MJRET

Open Access

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

ISSN:2348 - 6953

SECURE MULTI- RANKED MULTI-KEYWORD SEARCH FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING

Namrata Daware, Kirtana Bhatkar, Darshan Kumbhar, Nikhil Tayade, Prof.Bharati Kudale

Department of Computer Engineering
GSMCOE College of Engineering Pune, India

Abstract: *Now days with the advent of cloud computing, it has become increasingly popular for data owners to store their data to public cloud servers while allowing data users to retrieve this data. Users are stores their data in encrypted format on the cloud that's why unauthorized user cannot access the data. When user wants to access the data they have to get decryption key from user. However, most cloud servers in practice do not just Serve unique owner; instead, they support multiple owners to share the benefits of the cloud computing.*
This paper, we suggest 1) To keep safe the secrecy 2) Several-owners model search several keywords and Ranked. To make possible cloud servers to execute safe to look omission knowing the real information of both keywords and trapdoors,1)To keep alive the privacy of related scores between keywords and files and rank the search result, we suggest a novel Additive Order and Privacy Preserving Function family.2)dynamic hidden key creation rule and a new data user to establish as genuine rule

Keywords: *several owners, Cloud computing, Ranked keyword search, Privacy preserving;*

1. INTRODUCTION

Cloud storage is used for storing the data. Cloud storage stores the large amount of data and it stores data foe long time. It is a model of data storage in which the digital data is stored in logical pools. The physical storage requires multiple servers and the physical environment is typically owned and managed by hosting company. The cloud storage providers are responsible for keeping the data available and accessible whenever it is required and also physical environment protected and running. Organizations and peoples lease or buy storage capacity from the providers to store organizations, users, or applications data.

To make easy cloud servers to perform safe search excluding knowing the real value of both keywords and trapdoors, we properly build a novel safe search rule. So that various data owners use distinct keys to hide their files and keywords. Genuien data users can get a query excluding knowing confidential keys of these various data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggest a family which preserves privacy, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To protect from disclosing the result we propose a novel dynamic secret key generation protocol and a new data user authentication rule.

The main contributions of this paper are listed as follows:

- We supervise experiments on real-world Datasets to verify the effectiveness and capability our suggest schemes.
- We suggest a approach that performs multiple key word search and rank them properly.
- We suggest an Additive Order and Privacy Preserving Function family (AOPPF) which allows the cloud server produces the file that rank properly.
- We suggest an capable data user authentication rule, which stop attackers to disclose hidden key and only genuine data user can do search.
- We define search data on clued that data is hidden format and also providing the privacy when search the multiple keywords.

2. LITERATURE SURVEY

1] Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud:

Enabling keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data outsourced to the cloud. Existing solutions provide multi-keyword exact search that does not tolerate keyword spelling error, or single keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search schemes rely on building an expanded index that covers possible keyword misspelling, which lead to significantly larger index file size and higher search complexity. In this paper, we propose a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search without increasing the index or search complexity. Extensive analysis and experiments on real-world data show that our proposed scheme is secure, efficient and accurate. To the best of our knowledge, this is the first work that achieves multi-keyword fuzzy search over encrypted cloud data.[1]

2] Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud:Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before-outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search

schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi-contributor case. Inspired by attribute-based encryption (ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e. file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re-encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi-trusted cloud server. We formalize the security definition and prove the proposed ABKS-UR scheme selectively secure against chosen-keyword attack. Finally, performance evaluation shows the efficiency of our scheme. [2]

[3] A digital watermarking approach to secure and precise range query processing in sensor networks:

Two-tiered wireless sensor networks offer good scalability, efficient power usage, and space saving. However, storage nodes are more attractive to attackers than sensors because they store sensor collected data and processing sink issued queries. A compromised storage node not only reveals sensor collected data, but also may reply incomplete or wrong query results. In this paper, we propose QuerySec, a protocol that enables storage nodes to process queries correctly while prevents them from revealing both data from sensors and queries from the sink. To protect privacy, we propose an order preserving function-based scheme to encode both sensor collected data and sink issued queries, which allows storage nodes to process queries correctly without knowing the actual values of both data and queries. To preserve integrity, we proposed a link watermarking scheme, where data items are formed into a link by the watermarks embedded in them so that any deletion in query results can be detected.[3]

[4] Secure Ranked Multi-keyword Search for Multiple Data Owners in Cloud Computing:

With the advent of cloud computing, it becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve these data. For privacy concerns, secure searches over encrypted cloud data motivated several researches under the single owner model. However, most cloud servers in practice do not just serve one owner, instead, they support multiple owners to share the benefits brought by cloud servers. In this paper, we propose schemes to deal with secure ranked multi-keyword search in a multi-owner model. To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Extensive experiments on real-world datasets c While doing the research we discover following

issues regarding cloud computing security.[4]

1. **Security in Searching.**
    a. User fire query to server for searching which is not secure.
2. **Single Owner model.**
    a. Many public cloud servers as single owner model this limits the owners scalability.
3. **Privacy about the owner's data.**
    a. None of the cloud assured about the owners data. Owner does not right to protect their own data.
4. **None of the project combines both multi owner and multi user concept.**
    a. We confirm the efficiency and efficiency of our proposed schemes.

3. IMPLEMENTATION PROPOSED SYSYTEM

Implementation Details

We now describe the design of our proposed work, which considers multiple data owners, multiple data users, application server as a admin that activate the number of users and data owners and semi trusted cloud storage.

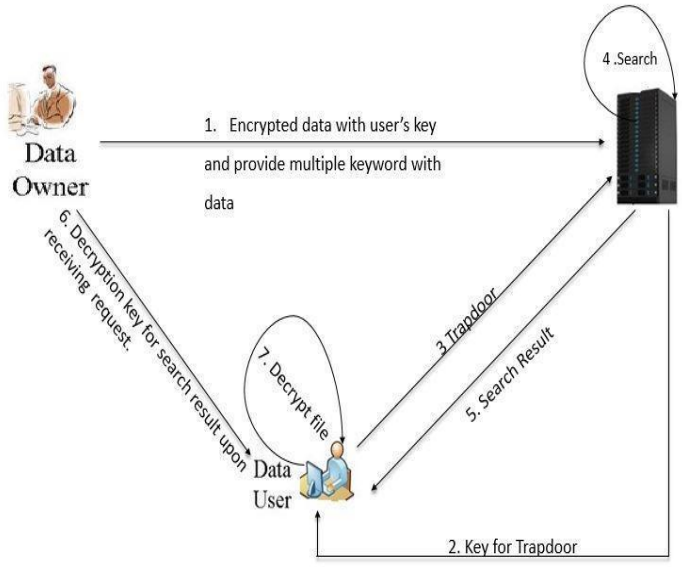

Fig 1. System Architecture

In this application data owner is created a data or we can say file. Also data owner generate a index for the file. After that owner encrypt the file and upload into the cloud. The application server also reencrypt the file. The data user when wants to access a specific file he/she send request to data owner. And it gets the decryption key. By using this key user decrypt the encrypted file. And get the plain text file.

In this phase we make experiment on discovered problem. To overcome the issues we go through the various papers. While we going through the papers we found nice solutions to above problem:

1. **Secure Searching :-**
    a. System will generate a search key for each user after approval from admin (one-time)
    b. The User enters a keyword in order to retrieve the associated File.
    c. Using that keyword along with the user's key and search key a trapdoor is calculated.
    d. This Trapdoor along with a search key used in this calculation is sent to the server.
    e. We also use n-gram algorithm for the fuzzy search.

2. **Multi-Owner Model and Secure Storage of owners data:-**
    a. Here we proposes Multi-Owner model over single Owner.
    b. In multiple owner model has rights to upload the over server.
    c. The user uploads the desired File to server which is securely stored using a User's key to access it.
    d. Along with the secured storage of the file, the keywords or index related to that file is also stored in the Server.
    e. The Owner of the file has the Right to provide access to other user for each file out of which the transmitted key plays a part in its Secured Storage.
    f. Will approve search requests of various users one-time after accessing the system

4. MATHEMATICAL MODEL

System S= {Multi Keyword Ranked Search Application} System S= {S1, I, d, O}
S1 = {User, Data}
I = {V, P}
d = function O = output
I1 = V =>> Variables
I2 = D =>> Data(Files)

[1] I1 = {Source Data, Files}

D1 = I1 =>> O1
O1 = {F1,F2,F3, …….,Fn}
F = Shared Files
[2] I2 = {Files, Search}
D2 = Cal
Cal = {Files, Search}
S = {S1, S2, S3, …. , Sn}
S1 = {Files, s1, s2, s3, ….. , sn}
Sample Data = Data [Files] + Searched Data SD Data [Data, Searched Data i]
i= 1
SF = {SF1, SF2, SF3, ….. , SFn}
[S = SharedFiles, SF = Searched Files]
Searched Files = Data (SF1, SF2, SF3, …. , SFn)
O2 = {Searched Files}
Show (Files)

5. ALGORITHM FOR ENCRYPTION AND DECRYPTION

I. Elliptic Curve Cryptography Algorithm:

1. Select the file type then select plain text from the file
2. After selecting file select the output file
3. After selecting output file check if file compress or not
4. If the file compress then check the plain text is converted to cypertext or not(encrypted file)
5. If text in file are hidden or converted to cypertext then encryption is successful.
6. For retrieving encrypted, hidden, compressed message select the output file for retrieving output file enter key or password.

Key generation:

(q, FR, a, b, G, n, h).

1. Select a random number d, d ∈ [1, n – 1]
2. parameters Compare Q = dG.
3. public key is Q and private key is d.

A public key Q = (xq, yq) associated with the domain parameters (q, FR, a, b, G, n, h) is validated using the following procedure

1. Check that Q ≠ O
2. Check that xq and yq are properly represented elements of Fq
3. Check if Q lies on the elliptic curve defined by a and b.
4. Check that nQ = O

II. N-Gram Algorithm:

We are using N-GRAM Algorithm for fuzzy searching keywords presents in file. It is actually perform on keyword search using scanning of all character in file on gram level. we are separate each character on 1^{ST} level then compare each character with our keyword .this procedure is repeat until we are reaching n-level .

After reaching n level we are achieving the result related with our keyword (search result).

5.1 Advantages:-

1. On cloud Secure Multi-keyword Ranked Search .
2. Search with the rank results and return the top-*k* relevant files.
3. Multi Keyword search.
4. Multi Keyword search with Rank also.
5. User Profile Management
6. Key Sharing with Friends using Email.
7. Also OTP (one time password)is used for authentications and sequrity.

6. CONCLUSION

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets.

REFERENCES

[1] *D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing",* SIAM J. Comput.*, vol. 32, no. 3, pp. 586-615, 2003.*

[2] *W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, et al., "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking",* Proc. IEEE 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security*, pp. 71-81, May 2013.*

[3] *J. Hur, "Improving security and efficiency in attribute-based data sharing",* IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 10, pp. 2271-2282, Oct. 2013.*

[4] *R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, "Order preserving encryption for numeric data",* Proc. ACM SIGMOD Int. Conf. Manage. Data*, pp. 563-574, Jun. 2004.*

[5] *A. Boldyreva, N. Chenette and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions",* Proc. 31st Annu. Conf. Adv. Cryptol.*, pp. 578-595, Aug. 2011.*

[6] *Y. Yi, R. Li, F. Chen, A. X. Liu and Y. Lin, "A digital watermarking approach to secure and precise range query processing in sensor networks",* Proc. IEEE INFOCOM*, pp. 1950-1958, Apr. 2013.*

[7] *R. A. Popa, F. H. Li and N. Zeldovich, "An ideal-security protocol for order-preserving encoding",* Proc. IEEE Symp. Security Privacy*, pp. 463-477, 2013.*

[8] *F. Kerschbaum and A. Schroepfer, "Optimal average-complexity ideal-security order-preserving encryption",* Proc. ACM SIGSAC Conf. Comput. Commun. Security*, pp. 275-286, 2014.*