Secured Service Chains Tuned Resource Sharing using Nsdp

VijayAnand R, Prabhu J, MuthamilSelvan T, Thanapal P, Manivannan S.S

Abstract--***In the current network area, cloud service providers offer infinite storage space and computing power for users to manage their data in the cloud. To enjoy these services, individuals or organizations store their private data on cloud servers. However, in the case of security breaches, users' private data stored in the cloud are no longer safer. When users outsource their data to cloud servers, they expect complete privacy of their data stored in the cloud storage. To enjoy these services, individuals or organizations store their private data on cloud servers. The semantic-based keyword search over encrypted cloud data becomes of paramount importance. Protecting the privacy and data of users has remained a very crucial problem for cloud servers Additionally, the existing approaches only process them as single words, the flexibility of the encryption policy and the description of users' rights, and it changes from a one-one to one-many scenario during the encryption and decryption phases, calculation method to measure the semantic similarity between compound concepts. Keyword has been widely used in many scenarios, particularly in cloud computing. In this Project in the proposed scheme we use the trusted authority to generate the trapdoor .The generated trapdoor will be send to the user's e-mail ID, the user will search.***

I. INTRODUCTION:

In cloud computing outsourcing the important files then assigning some multiple keyword for that file easy retrieving while outsourcing the data into cloud storage that file will be encrypted Before outsourcing from cloud. The encryption purpose will be apply for preserving our data or files securely and then it will be placed in the cloud.

A semantic-based keyword search is not convenient for users but it will express their intentions exactly. We outsourcing our data frequently using dictionary means want to make some changes like editing and modifying the document users might with not finding their encrypted file easily so we using some search keyword for getting our file easily. When user apply the keyword for searching their file that will be automatically check with the multiple keyword weather that will be matching or not, it will be matching means user getting the file from the cloud storage. The global dictionary will be built by the collection of documents in the datasets we want to update any one document means it will cause reconstruction of the dictionary. We propose semantic similarity keyword search for encrypted data and outsourcing in the cloud storage. In cloud storage each document will contain multiple search keyword.

In existing scheme the will contain only one so it is very difficult to retrieve from the cloud storage and then providing low accuracy for the users it will more time to finding our document because it will be in encrypted form some traditional key is used for encryption comparing with existing scheme our semantic similarity search keyword having more advantages.

The semantic similarity applied in the keyword because it will contain multiple keyword that will be related with the file such as based on the features, local density, file length or depth, file path these are the keywords for assigning our files while outsourcing in cloud storage. When the file is outsourced in cloud in that time the owner will generate some key that will be giving to the trust authority each document having some unique traditional key. A research based compound concept semantic similarity method will improve the accuracy of retrieving the file semantic will introducing the keyword vector we propose semantic based keyword search for encrypting the data and ranked keyword search for efficient update in cloud storage while the user searching there file using multiple keyword it will provide exact file for the user using the compound keyword search technique. The compound concept semantic similarity and semantic based compound keyword search technique used to implement and test the datasets it will prove our result will be accurate and efficient while using these technique.

II. RELATED WORK:

A semantic based keyword search scheme is used to improve the privacy of our sensitive information's where we kept in cloud storage provider. The searchable method is increasing the easy retrieval of encrypted data. Privacy preserving keyword based semantic search over encrypted data will containing two clouds one is private cloud and another one is public cloud for storing the data over encrypted scheme using keyword search in private cloud storing the data's expand upon query keyword then the public cloud contain the query keyword set to retrieve the index easily using public keyword [12]. Finally matched file are return to the users in required order this technique is useful for storing data in both cloud. Then securing data using semantic expansion based search over encrypted method will outsourcing the data in public cloud over encrypted form it will built the index and construct the semantic relationship library for keyword search when user searching some file via entering their keyword for particular file automatically it will searching in the semantic relationship library and that was matching with the query keyword and extensional word both are used to retrieving the file easily from the public cloud security analysis will providing the privacy for the files using the keyword search technique [7].

Revised Manuscript Received on August 05, 2019.

Dr.VijayAnand R, School of Information Technology and Engineering ,Vellore Intitute of Technology ,Vellore-632014,

Dr. Prabhu J, School of Information Technology and Engineering ,Vellore Intitute of Technology ,Vellore-632014,

Dr. MuthamilSelvan T, School of Information Technology and Engineering ,Vellore Intitute of Technology ,Vellore-632014,

Dr. Thanapal P, School of Information Technology and Engineering ,Vellore Intitute of Technology ,Vellore-632014,

Dr. Manivannan S.S, School of Information Technology and Engineering ,Vellore Intitute of Technology ,Vellore-632014,

Retrieval Number J94100881019/2019©BEIESP
DOI: 10.35940/ijitee.J9410.0881019

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In cloud computing technology more organizations are outsourcing their file in cloud with the robust and fast accessing of data that will be encrypted over using minhash function securing the data privacy we propose the minhash for encrypted purpose but using only single keyword search that may cause the less accuracy of retrieving file from cloud. So we using multiple keyword search for the each document while we outsourcing the file in cloud in that time we entering some multiple keyword for searching the file from the global dictionary these files are automatically over encrypted form it will kept our file privacy and securely in the cloud storage [3]. In existing they are concentrated on achieving the keyword based search scheme but currently searchable encryption search is very popular in the field of cloud computing technology all of them are totally depending upon the some index and queries for searching their files from cloud but that was not provide more accurate result for the user so we implementing the conceptual graphs for solving the problem of semantic search encryption method [16]. When user searching some sentences or keyword for getting their file first that will be generated in a graph then the conceptual graph will be convert into some vector in this manner we getting accurate result for the users. The cloud computing is a very trustful method for outsourcing the users sensitive data’s searchable semantic encryption of the user data will be securing in the cloud so we use server side ranking based on order preserving encryption but it will also causing some data leakage from cloud and the we propose the two round searchable encryption method [8]. Vector space model provide the accurate result for the user based on their requirements.

The data leakage will be eliminate using this proposed model our data’s will be very safe and secured in the cloud system.

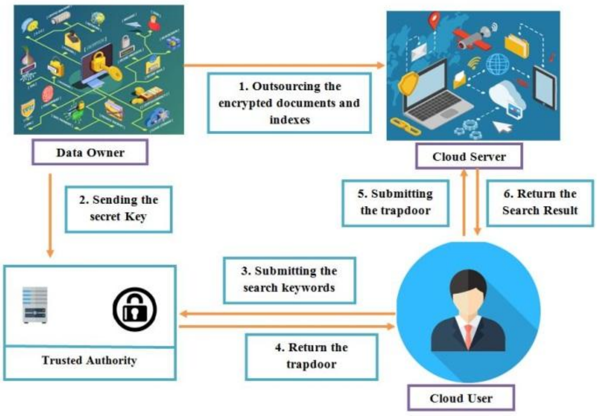

1. Outsourcing the encrypted documents and indexes
Data Owner
Cloud Server
2. Sending the secret Key
5. Submitting the trapdoor
6. Return the Search Result
3. Submitting the search keywords
4. Return the trapdoor
Trusted Authority
Cloud User

Fig.1 The model of keyword search.

In this model of keyword search method data owner is outsourcing the encrypted document and some search indexes to the cloud server for security purpose while data owner uploading their data in cloud in that time they providing some private key to the trust authority and then trust authority will regenerating the private key into the trapdoor key for each document.

Trust authority getting the private key from the data owner then that will be regenerate into the trapdoor key when user searching some file in that time trust authority will providing the certain key for the user and the user want to apply the key to cloud server and finally getting the required file from the cloud. The trapdoor key generation is the purpose of finding the user is authorized or not, if the user is authorized means them getting the file from the cloud server.

III. SEMANTIC SIMILARITY COMPOUND KEYWORD SEARCH SCHEME:

OVERVIEW:

In our scheme, data owner outsourcing the data to the cloud server in that time they fixing some keywords for the file that keyword will be related to the topic of the data. The vector keyword will be generated it will be equaling to the topic of the outsourced data it is very useful for the easy retrieval of user data from the cloud. The topic and keyword may change but the dimensionality of the keyword will not change we can delete or update the keyword or document will the help of the data update only possible in this scheme.

Each document having more than one keyword for searching the data from cloud server. Generation of the document index to be in the form of the multiple keyword vector will be present in only one vector fixing more than one keyword for the document is easy retrieval of the user required data from the cloud it will reducing the searching time and providing the accurate result for the user because of the generation of keyword vector will be present in only one vector in the compound keyword search method.

IV. SCKS SCHEME ALGORITHMS:

The scks scheme is mainly used for preserving and providing privacy for our outsourced data using encrypted form for these process they having some steps to achieve the result. The following algorithms are

KEYGENERATION: The key generation will be done by using some matrices each document having more than one keyword. The keyword will be must related to the topic for easy retrieval of the user data’s.

BUILDINDEX: The index will be generated based on the keyword vector multiple keyword will be with in only one vector. Each encrypted data will having the keywords the index will be generated based on the keyword.

TRAPDOOR: The trapdoor key will be generated for the security purpose for the cloud data the authorized user only having the trapdoor key. The private key will be given by the data owner to trust authority the key will be regenerate into the trapdoor key for authorized user for accessing the cloud files from the cloud server.

SEARCH: User can search their required file using multiple search keyword. Then the keyword must be related to the topic of the file so the searching will be very easy in the sematic compound keyword search technic.

V. SECURITY ANALYSIS:

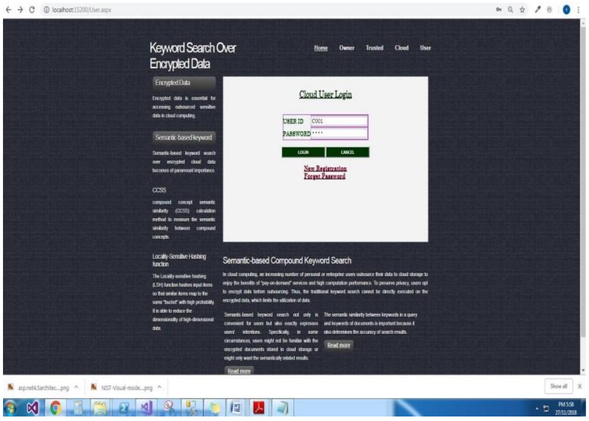
Cloud data’s will be fully secured by using the semantic compound keyword search scheme. When the data owner will be uploading their file using some private key for encryption purpose of the document while their uploading the file into the cloud in that time they fixing some keyword for easy retrieval of the file for the user when they are searching the file from the cloud server and then data owner providing some key to trust authority and then that key will be regenerate into trapdoor key. When the user required some file they want to get the trapdoor key from trust authority then that key will be apply into cloud then only the authorized user can view the document.

VI. SECURITY ENHANCED SE-SCKS:

In SE-SCKE method will be providing more security for the cloud data's while uploading the document to the cloud in that time them using some key for encryption and then fixing some keywords for the data retrieval. The authorized user only can access the required file based on the trapdoor key. Trapdoor key will be generated by the trust authority so it will be more secured and privacy in cloud server.

VII. SCREENSHOTS:

Cloud User Login Page



localhost:15200/User.aspx

Keyword Search Over Encrypted Data

Encrypted Data

Encrypted data is essential for accessing outsourced sensitive data in cloud computing.

Semantic-based keyword

Semantic-based keyword search over encrypted cloud data becomes of paramount importance.

CCSS

compound concept semantic similarity (CCSS) calculation method to measure the semantic similarity between compound concepts.

Locality-Sensitive Hashing function

The Locality-sensitive hashing (LSH) function hashes input items so that similar items map to the same "bucket" with high probability. It is able to reduce the dimensionality of high-dimensional data.

Cloud User Login

USER ID: C001
PASSWORD: ****

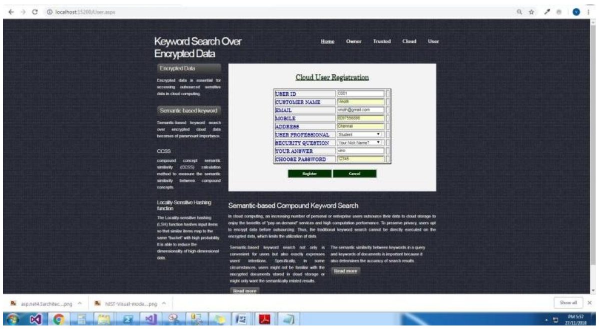
Semantic-based Compound Keyword Search

In cloud computing, an increasing number of personal or enterprise users outsource their data to cloud storage to enjoy the benefits of "pay-on-demand" services and high computation performance. To preserve privacy, users opt to encrypt data before outsourcing. Thus, the traditional keyword search cannot be directly executed on the encrypted data, which limits the utilization of data.

Semantic-based keyword search not only is convenient for users but also exactly expresses users' intentions. Specifically, in some circumstances, users might not be familiar with the encrypted documents stored in cloud storage or might only want the semantically related results.

The semantic similarity between keywords in a query and keywords of documents is important because it also determines the accuracy of search results.

Cloud User Registration Page



localhost:15200/User.aspx

Keyword Search Over Encrypted Data

Encrypted Data

Encrypted data is essential for accessing outsourced sensitive data in cloud computing.

Semantic-based keyword

Semantic-based keyword search over encrypted cloud data becomes of paramount importance.

CCSS

compound concept semantic similarity (CCSS) calculation method to measure the semantic similarity between compound concepts.

Locality-Sensitive Hashing function

The Locality-sensitive hashing (LSH) function hashes input items so that similar items map to the same "bucket" with high probability. It is able to reduce the dimensionality of high-dimensional data.

Cloud User Registration

USER ID	C001
CUSTOMER NAME	Vinoth
EMAIL	vinoth@gmail.com
MOBILE	8097556886
ADDRESS	Chennai
USER PROFESSIONAL	Student
SECURITY QUESTION	Your Nick Name?
YOUR ANSWER	vino
CHOOSE PASSWORD	12345

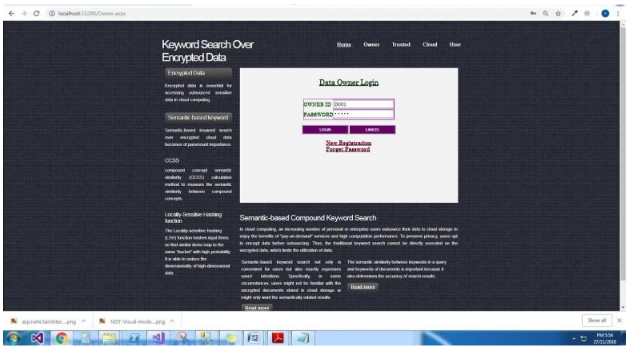
Semantic-based Compound Keyword Search

In cloud computing, an increasing number of personal or enterprise users outsource their data to cloud storage to enjoy the benefits of "pay-on-demand" services and high computation performance. To preserve privacy, users opt to encrypt data before outsourcing. Thus, the traditional keyword search cannot be directly executed on the encrypted data, which limits the utilization of data.

Semantic-based keyword search not only is convenient for users but also exactly expresses users' intentions. Specifically, in some circumstances, users might not be familiar with the encrypted documents stored in cloud storage or might only want the semantically related results.

The semantic similarity between keywords in a query and keywords of documents is important because it also determines the accuracy of search results.

Data Owner Login Page:



localhost:15200/Owner.aspx

Keyword Search Over Encrypted Data

Encrypted Data

Encrypted data is essential for accessing outsourced sensitive data in cloud computing.

Semantic-based keyword

Semantic-based keyword search over encrypted cloud data becomes of paramount importance.

CCSS

compound concept semantic similarity (CCSS) calculation method to measure the semantic similarity between compound concepts.

Locality-Sensitive Hashing function

The Locality-sensitive hashing (LSH) function hashes input items so that similar items map to the same "bucket" with high probability. It is able to reduce the dimensionality of high-dimensional data.

Data Owner Login

OWNER ID: D001
PASSWORD: *****

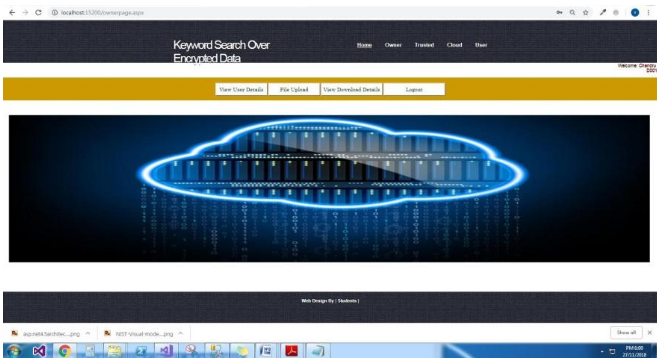
Semantic-based Compound Keyword Search

In cloud computing, an increasing number of personal or enterprise users outsource their data to cloud storage to enjoy the benefits of "pay-on-demand" services and high computation performance. To preserve privacy, users opt to encrypt data before outsourcing. Thus, the traditional keyword search cannot be directly executed on the encrypted data, which limits the utilization of data.

Semantic-based keyword search not only is convenient for users but also exactly expresses users' intentions. Specifically, in some circumstances, users might not be familiar with the encrypted documents stored in cloud storage or might only want the semantically related results.

The semantic similarity between keywords in a query and keywords of documents is important because it also determines the accuracy of search results.

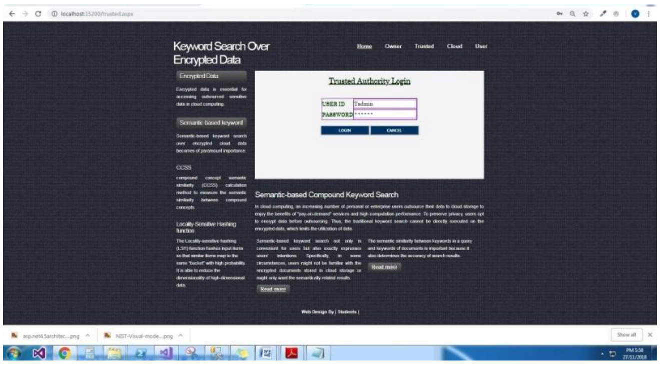
Data Owner Home Page:



localhost:15200/ownerpage.aspx

Keyword Search Over Encrypted Data

Trust Authority Login Page:



localhost:15200/trusted.aspx

Keyword Search Over Encrypted Data

Encrypted Data

Encrypted data is essential for accessing outsourced sensitive data in cloud computing.

Semantic-based keyword

Semantic-based keyword search over encrypted cloud data becomes of paramount importance.

CCSS

compound concept semantic similarity (CCSS) calculation method to measure the semantic similarity between compound concepts.

Locality-Sensitive Hashing function

The Locality-sensitive hashing (LSH) function hashes input items so that similar items map to the same "bucket" with high probability. It is able to reduce the dimensionality of high-dimensional data.

Trusted Authority Login

USER ID: Tadmin
PASSWORD: ******

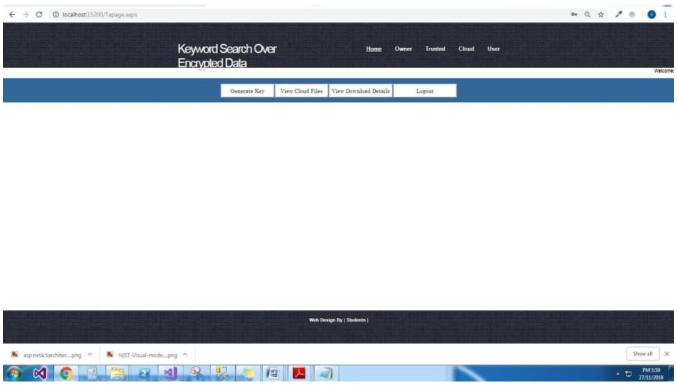
Semantic-based Compound Keyword Search

In cloud computing, an increasing number of personal or enterprise users outsource their data to cloud storage to enjoy the benefits of "pay-on-demand" services and high computation performance. To preserve privacy, users opt to encrypt data before outsourcing. Thus, the traditional keyword search cannot be directly executed on the encrypted data, which limits the utilization of data.

Semantic-based keyword search not only is convenient for users but also exactly expresses users' intentions. Specifically, in some circumstances, users might not be familiar with the encrypted documents stored in cloud storage or might only want the semantically related results.

The semantic similarity between keywords in a query and keywords of documents is important because it also determines the accuracy of search results.

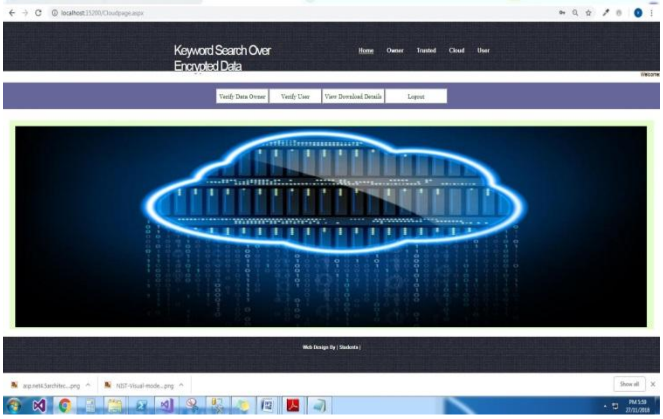
Trust Authority Home Page:



localhost:15200/Tapage.aspx

Keyword Search Over Encrypted Data

Cloud Admin login Page:



localhost:15200/Cloudpage.aspx

Keyword Search Over Encrypted Data

VIII. CONCLUSION:

We proposed a semantic based compound keyword search SCKS scheme is mainly used for the keyword based encrypting cloud data. It will provide exact result for the user. First they propose the ontology based compound concept semantic similarity method it will provide the similarity between compound concept then it will provide the accuracy result for the user then the variety information's will be in ontology. The SCKS scheme will providing the multiple keyword search option in the cloud in that file uploading time they fixing more than one keyword for the each document and then using some key for the encryption of the document when user require some file they want to get trapdoor key from the trust authority and then that will be apply into the cloud for getting the required document from the cloud server.

REFERENCES

1. R. Brindha and A. GhousiaSamrin,"Efficient privacy-preserving keyword search method for retrieving data from cloud",2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). March 2017.
2. L. Wu, Y. Zhang, K. K. R. Choo, et al. "Efficient and secure identity based encryption scheme with equality test in cloud computing". Future Generation Computer Systems, Pp- 22-31, 2017.
3. C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, and A. Y. Zomaya, "An efficient privacy-preserving ranked keyword search method," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 951–963, 2016.
4. S. Ma, Q. Huang, M. Zhang, and B. Yang," Identity-based encryption with outsourced equality test in cloud computing".IEEE,InformationSciences,pp- 389-402.2016.
5. Jevin D. West, Ian Wesley-Smith, Carl T. Bergstrom, "A Recommendation System Based On Hierarchical Clustering Of An Article-Level Citation Network", IEEE Transactions On Big Data, 2016.
6. Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu, Robert H. Deng, Fellow, "Duplication On Encrypted Big Data In Cloud", IEEE Transactions On Big Data, Vol. 2, No. 2, 2016.
7. Z. Fu, F. Huang, X. Sun, A. Vasilakos, and C. N. Yang, "Enabling semantic search based on conceptual graphs over encrypted outsourced data," IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2016.