Efficient Traceable Authorization Search System for Secure Cloud Storage

S. MUTHUKUMARAN, A. B. SANKESH, V. AJIN, RRANJITH KUMAR

Assistant Professor[1], Final Year[2]

Information technology, St Joseph College of Engineering, Sriperumbudur, Chennai.

ABSTRACT:

Watchword search over scrambled information is basic for getting to re-appropriated delicate information in distributed computing. In a few conditions, the watchwords that the clients look on are just semantically identified with the information as opposed to by means of a definite or fluffy coordinate. Thus, semantic-based watchword search over encoded cloud information is the fate of principal significance. Be that as it may, existing plots as a rule rely on a worldwide lexicon, which influences the exactness of list items as well as purposes wastefulness in information refreshing. Furthermore, albeit compound catchphrase search is basic by and by, the current methodologies just procedure them as single words, which split the first semantics and accomplish low exactness. To address these impediments, we at first propose a compound idea semantic similitude (CCSS) computation strategy to quantify the semantic comparability between compound ideas. Next, by coordinating CCSS with Locality-Sensitive Hashing capacity and the protected k-Nearest Neighbour plot, a semantic-based compound watchword search (SCKS) plot is proposed. SCKS accomplishes semantic-based hunt as well as multi- watchword search and positioned watchword search. Moreover, SCKS likewise disposes of the predefined worldwide library and can productively bolster information update. The test results on genuine world dataset demonstrate that SCKS presents low overhead on calculation and the inquiry precision outflanks the current plans.

INTRODUCTION:

Each element of the keyword vector corresponds to a field topic, and the value is the semantic similarity between the keyword and the topic. Because the keywords and field topics can be compound concepts. The compound is decomposed into subject headings and auxiliary words, and the relationships between them are used to measure the similarity. Moreover, CCSS comprehensively considers the information sources of ontology, such as taxonomical features, local density, path length and depth, which efficiently improves the ultimate accuracy.

EXISTING SYSTEM:

In existing system, the search keywords are usually semantically related to the document rather than via an exact or fuzzy match. For example, the predefined keyword of a document is “cloud-based storage”, and the keyword that a user search is “distributed storage”. Obviously, these two words are neither an exact nor a fuzzy match, but they are semantically related. Hence, the semantic-based keyword search is of practical importance and has attracted much attention. However, the existing

approaches must rely on a predefined global dictionary whose quality greatly influences the accuracy of the search result. Moreover, when the dataset is outsourced to the cloud, update operations that include inserting new documents and modifying and deleting existing documents are frequent. Because the predefined dictionary is constructed based on all documents in the dataset, the update of a single document can cause the reconstruction of the dictionary and even all document indexes, which is inefficient.

LIMITATIONS

- ✓ In schemes usually depend upon a global dictionary, which not only affects the accuracy ofsearch results but also causes inefficiency in data updating.
- ✓ The compound keyword search is common in practice, the existing approaches only processthem as single words, which split the original semantics and achieve low accuracy.

PROPOSED SYSTEM

In proposed system, the data owner publishes the encrypted documents and secure indexes to the cloud server. To reduce the computation burden, the data owner is allowed to outsource the generation of the trapdoor to TA by giving the private key to it. In this case, when a user wants to search over encrypted documents, he submits the keywords to TA which generates the corresponding trapdoor and returns it to the user. Then, the user sends the trapdoor to the cloud server. Finally, the cloud server executes the search algorithm with the trapdoor on all secure indexes and returns the relevant documents to the user. Since TA can obtain the private key, it should be entirely trustable, similar to the certificate authority (CA) of public key infrastructure (PKI). In applications, users or enterprises can choose TA according to this security requirement. TA is usually an internal server. If there is no such trustable server in the system, the trapdoor can be generated by the data owner.

ADVANTAGES:

- ✓ In advantage of SCKS is that it can support data update efficiently because no global dictionaryneed be predefined and each document is individually indexed.
- ✓ The query vector is generated similarly, which indicates SCKS can support multi-keyword search.
- ✓ To protect the privacy of documents and queries, (AES) technique could be chosen to encryptthem, which allows data servers perform some flexible functions over encrypted data

Module Description:

Modules:

1. Service request to TPA
2. TPA policy Creation

3. User file upload or file creator
4. KDC Key generation
5. Key revocation
6. Cloud Admin

SERVICE REQUEST TO TPA:

User will send request to Third Party Authenticator (TPA) for registration. The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Different policies for files, public key also differs. But for same public key for same policy will be generated. Then the client generates a private key by combining the username, password and security credentials. Then the file is encrypted with the public key and private key and forwarded to the cloud.

TPA POLICY CREATION:

TPA provides the rules and regulations to be followed by Creator, Reader and Writer. The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public key. The authenticated client can get the public key. Then the client can decrypt the file with the public key and the private key. The users credentials were stored in the client itself. During download the file the cloud will authenticate the user whether the user is valid to download the file. But the cloud doesn't have any attributes or the details of the user.

USER FILE UPLOAD OR FILE CREATOR:

File creator after getting proper authentication uploads his files in the cloud. The policy of a file may be revoked under the request by the client, when expiring the time period of the contract or completely move the files from one cloud to another cloud environment. When any of the above criteria exists the policy will be revoked and the key manager will completely removes the public key of the associated file. So no one recover the control key of a revoked file in future. For this reason we can say the file is assuredly deleted.

KDC KEY GENERATION:

Key Distribution Centres which are decentralized generate different keys to different types of user after getting tokens from users. To recover the file, the client must request the key manager to

generate the public key. For that the client must be authenticated. The attribute based encryption standard is used for file access which is authenticated via an attribute associated with the file. With file access control the file downloaded from the cloud will be in the format of read only or write supported. Each user has associated with policies for each file. So the right user will access the right file. For making file access the attribute based encryption scheme is utilized.

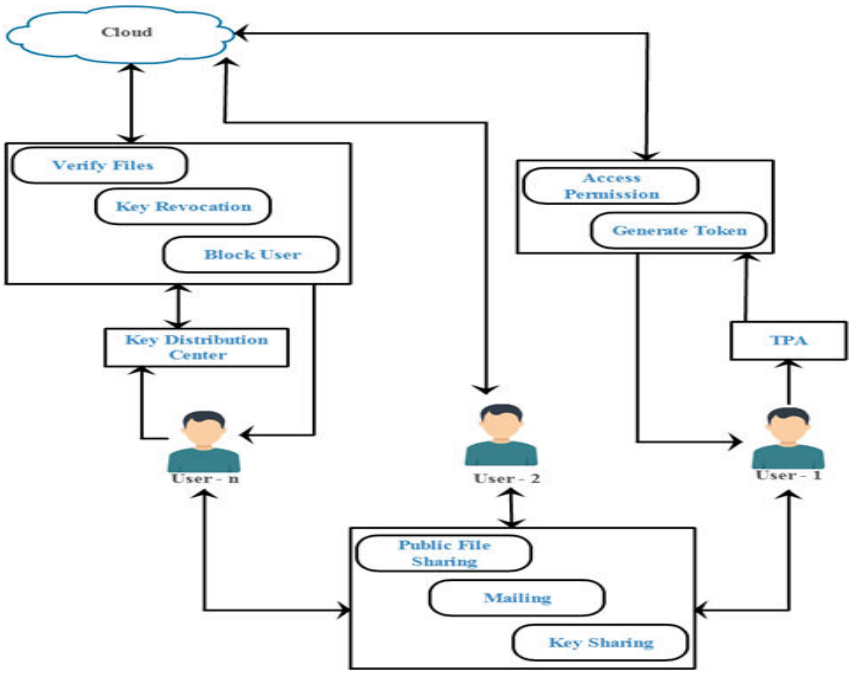
KEY REVOCATION:

Ability to limit and control the access to host systems and applications via communication links. To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files.

CLOUD ADMIN:

Cloud admin has the list of key distribution centers and TPA. Admin sets the norms to be followed by TPA and KDC. It monitors the key generation policies and informs abnormal behaviours.

SYSTEM ARCHITECTURE:



WHITE BOX TESTING

This type of testing ensures that

- All independent paths have been exercised at least once
- All logical decisions have been exercised on their true and false sides

- All loops are executed at their boundaries and within their operational bounds
- All internal data structures have been exercised to assure their validity.

To follow the concept of white box testing we have tested each form .we have created independently to verify that Data flow is correct, All conditions are exercised to check their validity, All loops are executed on their boundaries.

BASIC PATH TESTING

Established technique of flow graph with Cyclomatic complexity was used to derive test cases for allthe functions. The main steps in deriving test cases were:
Use the design of the code and draw correspondent flow graph.
Determine the Cyclomatic complexity of resultant flow graph,
using formula:V(G)=E-N+2 or
V(G)=P+1 or
V(G)=Number Of Regions
Where V(G) is Cyclomatic
complexity,E is the number
of edges,
N is the number of flow
graph nodes,P is the
number of predicate nodes.
Determine the basis of set of linearly independent paths.

CONCLUSION:

Concentrating on the catchphrase search over encoded cloud information, we propose a semantic- based compound watchword search (SCKS) conspire. To precisely separate the semantic data of watchwords, we initially propose an philosophy based compound idea semantic comparability figuring technique (CCSS), which significantly improves the precision of closeness estimation between compound ideas by exhaustively thinking about the compound highlights what's more, an assortment of data sources in metaphysics. At that point, the SCKS plan is developed by coordinating CCSS with LSH and SkNN. Notwithstanding a semantic-based watchword search, SCKS can accomplish multi-watchword search and positioned watchword search simultaneously. Since each report is filed exclusively, the update of one archive will not influence different archives, which implies that SCKS can bolster dynamic information productively. To improve the security of SCKS, we propose a security-upgraded SCKS (SE-SCKS) by presenting a pseudo-irregular capacity. Careful security investigation of both SCKS and SE-SCKS is given, and the trials on genuine world dataset show that the proposed methodologies present low overhead on calculation and that the inquiry exactness beats the current plans.

FUTURE WORK:

In Local Area Network, the proposed hybrid encryption mechanism may be customized for transferring the sensitive data from work station to host based applications. In web based applications, the proposed mechanism enables the transfer of sensitive data from user to user, from user to server and from server to server which are located outside of the organization. In a cloud environment, more number of people are accessing the web server locally or globally to share the

sensitive data. The proposed hybrid encryption technique is very helpful to enhance the security forweb based transactions in future.

REFERENCES

[1] Q. Chai and G. Gong, "Verifiable symmetric searchable encryptionfor semi-honest-but- curious cloud servers," in Communications (ICC), 2012 IEEE International Conference on. IEEE , 2012, pp. 917– 922.

[2] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keyword search for confidential investigation of remote forensics," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on.IEEE, 2011, pp. 595–599.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[4] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE.

[5] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55,2008.

[6] X. Yu and Q. Wen, "Design of security solution to mobile cloud storage," in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[7] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[8] O. Mazhelis, G. Fazekas, and P. Tyrvainen, "Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage," in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[9] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in- cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[10] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice

versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.