Multiple Fuzzy Keyword Search over Encrypted Data Using Date and Time

[1]Anagha RamnathKadve, [2]Prof. Dr.S.B.Vanjale
[1]M.Tech Scholar, [2] Professor
Department of Computer Engineering,
BharatiVidyapeeth Deemed University College of Engineering, Pune, India

***Abstract*—The enhancement of the network and the growth of huge knowledge, also the remotely out-sourced the data to the cloud, which may avoid the local management of data. The system reduces the required hardware cost. However, some sensitive information, like personal healthcare info and private property info should be encrypted first then outsourced to the cloud. The system will shield confidential information. However, the encrypted data on the cloud will increase the problem of the information retrieval. As a result, the data owner or unauthorized users can't search properly the information they have. It's impractical to transfer all of the information to host side from the cloud, which can end in large communication computation overhead.**

Index-Term: **Cloud Computing, Privacy-Preserving, Encryption/Decryption, Ranking, Relevance Score Find, Top-k Monitoring, Security.**

I. INTRODUCTION

Cloud computing is a revolutionary technology that is changing the way IT hardware and software are designed and purchased. As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment, and flexible resource management, etc. Initiatives of all sizes can control the cloud to escalationcollaboration andinnovation. Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records, and government confidential files, to the cloud. Once sensitive data are subcontracted to a remote cloud; the corresponding data owners lose direct control of the data. Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls. However, the mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses full control of cloud hardware, software, and owners' data.

Encryption on delicate data before subcontracting can reserve data privacy against CSP. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem. A trivial solution to this problem is to download all the encrypted data and decrypt them locally. However, the method is obviously impractical because it will cause a huge amount of communication overhead. Therefore, developing a secure search service over encrypted cloud data is of paramount importance. Secure search over encrypted data has recently attracted the interest of many researchers. The existing systemdefines and solves the problem of secure search over encrypted data. The existing systemproposes the conception of searchable encryption, which is a cryptographic primitive that the main contributions of the paper are listed as follows:

- The system will consider the problem of secure fuzzy keyword search.
- To generate adynamic key using fuzzy logic.

II. RELATED WORK:

The systemhas explained benefits of theproposed approach with different algorithms. For anexplanation of the proposed work techniques and algorithms such as indexing, trapdoor generation, re-encryption of thetrapdoor and top-k file display.

The paper conveys some hassle for data search. Searchable secret writing permits users to look over the encrypted data on cloud storage to retrieve the concerned data whilenot coding. Throughout the paper, a fine-grained searchable scheme with a pair of non aforethought cloud servers is planned. The systemhas a tendency to propose a fine-grained searchable scheme supporting multiple users utilizing the advantage of attribute-based coding techniques.**[1]**

Multi-keyword search mechanism explains that the users can search among the cloud merely per their search. In theproposedsystem, new public-key cryptosystems are planned to be secure, efficiently, andeasily share knowledge with others in cloud storage. The most set up are that one can mixture any set of secret keys and build them as compact collectively key, but all keys ought to be collective. The system is additional versatile than hierarchic key assignment. AES technique is employed within the projected system for effective data sharing. **[2]**

The paper explains the enhancement of the network and ahuge expansion of data. The data owner used to remotely outsources their data to thecloud, which could avoid the native info management and scale back the native hardware worth.The supply encrypted info to cloud can increase the matter of the information retrieval, as a result of knowledge owner or unauthorized users can't search properly the data they need, and in addition it's impractical to transfer all of the information to native facet from the cloud that is in a position to guide to giant communication a computation overhead. **[3]**

In the paper, the existing systemhas a tendency to propose schemes to touch upon secure hierarchic multi-keywordsearch during a multi-owner model. To change cloud servers to make asafe search while not knowing the particular knowledge of each keyword and trapdoors, the systemhas a tendency to consistently construct a unique secure search protocol. To rank the search results and preserve the privacy of relevancy scores between keywords and files, the systemhas a tendency to propose a unique Additive Order and Privacy conserving perform family. To modify the cloud server to perform asecure search among multiple owners' knowledge encrypted with totally different secret keys, system have a tendency to consistently construct a unique secure search protocol. Another resolution is to share a secret key among all knowledge house owners. However, life can cause the protection threat of single purpose of failure.i.e.Once the key secrets unconcealed by an information owner (e.g., careless key management), alternative knowledge owners'Secret key are going to be leaked similarly. [**4]**

III. PROPOSED SOLUTION:

The proposed systemis presenting an appropriate explanation for the target problem during the paper. The proposed systemtends to initially define a system model and a corresponding threat model. In this paper, we tend to propose PRMSM, a privacy-protective graded multi-keyword search protocol during a multi-owner cloud model. To modify cloud servers to perform asecure search without knowing theparticular value of each keywordand trapdoors, the proposed system consistently construct a completely unique secure search protocol. To rank the search results and preserve the privacy of relevancy scores among keywords and files, proposed system tend to propose a new additive order and privacy-protective function; a family that helps the cloud server, come back the foremost relevant search results to information users without revealing any sensitive data.

The main contributions of the paper are as follows:

Proposed systemsystematically constructs a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors.

The systemproposes an Additive Order and Privacy-Preserving Function family (AOPPF) which allows data holders to defend the secrecy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurate.

System Architecture:

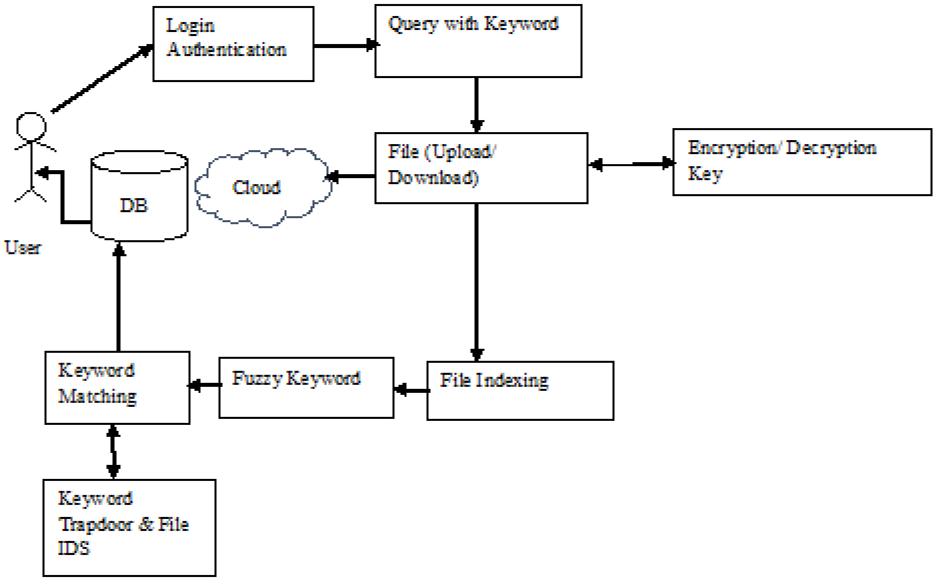

Fig 1. System Architecture

The following subsection describes the five steps in detail.

1. Authentication-secret key generation

In the authentication phase, user login to the system by providing his credentials. The system authenticates theuser by verifying the credentials. The secret key generated to give theauthenticated user. Thesecret key generated by using ahash function and secret key generation algorithm.

2.Indexing

This is thesecond module of the proposed system. Indexing is done on the uploaded and downloaded file. Indexing is done for file reference. For that, in the proposed system we have used context-based indexing.

3. Encryption

Following are the few conditions which would be satisfied for encrypting keyword
First is data owners need to utilize their own secret key for encryption?
Secondly, the secret key must be encrypted to different ciphertext every time for thesame keyword.

These conditions are very advantageous to proposed system for few reasons. First, is trailing the secret key of one owner wouldn't allow disclosing data of another owner. Second is cloud server would not look at any relationship between keywords which are encrypted.

4.Trapdoor calculation

The proposed system must satisfy following two conditions to make use of data to generate encrypted keywords (trapdoors) conveniently, efficiently and securely:

First, the data user doesn't require asking several data owners for secret keys to produce trapdoors.

Second, each time the generated trapdoor must be different for thesame keyword. To meet these conditions, the generation of trapdoor is performed in two steps:

Firstly, theuser of data produces trapdoor which is based on users search keyword as well as random number. Secondly, the trapdoors are re-encrypted by theadministrative server for authenticated users of data.

5. Top-k file display

The proposed system must fulfill conditions given next for ranking the relevance score while maintaining its privacy.

This function must save data order, as this helps cloud server for determining which file is more appropriate to a certain keyword, according to the encoded relevance scores.

The top-k function must not be exposed by the cloud server due to which cloud server can make comparison evaluation on encoded relevance scores without knowing their actual values.

Special data owners must have special functions such that illuminating the encoded data owner value wouldn't result in the leakage of encoded values of other data owners.

ALGORITHMS:

In the system following types of algorithms basically used:

1) AES Algorithm for File Encryption

2) TFIDF

3) Jaccard similarity Algorithm

4) Trapdoor Generation

5) Globally unique identifier (GUID) algorithm for file indexing.

The Apriori Algorithm:The Apriori Algorithm is an influential algorithm for mining frequent itemsets for Boolean association rules.

Key Concepts:

- Frequent Itemsets: The sets of theitem which has minimum support (denoted by Li for ith-Itemset).
- Apriori Property: Any subset of afrequentitemset must be frequent.
- Join Operation: To find L k, a set of candidate k-itemsets is generated by joining Lk-1 with itself.

Pseudocode:

Join Step: C_k is generated by joining $L_{k-1}$with itself

- Prune Step: Any (k-1)-itemset that is not frequent cannot be a subset of a frequent k-item set.
- Pseudo-code:

```
        $C_k$: Candidate item set of size k
        $L_k$: frequent item set of size k
        $L_1$ = {frequent items};
        For(k = 1;$L_k$ != ∅; k++) do begin
        $C_{k+1}$ = candidates generated from $L_k$;
  For each transaction t in database do increment the count of all candidates in $C_{k+1}$ that are contained in t
     $L_{k+1}$ = candidates in $C_{k+1}$ with min_support
     End
     **Return**∪ k L k;
```

IV. CONCLUSION:

To enable the cloud server to perform asecure search among multiple owners' data encrypted with different secret keys. To rank the search results and preserve the privacy of relevance scores between keywords and files, the systemproposes a novel Additive Order and Privacy-Preserving Function family. The approach is efficient, even for large data and keyword sets.

V. ACKNOWLEDGMENT

To prepare proposed methodology paper on “Multiple Fuzzy Keyword Search Over Encrypted Data Using Date And Time " has been prepared by AnaghaRamnathKadve and Prof. Dr. S.B.Vanjale.

Author would like to thank my faculty as well as my whole department, parents, friends for their support. Author has obtained a lot of knowledge during the preparation of this document.

REFERENCES:

[1] J. Ye, J. Wang, J. Zhao, J. Shen, K-C Li “Fine-grained searchable encryption in amulti-user setting,” Soft Compute DOI 10.1007/s00500-016-2179-x, © Springer-Verlag Berlin Heidelberg 2016.

[2] G. Arthi et.al, “Efficient search of Data in Cloud Computing using Cumulative Key,” IJSTE - International Journal of Science Technology & Engineering, Volume 2, Issue 09, March 2016.

[3] J. Shen et.al, “Privacy-Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey,” 2015 First International Conference on Computational Intelligence Theory, Systems and Applications.

[4] W. Zhang et.al, “Secure Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing,” 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.

[5] W. Zhang, Y. Lin, “Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing,” Member, IEEE,JOURNAL OF LATEX CLASS FILES, VOL. 6, NO. 1, JANUARY 2015.

[6] “*A Survey on Secure Cloud: Security and Privacy in Cloud Computing*”,ShyamNandan Kumar1,*, Amit Vajpayee2,*American Journal of Systems and Software, 2016, Vol. 4, No. 1, 14-26* Available online at http://pubs.sciepub.com/ajss/4/1/2 © Science and Education Publishing DOI:10.12691/ajss-4-1-2

[7] “*A Survey on Multi-Keyword Search Tracking Based On Privacy Preserving in Cloud Computing*”,AnaghaRamnathKadve, Prof Dr. S.B. Vanjale,International Journal of Control Theory and Applications, ISSN : 0974-5572, International Science Press, Volume 9-Number 44-2016

[8] “An analysis of security issues for cloud computing”, Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1Hashizume et al. Journal of Internet Services and Applications 2013, 4:5,http://www.jisajournal.com/content/4/1/5

[9] ”Multi-Tenant Engineering Architecture in SaaS”**,**Sunil Kumar Khatri ,HimanshuSinghal ,KhushbooBahri, *International Journal of Computer Applications (0975 – 8887) International Conference on Reliability, Infocom Technologies and Optimization, 2013*

[10] “Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework”,NabeelKhana, Adil Al-Yasirib, Procedia Computer Science 94 (2016) 485 – 490 1877-0509 © 2016 Published by Elsevier B.V. doi: 10.1016/j.procs.2016.08.075 The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT’ 2016)

[11] “A survey on security issues in service delivery models of cloud computing”, S. Subashini n, V.Kavitha, 1084-8045 & 2010 Elsevier Ltd. All rights reserved. doi:10.1016/j.jnca.2010.07.006.