2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

AN EFFICIENT RANKED MULTI KEYWORD SEARCH FOR MULTIPLE DATA OWNERS OVER ENCRYPTED CLOUD DATA

[#1]RAMAVATH SARITHA, [#2]CH.PRANAVI

MBA STUDENT, DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

ASSISTANT PROFESSOR,DEPARTMENT OF CSE, SCIENT INSTITUTE OF TECHNOLOGY,IBRAHIMPATNAM, RANGAREDDY,T.S.

Abstract:- With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, also the internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information .Besides that, digital documents are also easy to copy and distribute, therefore it will be faced by many threats. Although there are many benefits to migrate data on cloud storage it brings many security problems. Therefore the data owners hesitate to migrate the sensitive data. In this case the control of data is going towards cloud service provider. This security problem induces data owners to encrypt data at client side and outsource the data. By encrypting data improves the data security but the data efficiency is decreased because searching on encrypted data is difficult. The search techniques which are used on plain text cannot be used over encrypted data. The existing solutions supports only identical keyword search, semantic search is not supported. In the paper we proposed semantic multi-keyword ranked search system. To improve search efficiency this system includes semantic search by using Word Net library. Vector space model and TF-IDF model is used for index construction and query generation.

Keywords: Cloud data, TF-IDF, Searchable encryption, Multi-keyword Search.

1. Introduction

In today's data intensive world, cloud computing is new type of computing paradigm which enables sharing of computing resources over the internet. The cloud characteristics are on-demand self-service, location independent network access, ubiquitous network access and usage based pay. Due to this charming features private and public organization are outsourcing their large amount of data on cloud storage.The cloud provider manages platforms and infrastructure on which the applications run. Cloud users can access cloud-based applications through a web browser or mobile application. The user data are stored on servers at a remote location. Cloud computing allows institution to get their applications and running faster with enhanced manageability and less maintenance. It enables IT professional to adjust resources to meet fluctuating and unpredictable business demand. Cloud security architecture recognizes issues with security control and management. Security control help to recover weakness

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

in the system and reduce the effect of an attack. There are some techniques are described below to enhance security from data loss.

Cloud service providers (CSPs) can access user's sensitive data without any authorization. General approach of CSPs is to protect the data confidentiality in which data is encrypting before outsourcing it to cloud server and this will affect a huge cost of data usability. In secure search over encrypted data, data owners outsourced their data to cloud server in encrypted form to preserve their privacy. When data user wants to search any file, data user send keyword request to cloud server. Cloud server then generate top relevant results to data user. Secure search over encrypted data is shown in following figure 1. Secure search over encrypted data not only reduce computation cost and storage cost for secure keyword search but also support multi-keyword ranked search, fuzzy keyword search and similarity search. All these schemes are limited to single-owner model. Earlier work support single-owner model, where data owner has to stay online to generate trapdoors for data user. Therefore, this paper proposes a multi-owner model to overcome the limitations of the earlier methods, where encrypted data are stored by multiple data owners and simultaneously data owners stay online to generate trapdoors. Different data owners share different secret keys to encrypt their secret data with different secret keys.

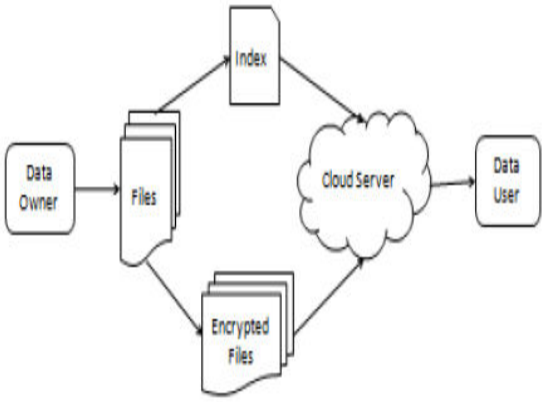

Fig.1. Secure Search over Encrypted Data

In this paper, secure search protocol is propose in which cloud server can perform secure search without knowing the actual value of keywords and trapdoors. Different data owners use different secret keys to encrypt files and keywords which are outsource to cloud server. Authenticated data users can send encrypted query without knowing secret keys of data owners. A novel dynamic secret key generation protocol and a new data user authentication protocol use to prevent the unauthorized users from accessing cloud data

II. RELATED WORK

Searchable encryption has been an import research area and many researchers and organizations have investigated search techniques to search on chipper text data. Searchable encryption allows storing data in encrypted format and you can apply keyword search over chipper text data. These search techniques builds searchable index tree such that its contents are hidden from server however it still allows performing document searching.These solutions differ from each other mostly in terms of whether they allow single keyword, multi-keyword, similarity search, ranked search. By using multi-keyword ranked search user can query

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

with multiple keywords and retrieve accurate search result. But all these search schemes does not allow synonym based queries.

Secure Index for Resource-Constraint Mobile Devices in Cloud Computing

Hanbing Yao et al. [3] proposed a secure index based on counting Bloom filter (CBF) for ranked multiple keywords search. Nowadays more organizations and users are outsourcing their data into cloud server. In order to protect data privacy, the sensitive data have to be encrypted, which increases the heavy computational overhead and brings great challenges to resource-constraint devices. In this scheme, several algorithms are designed to maintain and lookup CBF, while a pruning algorithm is used to delete the repeated items for saving the space. The problem of secure ranked search over encrypted data in the cloud server is discussed here. In the proposed scheme, counting Bloom filter is used to generate the secure index for ranked multiple keywords search. Moreover, several algorithms are designed to maintain and lookup CBF and a pruning algorithm is used to delete the repeat items for saving the space. The Paillier cryptosystem is employed to encrypt relevance scores. It ensures that even the same relevance scores will be encrypted into different bits, which can help to resist statistical analyses. The major computing work in rank is done by the cloud server on the encrypted relevance scores, which make the resource constraint mobile devices can easily search over encrypted data.

The Paillier cryptosystem is used to encrypt relevance scores. It will make sure that the same relevance scores are encrypted into different bits. So this can resist the statistical analyses on the ciphertext of the relevance scores. Moreover, the Paillier cryptosystem supports the homomorphic addition of ciphertext without the knowledge of the private key, the major computing work in ranking could be moved from user side to the cloud server side. Therefore, this scheme can effectively use in resource constraint mobile devices such as 5G mobile terminals.

An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing

Shulan Wang et al.[6] proposed an efficient file hierarchy attribute-based encryption scheme in cloud computing. This encryption technology can solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the areas like healthcare, military etc.

However, the hierarchy structure of shared files has been done using Ciphertext-policy attribute-based encryption(CPABE).

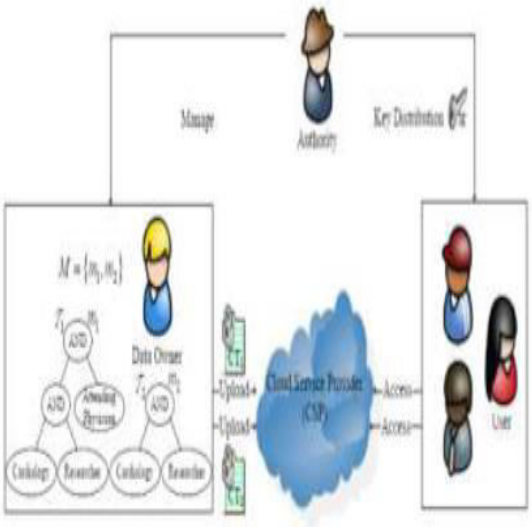

Fig -2: File sharing in cloud

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

The data files in multiple levels are integrated into a single access structure. That is data files of different data users in a group can be integrated into one. Then the hierarchical files are encrypted using the integrated one. The components of Ciphertext that related to attributes can be shared by the files. So, the ciphertext storage and time cost of encryptions are saved. As the number of files increasing, the advantages of this scheme become more and more noticeable.

In cloud computing server accepts the user files and creates some parameters. The one who manages the cloud servers and provides multiple services for client is the Cloud Service Provider (CSP). A data owner can encrypt the data files and upload the generated ciphertext to CSP. A user can downloads and decrypts the ciphertext from CSP. These shared files must have hierarchical structure.

That is many hierarchy subgroups or a group of files may be located at different access levels. If the files in the same hierarchical structure can be encrypted by using integrated access structure, then the storage cost of ciphertext and time cost of encryption could be saved.

The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. The main advantage of this method is that users can decrypt all authorization files by computing secret key once.

III. PROPOSED WORK

Above we represent system architecture

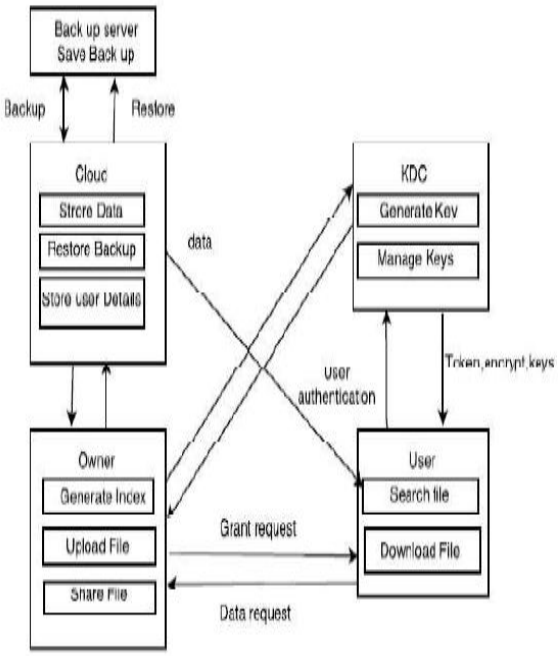

Fig.3. System Architecture.

1. Register:

Step 1: User Registration

Step 2: During registration user provides some necessary information.

Step 3: Token is given to end user by administrative server provide.

2. Upload File:

Step 1: Login.

Step 2: Upload file.

Step 3: Administrative Server provides an encryption key to the user

Step 4: Index of files for user.

Step 5: Encrypt user index.

Step 6: To encrypt index SHA-1 algorithm is used.

Step 7: Encrypt document AES algorithm

3. Share document with another User:

Step 1: Access privileges to data structure present on Administrative Server.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

4. Search:
Step 1: User login that verified by Administrative Server.
Step 2: Get key from Administrative Server.
Step 3: Generate Trapdoor for search.
Step 4: Achieved result set.

5. Backup:
Step 1: User login that verified by Administrative
Server.
Step 2: User get key from Administrative Server.
Step 3: Show own files.
Step 4: Select file and use backup facility where last modified copy is saved.

6. Restore:
Step 1: User login and verified by Administrative Server.
Step 2: User get key from Administrative Server.
Step 3: Show own deleted files. Step 4: Select file for restore.

IV. ALGORITHM

There are two types of algorithm used in this project.

1. Encryption:

This is used to encrypt the data files. This convert the plain text into the cipher text. This uses the AES (Advanced Encryption Standard) algorithm.

2. Decryption:

This is used to decrypt the data files. This convert the cipher text into the plain text. This uses the ADS (Advanced Decryption Standard) algorithm.

3. SMTP:

Simple Mail Transfer Protocol is used to send mail to the users

V.RESULTS

The performance of the proposed system is analyzed by using the three main characteristics of any network. These include encryption time, the searching time and the throughput of the system. We perform various experiments to compare the existing system with proposed system.

Encryption Time:-

We perform the experiments to calculate the total encryption time of the proposed system. We increase the message size with each experiment. The fig 8.1 of graph shows the total encryption time of the system. This graph shows that the proposed system has very less encryption time than existing system. As the message increases the encryption time of the system is increased with less amount of time.

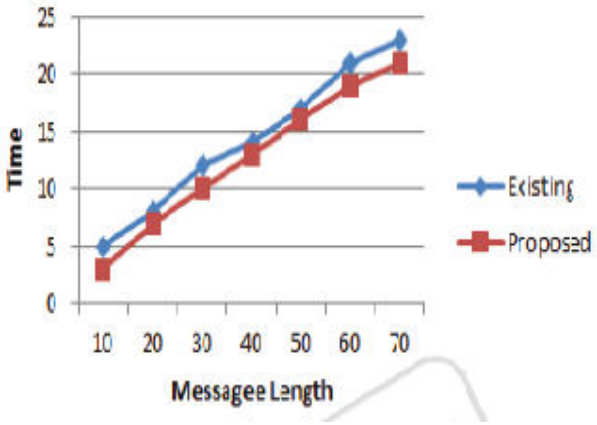

Fig.1.Encryption time

Searching Time:-

The searching time for the cloud data in proposed system is lower than the existing system, which show the searching time required for the searching of data in cloud. The data is on the cloud in encrypted format. The proposed system performance is much higher than existing system.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

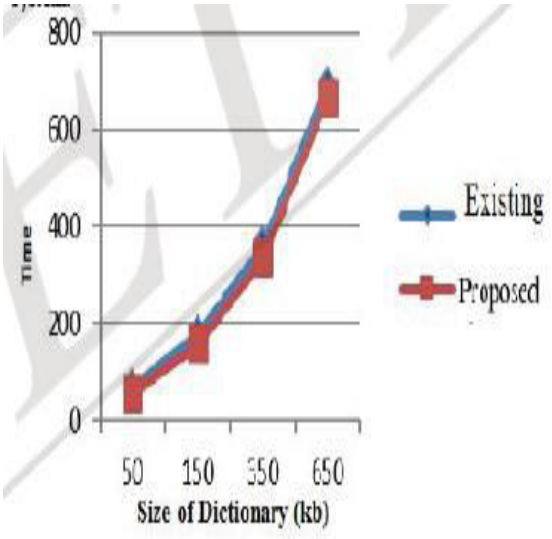

Fig.2.Searching Time

The table for above graph is shown below. The table given below gives the different values of time in seconds for existing and proposed system.

VI. CONCLUSION

This project establishes the importance of faster retrieval of data from Cloud. This has become more important in the current scenario where usage of cloud infrastructure is on a rise. As more users move towards cloud for storing their information, it is essential for cloud providers to use newer algorithms which give speedy retrieval without compromising security of user data.

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, A smdp based service model for inter domain resource allocation in mobile cloud networks, IEEE Transactions on Vehicular Technology, vol. 61, no. 5,pp. 2222-2232, 2012.

[2] M. M. Mahmoud and X. Shen, A cloud-based scheme for protecting source-location privacy against hotspotlocating attack in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805-1818, 2012.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, Exploiting geo-distributed clouds for e-health monitoring system with minimum service delay and privacy preservation, IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430-439, 2014.

[4] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, Privacy preserving data aggregation without secure channel: multivariate polynomial evaluation, in Proceedings of INFOCOM. IEEE, 2013, pp.2634-2642.

[5] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage, IEEE Transactions on Emerging Topics in Computing, 2014,DOI10.1109/TETC.2014.237-1239.

[6] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, Orderpreserving symmetric encryption, in Advances in Cryptology-EUROCRYPT. Springer, 2009, pp. 224-241.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking, IEEE Transactions on Parallel and Distributed Systems, vol. DOI: 10.1109/TPDS.2013.282, 2013.

[8] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, Towards secure multi keyword top-k retrieval over encrypted cloud data, IEEE Transactions on Dependable and Secure

Computing, vol. 10, no. 4, pp. 239-250,2013.

[9] A. Arvanitis and G. Koutrika, towards preference-aware relational databases, in International Conference on Data Engineering (ICDE).IEEE, 2012, pp. 426-437.

[10] N. Ferguson, R. Schroeppel, and D. Whiting, A simple algebraic representation of rijndael, in Selected Areas in Cryptography. Springer, 2001, pp. 103-111.

[11] Wang, N. Cao, K. Ren, and W. Lou, Enabling secure and efficient ranked keyword search over outsourced cloud data, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467-1479,2012.

[12] P. Golle, J. Staddon, and B. Waters, Secure conjunctive keyword search over encrypted data, in Applied Cryptography and Network Security. Springer, 2004, pp. 31-45.

[13] D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data, in Theory of cryptography. Springer, 2007, pp. 535-554.

[14] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, in Advances in Cryptology Eurocrypt. Springer, 2004, pp. 506-522.

[15] Q. Liu, C. C. Tan, J. Wu, and G. Wang, Efficient information retrieval for ranked queries in cost-effective cloud environments, in Proceedings of INFOCOM. IEEE, 2012, pp. 2581-2585.

AUTHOR'S PROFILE:

[1]. RAMAVATH SARITHA, Pursuing *M.Tech in CSE* **at** Scient Institute Of Technology, Ibrahimpatnam, Rangareddy, T.S.

[2]. Ms. CH. PRANAVI, She pursued her B.Tech in MTCET from JNT University Hyderabad, M.Tech Computer Science and Engineering from JNT University Hyderabad, She is currently working as Asst Prof in the Department of CSE at **Scient Institute of Technology Ibrahimpatnam**. She has 3 years of Academic experience. She Attended Many Workshops in different areas.