ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/3636
DOI URL: http://dx.doi.org/10.21474/IJAR01/3636

RESEARCH ARTICLE

SMART CLOUD FILE RETRIEVAL USING SEARCHABLE CIPHERTEXT KEYWORDS & ACCESS CONTROL ON INDEX

Sadeer Dheyaa Abdulameer.
Faculty Of Computer Science, Cihan University, Sulaimaniya, Kurdistan, Iraq.

Manuscript Info

Manuscript History

Received: 08 January 2017
Final Accepted: 06 February 2017
Published: March 2017

Key words:-
Cloud Computing, Data Security, Access Control, ABE & IBE

Abstract

Cloud Storage becomes more popular and many corporate, government organizations, share their data in public cloud which are semi-trusted cloud storage. Public cloud storages are hack able and data can be leak out, so we need a system where the files are encrypted and then stored in cloud. If the volume of the files is large then system need search engine to retrieve the file, in-turn search engine need keyword index for the fast performance. There may be a chance for the intruder to get the details of the files through unencrypted index keywords, So in proposed system index keywords are undergo hashing technique and cipher text are stored in index. This system will encrypt the file and encode the index keywords which give double production to the data in cloud. Further to the data security this system has access control system. At present ABE (Attribute Based Encryption) & IBE (Identity based Encryption) are used for the file access control in cloud which requires more processing time and calculations. Proposed system uses a new technique where Access Control is included in search index keywords, which require less computation and quick retrieval.

Introduction:-

Cloud computing allows users to use enormous data storage and infinite computation capabilities at a very low price. Even though cloud storage gives lot of benefits, Data Owner is not having the full control over the outsourced data, it can be hacked. To avoid this problem, user should encrypt their data before outsourcing to the cloud. However, encryption can obstruct some useful functions such as searching over the encrypted data which is outsourced in cloud, while enforcing an access control policy. Moreover, it is natural to outsource the search operations to the cloud, while keeping the outsourced data private. There is a need to allow the data consumers to verify whether the cloud faithfully executed the search operations or not. To the best of our knowledge, existing solutions cannot achieve these objectives simultaneously.

Our Contributions:-

We propose a new concept, called ***Smart Cloud File Retrieval using Searchable Cipher text Keywords & Access Control on Index.*** This system allows a user to control the search, and retrieve its outsourced encrypted data according to a user access control policy, while allowing the authorized users to search and retrieve files through innovative index based access control system.

Corresponding Author:- Sadeer Dheyaa Abdulameer..
Address:- Faculty Of Computer Science, Cihan University, Sulaimaniya, Kurdistan, Iraq.

In other words, a data user with proper authentication and attribute can access the encrypted files in the cloud with access control rules. This system provide followings (I) Data Owner can upload the files into the cloud in encrypted form, (ii) Data Owner can able to set Access Control Policies for the outsourced files (iii) Data User can able to search and retrieve the file through access control based cipher text index keywords.

We formally define the security properties of proposed system and present schemes that provably satisfy them. The scheme is constructed in a modular method, by using attribute-based encryption, bloom filter, digital signature, and a new building-block we call attribute-based Cipher text keyword search (ABCKS) that may be of independent value. Experimental evaluation shows that the system provides good result and performance.

Associated Works:-

To the best of our knowledge, no existing solution is sufficient for what we want to achieve. In what follows we briefly review the relevant techniques.

Attribute -Based Encryption (ABE). ABE is a popular method for enforcing access control policies via cryptographic means. Basically, this technique allows entities with proper credentials to decrypt a cipher text that was encrypted according to an access control policy [2]. Depending on how the right of entry control policy is enforced, there are two variants: KP-ABE (key-policy ABE) where the decryption key is associated to the right of entry control policy [2], and CP-ABE (cipher text-policy ABE) where the cipher text is associated to the access control policy [5]. ABE has been enriched with various features. In this paper, we use ABE to construct a new primitive called attribute-based keyword search (ABKS), by which keywords are encrypted according to an access control policy and data users with proper cryptographic credentials can generate tokens that can be used to search over the outsourced encrypted data. This effectively prevents a data owner from knowing the keywords a data user is searching for, while requiring no interactions between the data users and the data owners/trusted authorities. This is in contrast to [6], where the data users interact with the data owners/trusted authorities to obtain search tokens.

Keyword Search over Encrypted Data. This method allows a data owner to generate some tokens that can be used by a data user to search over the data owner's encrypted data. Existing solutions for keyword search over encrypted data can be classified into two categories: searchable encryption in the symmetric-key setting and searchable encryption in the public-key setting. Several variants have been proposed to support complex search operations. Moreover, searchable encryption in the multi-users setting has been investigated as well [9], [10], where the data owner can enforce an access control policy by distributing some (state full) secret keys to the authorized users. However, all these solutions do not solve the problem we study, because (i) some of these solutions require interactions between the data users and the data owners (or a trusted proxy, such as a trapdoor generation entity [6]) to grant search capabilities, and (ii) all these solutions assume that the server faithfully executed search operations. In contrast, our solution allows a data user with proper credentials to issue search tokens by which the cloud can perform keyword search operations on behalf of the user, without requiring any interaction with the data owner. Moreover, the data user can verify whether or not the cloud has faithfully executed the keyword search operations. This is true even for the powerful technique called predicate encryption, which does not offer the desired verifiability.

Verifiable Keyword Search. Recently, verifiable keyword search solutions have been proposed in [12], where each keyword is represented as a root of some polynomial. It is possible to check whether a keyword is present by evaluating the polynomial on the keyword and verifying whether the

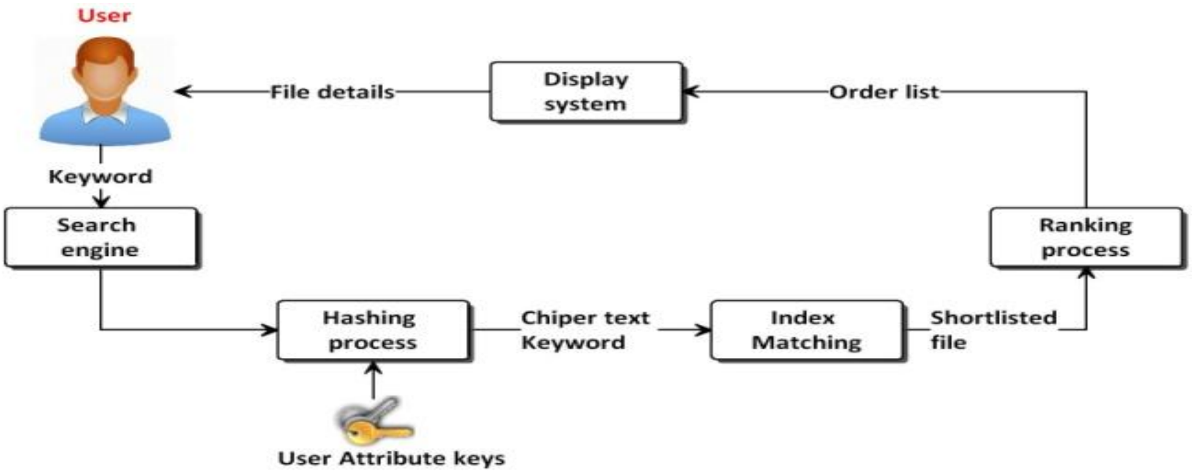
Output is zero or not. However, these approaches work only when keywords are sent in plaintext to the cloud, and are not suitable for our purpose because the cloud should not learn anything about the keywords. It is worth mentioning that the secure verifiable keyword search in the symmetric-key setting can be insecure in the public-key setting because the attacker can infer keywords in question via an off-line keyword guessing attack (in lieu of the off-line dictionary attack against passwords).

Problem Statement:-

Consider a situation where a college has to store lot of e-books in cloud storage. That e-book has to be accessed by their students. If the e-books are less in number, the students can able to browse and download. Consider a situation the number of e-books is huge it is not possible to browse and download the file, so the students need a search engine. Whenever search engine come into picture, indexing technique have more weight age. The problem here is to safeguard the file content and index keywords, index keywords are usually sensitive and which are linked with the file they are connected when a hacker get this index data he may guess the file content. Our aim is to safeguard the index keyword, file content and to implement access control system.

Access control is a big challenge, in current cloud storage for access control, attribute based encryption (ABE), identity based encryption (IDE) are used. Now in this system we are using Attribute Based Cipher text Index Keyword for access control.

The assumption in this system is each department in the college will have one Unique Attribute Key (UAK). At the time of uploading the file into the cloud the concern user has to provide the access policy details, like which are the department students and staff can able to access the file from the cloud.
Proposed system will automatically remove the unnecessary words from the file and create the keywords with weights using Term Frequency (TF)



algorithm. All the extracted keywords will processed with hashing technique of allowed department Attribute

Keys which will provide Attribute based cipher text Keywords; these cipher text keywords are stored in index array for searching process. For example there are I keywords are extracted from the e-book and the authority selected J departments in access control setting then in Attribute Based Cipher text Keywords generated will be I * J. All the ABCK are inserted into index array. The idea behind this is each keyword will undergo hashing process with accessible department unique attribute keys. Since department based attribute keys are unique and this will create the same Attribute Based Cipher text keywords when the users from the same department search in the search engine. This is show in fig.1.

In this paper, we propose the new approach of *Smart Cloud File Retrieval using Searchable Cipher text Keywords & Access Control on Index* as a better solution, as depicted, in Fig. 2, Data owner only needs to generate one department one attribute key instead of attribute key to all user , instead of $\{k_i\}^m_{i=}1$ for sharing m documents with User, and User only needs to submit a Login ID for accessing the file, from the Login ID user's department is identified and then the corresponding department attribute key is used to generate the attribute based cipher text keywords. The cloud server can use this aggregate trapdoor and some public information to perform keyword search and return the result to User. Therefore, in Smart Cloud File Retrieval, the delegation of keyword search right can be achieved by sharing the single aggregate key. We note that the delegation of decryption rights can be achieved using the key-aggregate encryption approach recently proposed in, but it remains an open problem to delegate the keyword search rights together with the decryption rights, which is the subject topic of this paper. To summarize, the problem of constructing a *Smart Cloud File Retrieval* scheme can be stated as:

"To design a Smart Cloud File Retrieval using ***Searchable Cipher text Keywords & Access Control on Index scheme*** *under which any keyword cipher texts from any document is searchable with a constant-size cipher text keywords generated by a constant-size department attribute key."*

Implementation:-

This system is developed in web technology with MVC architecture. The proxy server has crypto system process which encrypts and decrypts the file, hashing technique which is used to get the keyword from the user and produce user attribute based hash code. A powerful search engine with access control based indexing system. There, is a ranking system which short the shortlisted file based on search keyword weights. The proxy server provides software as a service, which is a private server and the encrypted files are stored in public cloud storage which provides storage as a service. This system combines private server and public server so it forms hybrid cloud approach.

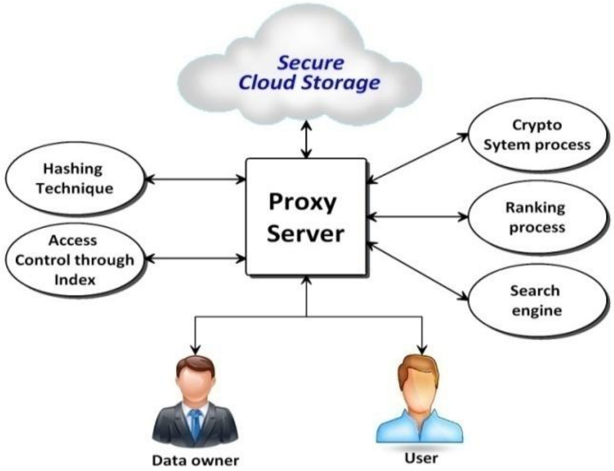


Fig. 2:- System Architecture

Security Analysis:-

The security system of proposed work is very strong. It gives security from outside hackers as well as security from insider (with access control) the registered user. The files which are stored in cloud storage are encrypted and the index keywords are in hash tag which gives double protection from the hackers. Since attribute based cipher text keywords are used even though the registered user can able to retrieve the files for which they have the access.

Conclusion:-

By considering the disadvantage of data outsourcing in public cloud storage we come up with a new idea attribute based cipher text keyword search (ABCK). In this the access control mechanism is built in search index. There is no need to provide attribute based key for each and every user. With the experimental result and evaluation technique our system result shows it is much better in performance and convince in secure file retrieval system from cloud storage for the further feature work. We consider multi owner document storage system and issues related to that.

References:-

1. M Li, J Li, PPC Lee, W Lou . Owens, R., Bhargava, B.: “Secure Deduplication with Efficient and Reliable Convergent Key Management”. In: IEEE transactions on …, 2014.
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. of ACM CCS, pp. 89–98, 2006.
3. A Sahai, H Seyalioglu, B Waters , and B. Waters, “Dynamic Credentials and Cipher text Delegation for Attribute-Based Encryption,” in Proc. of Advances in Cryptology–CRYPTO 2012.
4. C. Chu, S. Chow, W. Tzeng, et al. “Key-Aggregate Searchable Encryption for Group of Data Sharing via Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2016, 25(2): 468-477.
5. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing”, Proc. IEEE INFOCOM, pp. 534-542, 2010.
6. T Jung, XY Li, Z Wan, M Wan. “Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption”, IEEE Transactions on 2015.
7. J Li, YK Li, X Chen, PPC Lee. “A Hybrid Cloud Approach for Secure Authorized Deduplication”, Secure Data Management, IEEE Transactions on, 2015.
8. J Li, J Li, X Chen, C Jia, W Lou, “Identity-based Encryption with Outsourced Revocation in Cloud Computing,” Ieee Transactions on, 2015

9. M Aigali, JB Madalgi, PB Patil, G. Persiano. “Sharing of Data in a Group by Generating Key Clump”, Bonfring International Journal on 2016.
10. Z Fu, X Sun, Z Xia, L Zhou, J Shu. “Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing”, in: Conference (IPCCC), 2013.
11. J Wang, H Ma, Q Tang, J Li, H Zhu. “Efficient verifiable fuzzy keyword search over encrypted data in cloud computing”, on 2013.
12. Q Zheng, S Xu, G Ateniese - Infocom,, “VABKS: Verifiable attribute-based keyword search over outsourced encrypted data,” in Proc. 2014 proceedings IEEE, 2014.
13. D Koo, J Hur, H Yoon. “Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage”, ELSEVIER of Computers & Electrical engineering on 2013.
14. Z Liu, H Yan, Z Lin, L Xu - J. UCS. “An Improved Cloud Data Sharing Scheme with Hierarchical Attribute Structure”, Journal of Universal Computer Science 2015.
15. X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. “Key Aggregate Cryptosystem for Efficient way data sharing in cloud Environment”, Journal of IJETCSE 2016.
16. [16]SB Lambhate, S Patil .“Key Aggregate Searchable Encryption: Improved Construction under Multi-Owner Setting”, International Journal of Engineering Science, 2016.
17. K Yang, X Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing”, IEEE transactions on parallel and distributed, 2013.
18. X Liu, Y Zhang, B Wang, J Yan, “Mona: Secure multi-owner data sharing for dynamic groups in the cloud”, IEEE transactions on parallel, 2013.
19. V Sathana, J Shanthini. “Three Level Security System for Dynamic Group in Cloud”, International Journal of Computer Science Trends and Technology, 2013.
20. P More, DG Harkut , S. F. Shahandashti, et al. “Cloud data security using attribute-based key-aggregate cryptosystem ”, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),2016.
21. F Zhang, R Safavi-Naini, W Susilo . “An Efficient Signature Scheme from Bilinear Pairings and Its Applications”, International Workshop on Public Key Cryptography, 2004.