CONFIDENTIAL DATA SHARING WITH RANKED QUERY OVER ENCRYPTED CLOUD DATA

Mr.S.S.Aravinth / AP / CSE / Knowledge Institute of Technology, Salem
Mail ID: ssacse@kiot.ac.in   Mobile No: 98944 – 48683
Mr.S.Sakthivel / ASP / CSE / Knowledge Institute of Technology, Salem, sscse@kiot.ac.in
Ms.S.Kiruthika/ AP / CSE / Knowledge Institute of Technology, Salem
Ms.S.S. Kiruthika / AP / CSE / Knowledge Institute of Technology, Salem
Mr.M.Ramkumar/ AP / CSE / Knowledge Institute of Technology, Salem

ABSTRACT

Cloud Computing is a new paradigm for the provisioning of every network available resource(X) as a service (Xaas). In these services provided by cloud, we consider Storage-as-a-Service. Storage-as-a-Service offered by cloud computing allows the user to outsource their sensitive data on cloud servers. When the users are outsourcing their data on the cloud, they want their data to be guaranteed with Confidentiality, Integrity and proper access control. In the present work we focus on a cloud based storage system where users can benefit from the facilities offered by the Cloud Service Provider (CSP) and enables indirect mutual trust between them. Four main features of the proposed scheme are i) the data owner i.e., user can store their sensitive data on cloud server and allowed to perform full block level dynamic operations on the stored data. The dynamic operations include block modification, insertion, deletion, and append ii) it enables the authorized users (i.e., group members of data owner who have the privilege to access data owner's file) to receive the last modified content of the stored data on cloud iii) it enables indirect mutual trust between the owner and the CSP, and iv) the owner is allowed to grant or revoke access to the stored data on cloud. The proposed design supports productivity and efficient activities, including block modification, deletion and append. The proposed system is very effective against data modification attack.

KEYWORDS: CLOUD, SECURITY,ENCRYPTION AND SHARING

1. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is a believing paradigm, where a enormous pool of systems are connected in private or public networks, to provide dynamically accessible infrastructure for application, data and file storage. With the arrival of this skill, the cost of computation, application hosting, comfortable storage and delivery is reduced significantly. It is a practical method for direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable appreciated environment. The responsiveness of cloud computing is based on a fundamental principle of IT capabilities. The difference that brings compared to traditional concepts of grid computing, distributed computing, utility computing or autonomic computing is to increase horizons across organizational boundaries.

1.2 TYPES OF CLOUD COMPUTING

Initiatives can choose to organize applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in responsible the accurate cloud path for each organization.

1.2.1 PUBLIC CLOUD

Public clouds are preserved and functioned by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a combination of users, giving each individual client an attractive low-cost, Pay-as-you-go model. All customers portion the identical organization pool with limited configuration, security protections, and availability variances. These are achieved and supported by the cloud provider. One of the advantages of a Public cloud is that they may be in excess of an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

1.2.2 PRIVATE CLOUD

Private clouds are built entirely for a single enterprise. They aim to address concerns on data security and offer greater control, which is naturally lacking in a public cloud. There are two variations to a private cloud.

On-premise Private Cloud:

It is also known as interior clouds are hosted within one's own data center. This model provides a more consistent process and protection, but is restricted in

aspects of size and scalability. IT departments would also need to earn the capital and active costs for the physical resources. This is best suited for applications which need complete switch and configurability of the arrangement and security.

Externally hosted Private Cloud: The private cloud is hosted outside with a cloud provider, where the provider facilitates an exclusive cloud environment with full assurance of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources.

1.2.3 HYBRID CLOUD

Hybrid Clouds combine together public and private cloud models. It is a service providers can utilize third party Cloud Providers in a full or incomplete manner thus increasing the flexibility of computing. The Hybrid cloud environment is accomplished of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the incomes of a public cloud can be used to manage any unpredicted surges in workload.

1.2.4 COMMUNITY CLOUD

In a community cloud, the service is common by several organizations and

made accessible only to those groups. The infrastructure may be maintained and worked by the administrations or by a cloud service provider.

1.3 DATA SHARING IN CLOUD

Privacy and Confidentiality of data in Health care:

In the environment of healthcare, patients description their health-related information to healthcare professionals in order to diagnose and treat illnesses. The Health Insurance Portability and Accountability Act (HIPAA) provides federal protection of an individual's personal health information. The HIPAA Privacy Rule provides safety of patient personal health information and external individuals such as doctors and nurses can rise access to the patient's data with the patient's approval. As argues, since the patient decides to share their data with one or more healthcare professionals and their data is no lengthier private, but it is more secured.

Privacy and Confidentiality of data in Social Networking:

Social networking has changed the lives of today's generation. There are many social networking sites with millions of

users communicating with each other. Some examples are Facebook, Twitter, MySpace, Blogger, and Flickr. Privacy has been determined as the right to be left alone. The technology that is built to support social networking does not effectively support privacy and may even sell personal information about the individual to third parties and it is mainly up to the individual to disclose information while maintaining privacy. The individual needs to make sure that they do not unknowingly disclose personal information about themselves. Simply disclosing their age, suburb and nationality is enough for malicious users to identify the person. Facebook had undergone scrutiny in the past for not strengthening its privacy measures on user profiles as private photos could still be viewed by non-private viewers through a friend-of-a-friend by simply having a friend comment on it .

2. SYSTEM ANALYSIS
2.1 EXISTING SYSTEM

The huge number of data users and documents in cloud, it is critical for the search to permit multi-keyword query and deliver result similarity ranking to meet the actual records retrieval need. The searchable encryption focuses on solitary keyword search or Boolean keyword search, and rarely differentiates the search results. The drawbacks of existing system are Single-keyword search without ranking. Boolean-keyword search without ranking. Single-keyword search with ranking.

2.2 PROPOSED SYSTEM

We define and solve the interesting problem of privacy-preserving multi-keyword graded search over encrypted cloud data (MRSE), and establish a set of severe privacy requirements for such a secure cloud data utilization system to become a reality. Among several multi-keyword semantics, we choose the capable principle of organise matching snapshot. Access either displays the snapshot for us to view or achieve an action on it, such as deleting or updating.
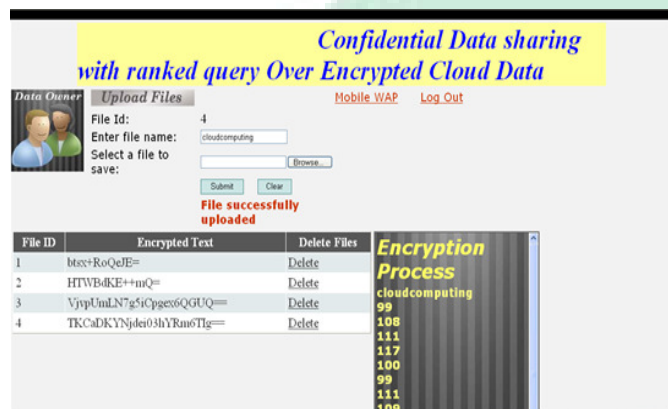
ARCHITECTURE

Fig 1 Cloud Architecture
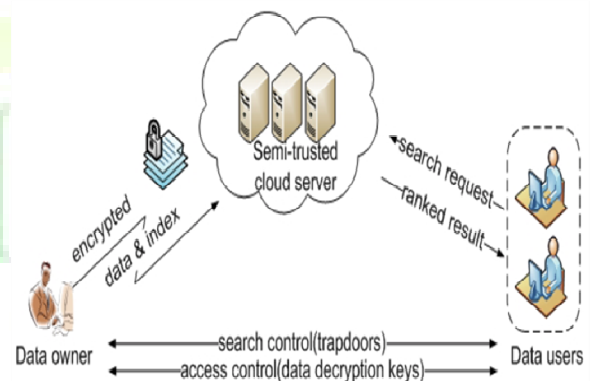
# 3. MODULE DESCRIPTION
3.1 MODULES

1. Encrypt Module:

It used to support the server to encrypt the data using RSA Algorithm and to convert the encrypted data into Zip file with activation code and then code is send to the user for download.

2. Client Module:

Client module is focusing on client to search the file using the multiple key words concept. The result will be more accurate based on the user query. The user is accepted to select the required file and register the user details to get code via mail from the customer service404 email before enter the activation code. After user can download the Zip file and remove that file.
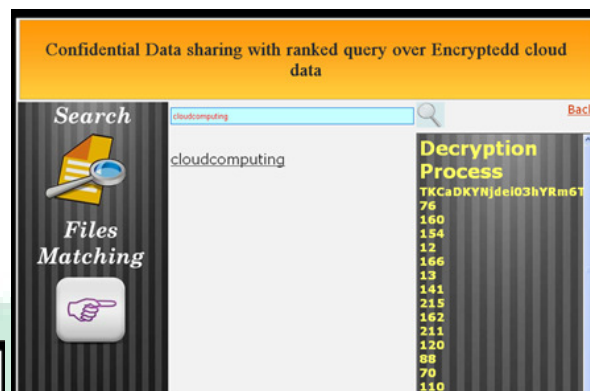
3. Multi-keyword Module:

This module is obtained accurate result from the multiple keyword concepts to help the user. While user can enter the query,

the server is going to split into a particular word after search that word file in our database like priority based . Finally, display the matched word list from the record and the user gets the file from that list.

4. Admin Module:

This module is created for server Especially, to view the details and upload files with the security. Admin customs the log key to the login time. Before the management logout, alteration of the log key is required. The admin can change the password after the login and understanding the user downloading required details and the counting of file request are mentioned on flowchart. The admin can upload the file after the translation of the Zip file format.

4. CONCLUTION:

Cloud Computing is the emerging trend in today's IT industry. The services offered by various cloud providers are getting a deeper insight by industries. This paper helps to the cloud computing researchers in the area of cloud security. In near future, the sharing of steganography based image hiding techniques along with Fourier series will be accounted

REFERENCES:

1. Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145.
National Institute of Standards and Technology, U.S. Department of Commerce. Source: http:// csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Accessed on Oct 2012
2. Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud_computing. Accessed on Oct 2012
3. HealeyM(2010) Why IT needs to push data sharing efforts. InformationWeek. Source: http:// www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/ 225700544. Accessed on Oct 2012
4. Gellin A (2012) Facebook's benefits make it worthwhile. Buffalo News.
5. Riley DA (2010) Using google wave and docs for group collaboration. Library Hi Tech News.
6. Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona State