud server also creates some challenges. It poses problems that must be dealt with properly to ensure a secure cloud computing environment. As more and more sensitive data is being uploaded on the cloud in the present scenario, the privacy and security concerns associated with the data is continuously increasing. To address this, issue the data is stored on the cloud in the encrypted form. Also, as the amount of data stored is usually tremendous, so an efficient search scheme is also necessary. So here, we deal with two significant aspects of cloud computing: Encryption and Searching. We are proposing a secure and efficient encryption scheme to encrypt the data stored in the cloud as well as the queries along with a multi-keyword search scheme to search over the encrypted cloud data.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The cost and implementation advantages offered by cloud computing are enormous. Due to these advantages, both individual users and the enterprise users are increasingly outsourcing the data to the cloud, instead of spending a significant amount in procuring the required hardware themselves. Despite the many distinct advantages of cloud computing, some concerns are also there. * Sensitive and personal information of people such as medical records, bank records, private photos are outsourced and stored on a cloud, which causes privacy concerns. | * In this paper, we propose a secure tree-based multi-keyword ranked search scheme over encrypted data, and dynamic operation on the document collection. As more and more sensitive data is being uploaded on the cloud in the present scenario, the privacy and security concerns associated with the data is continuously increasing. * Also, The data is stored on the cloud in the encrypted form. |
| **EXISTING ALGORITHM**  Lightweight cryptographic algorithms (DES) | **PROPOSED ALGORITHM:-**  AES,RSA & SHA algorithm |
| **ALGORITHM DEFINITION:-**  The cloud service provider, which is storing this sensitive data, may access it without the requisite authorization. Therefore, to protect data confidentiality, data is encrypted before outsourcing. However, this gives rise to some significant problems. Most of the keyword-based retrieval techniques, which work very efficiently on plain text data, cannot be applied at all on the cipher text. Downloading all the data on the cloud, decrypting it, and then searching is logistically impractical. | **ALGORITHM DEFINITION:-**  In this paper, we propose an encryption scheme that uses a combination of all three algorithms to encrypt the data and make sure the transfer has taken place correctly. In this paper, we have used SHA as our hashing algorithm. It is the most recent and secure hashing algorithm. We are proposing a secure and efficient encryption scheme to encrypt the data stored in the cloud as well as the queries along with a multi-keyword search scheme to search over the encrypted cloud data. |
| **DRAWBACKS:-**   * Less Security. * Confidentiality for data is not there. * Causes Privacy concerns | **ADVANTAGES:-**   * High Security. * Provides high confidentiality. * Overcomes the privacy concerns problem. |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE