International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Secure and Efficient Data Retrieval in Cloud Computing

Anuradha N. M
Student, ME (CSE)-II,
D.Y.Patil College of Engineering and Technology,
Kolhapur, Maharashtra.

G. A. Patil
Head and Associate Professor of Computer Science Dept,
D.Y.Patil College of Engineering and Technology,
Kolhapur, Maharashtra.

***Abstract*— In Cloud computing, cloud customers can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. The fact that data owners and cloud server are no longer in the same trusted domain may put the outsourced unencrypted data at risk. It follows that sensitive data has to be encrypted prior to outsourcing for data privacy. However, data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data files. Also outsourcing data to the cloud causes loss of control over data on a data owner's part. This loss of control over data is further intensified with the lack of managing users' access to the data from practical cloud computing perspectives. We address these challenging issues using Ranked Searchable Symmetric Encryption Scheme.**

***Keywords- Cloud computing, secure data access, keyword search*.**

I. INTRODUCTION:

Cloud storage services allow the users to outsource their data in the cloud storage servers and retrieve them whenever and wherever required. This avoids the cost of building and maintaining their data store. But the users need to provide privacy for the data and also to be able to search it without losing privacy. The users always search their documents through keyword in plaintext, which may leak privacy of users in cloud storage environment. So allowing a cloud service provider (CSP), whose purpose is mainly for making a profit, to take the custody of sensitive data, raises underlying security and privacy issues. To keep user data confidential against an untrusted cloud, a natural way is to apply cryptographic approaches, by disclosing the data decryption key only to authorized users. In this paper we propose an efficient, secure and privacy preserving keyword search scheme which supports multiple users with low computation cost and flexible key management.

II. RELATED WORK:

A number of different mechanisms have been proposed for security aspects in cloud computing. Some of the researchers have suggested the following strategies to support secure access in cloud computing.

1. Cong Wang, Ning Cao, Kui Ren, Wenjing Lou [1] addresses Ranked Searchable Encryption technique that allow users to securely search over encrypted data through keywords. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. But here efficiency of data retrieval is preferred more over security and authorization of users is not mentioned.

2. Mahbub Ahmed, Yang Xiang [2] introduce a new mechanism of ensuring trust and security in Software as a Service (SaaS) CC. Trust Ticket mechanism is used that helps a data owner in establishing a link between a CSP and a registered user. Thus gain control over data by managing users' access to the data on cloud. The algorithmic protocol for Trust Ticket deployment establishes a data owner's trust. This trust is established through a data owner's control over data and a registered user; because a registered user is linked with a CSP by a data owner through Trust Ticket. Management of Trust Ticket is not mentioned.

3. Boneh D, Crescenzo G, Ostrovsky R, Persiano G [3] introduce a Public key encryption with keyword search that enables the service provider to determine whether a document contains a specified keyword without getting any information about the document or keyword. It supports multi user requirements with user authentication and also avoids statistical attack on keywords. It also enables the service provider to participate in partial decipherment thus reducing the users computational overhead. In this scheme, user authentication is provided before giving the secret key for decryption of document. Here when a user is revoked, all the documents in which the user has access needs to be re encrypted. This introduces heavy computation overhead for the owner of the document.

III. OBJECTIVES:

To enable ranked searchable symmetric encryption for effective utilization of outsourced and encrypted cloud data under the proposed model, our system design should achieve the following security and performance guarantee. Specifically, we have the following goals:

1. Ranked keyword search: to explore mechanisms for designing effective ranked search schemes.
2. Security guarantee: to prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the "as-strong-as-possible" security strength.
3. Efficiency: above goals should be achieved with minimum communication and computation overhead.

III. PROPOSED SCHEME:

The proposed system architecture consists of three entities:

1. Data owner: Data owner has collection of data files that he wants to outsource into the cloud server. For data privacy files must be encrypted before uploading to cloud. To enable CSP, keyword search on these encrypted files, a searchable index is built before encryption and is outsourced to CSP along with encrypted files.

2. Data user: User is one who wants to retrieve files relevant to a specified keyword. For this he enters a keyword and sends the request to CSP.

3. Cloud Service Provider (CSP): Upon receiving the search request, the cloud server is responsible to search the index and return the corresponding set of encrypted files to the user.

Following figure shows the architecture of the proposed system for secure and efficient data retrieval from cloud with three entities, data owner, users and cloud service provider.

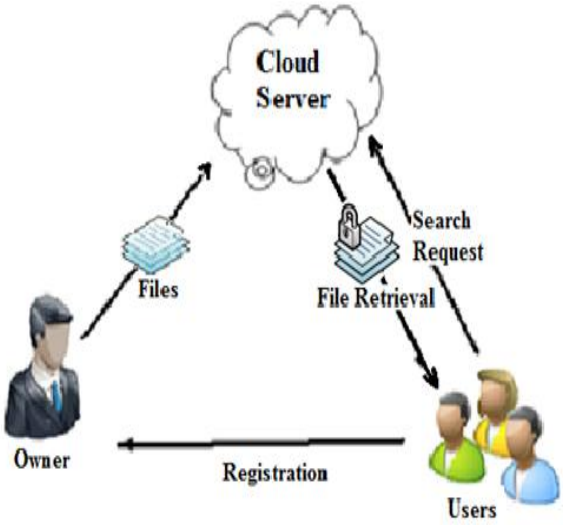

Figure 1: System Architecture

IV. IMPLEMENTATION

The system is designed and implemented in the following steps,

- User Registration.
- Building Searchable Index and Outsourcing Data to CSP.
- Authorization and Efficient Data Retrieval.
- Analysis of the System.

1: User Registration

In this module mechanism for registration of new user to the system is provided. User has to first register himself to the system to upload or retrieve data to or from cloud. User has to enter valid Email_id and password during registration.

When a new user registers to the system, a confirmation mail is sent to the user specified email_id. This mail is used to confirm that the email_id is valid. This mail contains a link and on clicking the link the user will be activated. A list of registered users is sent to the cloud service provider and this list is used by CSP to authenticate users when they login and request for service.

UID	Name	Email_id	Password	Is_Active
123	Abcd	aa@a.com	******	1

Table 2: Registered Users List

2: Building Searchable Index and Outsourcing Data to CSP:

For data privacy, files are encrypted before outsourcing them to cloud. However, encryption makes effective data utilization a challenging task. To enable the cloud service provider to efficiently search files with specified keyword from an encrypted file collection, a searchable index is built before file encryption and is stored at CSP. The CSP will retrieve the exact files containing the specified keyword using the searchable index. The searchable index stores list of mappings from keyword to the corresponding set of files that contain the keyword, allowing full text search. Score in the below table is number of times the keyword exist in the document or file.

Keyword	File_id	Score
W_i	F_1	45

Table 1: Searchable Index

In our system secure AES symmetric encryption algorithm is used to encrypt the data files, same key is used to encrypt and decrypt a file. Encryption is done at user side.

3: Authorization and Efficient Data Retrieval.

In this module a mechanism to authorize a user and to efficiently retrieve data files for the users at the CSP is developed. User has to first login to the system to avail services from cloud. When a user logs in to the system CSP uses registered users list to authorize users. The authorized user can then outsource or search files to or from CSP.

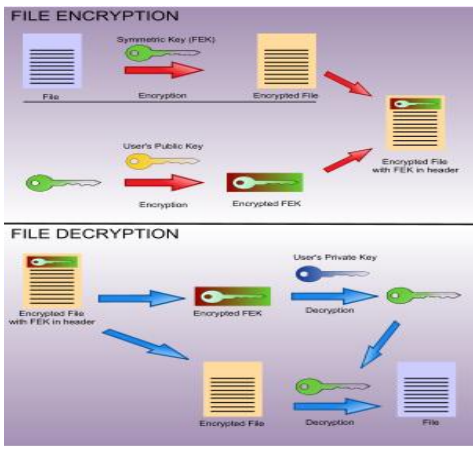

Figure 2: File Encryption and Decryption

When the user sends a request to the CSP to retrieve files containing a keyword, the CSP first searches the searchable index bu, gets the file ID's of files relevant to the user specified keyword, efficiently retrieve encrypted files and sends them to the requesting user in a rank order i.e. top files are more relevant than other. Files will be decrypted using decryption algorithm and downloaded at the user end.

4: Analysis of the System.

The analysis is done on the following parameters,

1. Security analysis: Data confidentiality is analyzed by comparing with standard encryption algorithms that use symmetric keys.

2. Performance analysis: Performance of our proposed system is calculated based on the efficiency. This includes time and cost for searching the matching's. The computational complexity of searching and building the searchable index is calculated.

V. IMPLEMENTATION RESULTS:

1. *User Registration:*

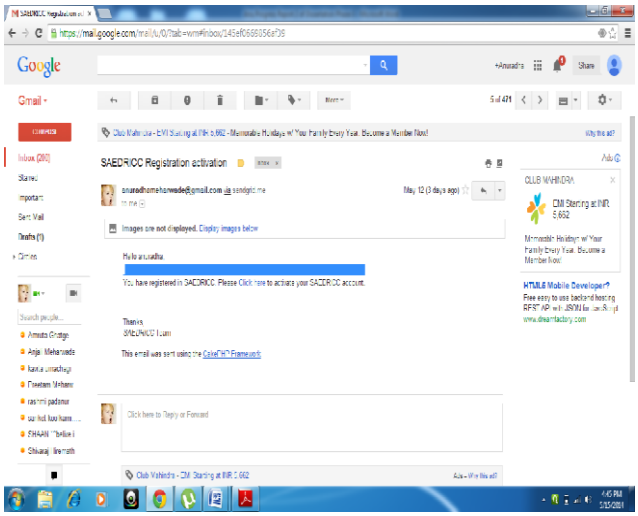

Figure 3: Confirmation Mail

2. *Outsourcing Files:*

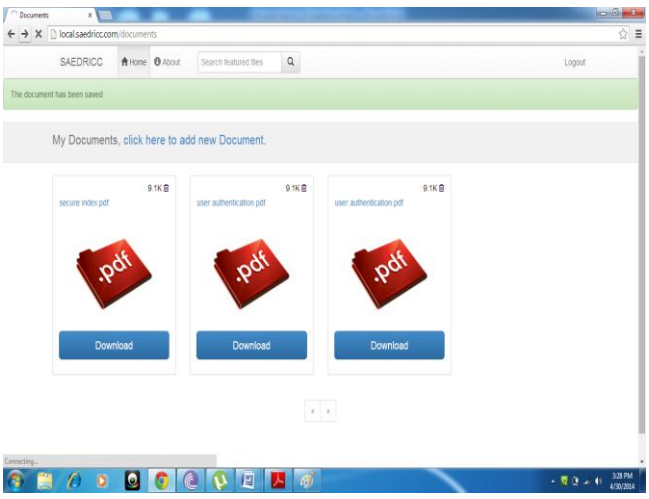

Figure 4: Outsourcing Encrypted Files

3. *Efficient Data Retrieval:*

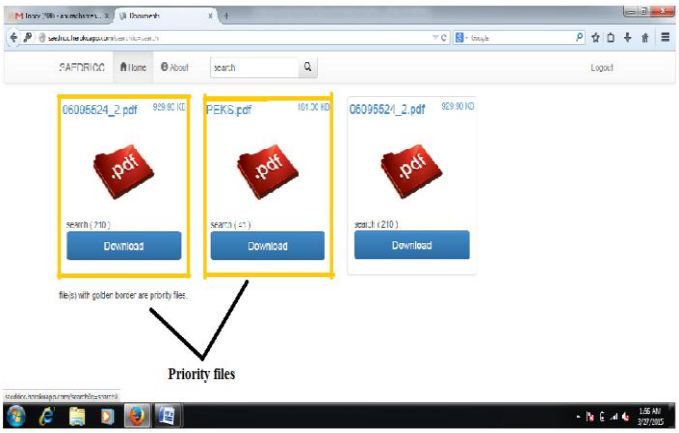

Figure 5: Output of Search Request

VI. CONCLUSION:

In this paper we solve the security problems which may occur during outsourcing the data. It not only provides data privacy but also enables keyword search on encrypted file collection thus providing secure and efficient data utilization. Present solution is best for effective data utilization and provides security for outsourced cloud data compared to previous ones.

V. REFERENCES:

(1) Cong Wang, Ning Cao, Kui Ren and Wenjing Lou. "Enabling Secure and Efficient Keyword Search over Outsourced Cloud Data" IEEE Transaction on Parallel and Distributed Systems, VOL. 23, NO. 8, August 2012.
(2) Ahmad. M. and Yang Xiang "Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing" IEEE Security & Privacy, 16-18 Nov. 2011.
(3) Boneh D, Crescenzo G, Ostrovsky R, Persiano G. Public Key Encryption with Keyword Search. In: Proceedings of Eurocrypt 2004, Lecture notes in computer science, vol.3027; 2004.p. 506-22.
(4) M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable Secure File Sharing on Untrusted Storage," in Proc. of FAST'03, 2003.
(5) L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Of ICICS'05, 2005.
(6) D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00, 2000.
(7) N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data" in Proc.of INFOCOM'11, 2011.
(8) http://technet.microsoft.com/enus/magazine/2006.05.howitworks.aspx
(9) https://devcenter.heroku.com/articles/quickstart
(10) Amazon EC2 and S3, Online at http://aws.amazon.com/