IJSEAT International Journal of Science Engineering and Advance Technology

A Scalable Framework to Allow Users for Keyword Search With Access Control Over Encrypted Data

[1]G.Manikanta, [2]P.RadhikaKrupalani

[1]FinalMSc(CS), Ideal College of Art & Sciences, , Ideal College of Arts and Sciences., Vidyuth Nagar, Kakinada, E.G.Dist., A.P., India.

[2]Associate professor, Dept of Computer science, Ideal College of Arts and Sciences., Vidyuth Nagar, Kakinada, E.G.Dist., A.P., India.

ABSTRACT:
In certain conditions, the keywords that the client searches on are just semantically identified with the data instead of through a definite or fluffy match. Subsequently, semantic-based keywordsearch over encoded cloud data is the fate of central significance. Be that as it may, existing plans as a rule rely on a worldwide word reference, which influences the precision of indexed lists as well as purposes wastefulness in data refreshing. Also, albeit compound keywordsearch 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 Concept Semantic Similarity (CCSS) estimation strategy to gauge the semantic closeness between compound ideas. Next, by incorporating CCSS with Locality-Sensitive Hashing (LSH) capacity and the safe k-Nearest Neighbor conspire, a Semantic-based Compound Keyword Search (SCKS) plot is proposed. SCKS accomplishes semantic-based search as well as multi-keywordsearch and positioned keywordsearch. Furthermore, SCKS likewise disposes off the predefined worldwide library and can effectively bolster data update.

KEYWORDS: Semantic similarity, Searchable encryption, Private key

1] INTRODUCTION:

In cloud computing, an expanding number of individual or venture clients re-appropriate their data to cloud storage to appreciate the advantages of "pay-on-request" administrations and high calculation execution. To safeguard security, clients select to encode data before redistributing. Accordingly, the conventional keywordsearch can't be straightforwardly executed on the encoded data, which constrains the usage of data. To address this issue, Song et al. [1] proposed the possibility of accessible encryption (SE) that enables clients to search on encoded data through a keyword. In this manner, different accessible encryption plans were proposed to meet diverse necessities, for example, fluffy keywordsearch [2]– [4], multikeyword search [5]– [8], positioned keywordsearch [9]– [11], and semantic-based keywordsearch [12]– [17]. By and by, semantic-based keyword scan not exclusively is advantageous for clients yet in addition precisely communicates clients' goals. In particular, in certain conditions, clients probably won't be comfortable with the scrambled records put away in cloud storage or may just need the semantically related outcomes; in this manner, the searchkeywords are typically semantically identified with the archive as opposed to by means of a careful or fluffy match.

2] LITERATURE SURVEY:

[1] C. Wang we research the issue of secure and effective likeness search over re-appropriated cloud data. Likeness search is a principal and incredible asset broadly utilized in plaintext data recovery, yet has not been very investigated in the encoded data area. Our component plan first endeavors a smothering method to fabricate capacity productive comparability keyword set from a given report gathering, with alter remove as the similitude metric. In light of that, we at that point manufacture a private trie-navigate searching record, and show it accurately accomplishes the characterized closeness search usefulness with steady inquiry time multifaceted nature. We formally demonstrate the protection safeguarding assurance of the proposed system under thorough security treatment. To exhibit the all-inclusive statement of our system and further enhance the application range, we likewise demonstrate our new development normally bolsters fluffy pursuit, a recently examined idea pointing just to endure grammatical errors and portrayal irregularities in the client searching input.

[2] J. Yuwe center around tending to data protection issues utilizing SSE. Out of the blue, we define the protection issue from the part of comparability significance and plan strength. We observe that server-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a two-round searchable encryption (TRSE) scheme that supports top-k multikeyword retrieval. In TRSE, we utilize a vector space display and homomorphic encryption. The vector space show gives adequate pursuit exactness, and the homomorphic encryption empowers clients to include in the positioning while most of figuring work is done on the server side by activities just on ciphertext. Subsequently, data spillage can be disposed of and data security is guaranteed.

3] PROBLEM DEFINTION:

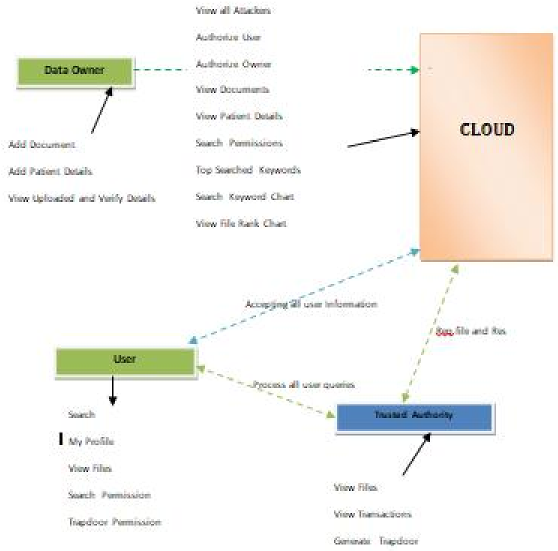
When all is said and done, the plans going for multi-keywordsearch can likewise accomplish positioned keywordsearch. Orencik et al. [7] used the MinHash capacity and Term Frequency-Inverse Document Frequency (TF-IDF) to build a record file. Nonetheless, the TF-IDF ought to be recalculated when archives or keywords are included or evacuated, which causes andata refreshing trouble.

[3]Yu et al.proposed a tworound pursuit plot utilizing homomorphic encryption to help multi-keywordsearch. This plan additionally embraces TF-IDF; along these lines, it can't proficiently bolster data refreshing. In the plan proposed by Cao et al. [4], each archive is related with a twofold vector of which the dimensionality is equivalent to the quantity of keywords in the worldwide keyword set. Henceforth, the worldwide keyword set ought to be static since its including or erasing will cause the reproduction of the report record. By bringing apportioned lattices into [5], Li et al. [6] improved proficiency when new keywords and records are included, which lightens the issue of database update.

4] PROPOSED APPROACH:

The framework proposes Semantic-based Compound Keyword Search (SCKS) plot over scrambled data in this paper. SCKS utilizes a subject set in a field and Vector Space Model (VSM) to express the semantic data of keywords. Every component of the keyword vector relates to a field subject, and the esteem is the semantic similitude between the keyword and the theme. Since the keywords and field subjects can be compound ideas, we at first propose a metaphysics based Compound Concept Semantic Similarity (CCSS) estimation strategy to gauge their semantic likeness [24]. In CCSS, the compound is decayed into subject headings and helper words, and the connections between them are utilized to gauge the similitude. Besides, CCSS completely considers the data wellsprings of cosmology, for example, taxonomical highlights, nearby thickness, way length and profundity, which effectively improves a definitive exactness.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

MODULES:

Data Owner

The dataowner performs activities, for example, Add Document, Add Patient Details, View Uploaded and Verify Details

User

He signs in by utilizing his/her client name and secret key. After Login collector will perform tasks like Search, My Profile, View Files, Search Permission, Trapdoor Permission

Trusted Authority

The division can do following activities, for example, View Files, View Transactions, and Generate Trapdoor

Cloud

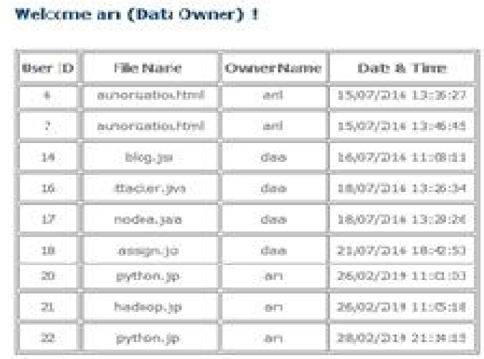
The Admin deals with a server to give data stockpiling administration and can likewise do the accompanying activities, for example, View all Attackers, Authorize User, Authorize Owner, View

Documents, View Patient Details, Search Permissions, Top Searched Keywords, Search Keyword Chart, View File Rank Chart

7] COMPOUND KEYWORD SEARCH ALGORITHM:

INPUT:TA,D,SK,I,T,Q,K
Step1: Generation of keyword vector with field topics.
Step2: Trusted authority generates key used to send data owner.
Step3: Data owner upload the encrypted document and encrypted keyword index to cloud.
Step4:trusted authority generates trapdoor based on keyword set.
Step5: User sends the query keyword which retrurns trapdoor by authority.
Step6: Cloud accept the trapdoor and returns the searched and relevant document to user.
Step7: User decrypt the document by using secret key.

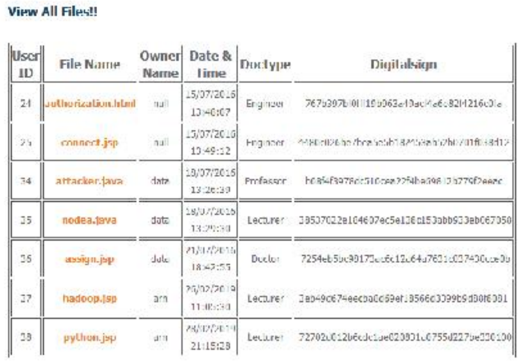
8]RESULTS



Welcome ani (Data Owner) !

User ID	File Name	Owner Name	Date & Time
6	aunorizatioi.html	ani	15/07/2016 13:36:27
7	aunorizatioi.html	ani	15/07/2016 13:46:45
14	blog.jsp	daa	16/07/2016 11:08:11
16	ttacker.jvs	daa	18/07/2016 13:26:34
17	nodea.java	daa	18/07/2016 13:29:26
18	assign.jp	daa	21/07/2016 18:42:53
20	python.jp	an	26/02/2019 11:01:03
21	hadoop.jp	an	26/02/2019 11:05:18
22	python.jp	an	28/02/2019 21:34:15

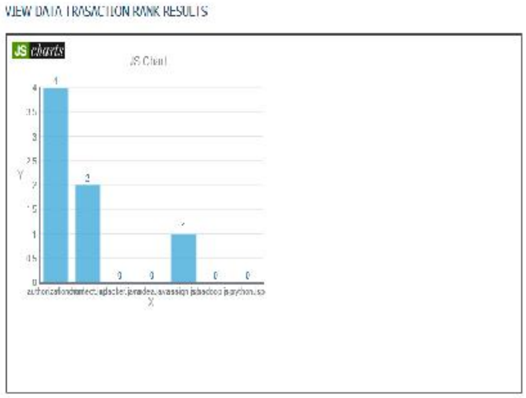
Upload file view



View All Files!!

User ID	File Name	Owner Name	Date & Time	Doctype	Digitalsign
24	authorization.html	null	15/07/2016 13:46:07	Engineer	767b397b0[illegible]19b063a49ac4a6c82f4216c0a
25	connect.jsp	null	15/07/2016 13:49:12	Engineer	[illegible]
34	attacker.java	data	18/07/2016 13:26:39	Professor	b68f4f3978dc510cea22f4ba98[illegible]b779f2eeac
35	nodea.java	data	18/07/2016 13:29:30	Lecturer	38537022a104607ec5e136d153abb933eb067050
36	assign.jsp	data	21/07/2016 18:42:55	Doctor	7254eb5bc90173[illegible]c037430cce0b
37	hadoop.jsp	ani	26/02/2019 11:05:30	Lecturer	3eb49c674eecba0c69ef[illegible]3566d3099b9d30f6301
38	python.jsp	ani	28/02/2019 21:15:28	Lecturer	72702c012b6cdc1ae020801c0755d227be330100

View all file uploaded



View data transaction rank result

9] CONCLUSION:

We propose a Semantic-based Compound Keyword Search (SCKS) plot in this paper. To precisely remove the semantic data of keywords, we first propose a ontology-based Compound Concept Semantic Similarity calculation method (CCSS),which incredibly improves the exactness of likeness estimation between compound ideas by exhaustively considering the compound highlights and an assortment of data sources in metaphysics. At that point, the SCKS plot is built by coordinating CCSS with LSH and SkNN. Notwithstanding a semantic-based keywordsearch, SCKS can accomplish multi-keywordsearch and positioned keywordsearch in the meantime. Since each report is listed independently, the update of one archive won't influence different records, which implies that SCKS can bolster dynamic data efficiently.

10] REFERENCES:

[1] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[2] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud,” in IEEE International Conference on Computer Communications, 2014, pp. 2112–2120.

[3] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient similarity search over encrypted data,” in IEEE 28th International Conference on Data Engineering (ICDE), 2012, pp. 1156–1167.

[4] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity

search over outsourced cloud data," in 2012 Proceedings of IEEE INFOCOM, 2012, pp. 451–459.

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

[6] R. Li, Z. Xu, W. Kang, K. C. Yow, and C. Z. Xu, "Efficient multikeyword ranked query over encrypted data in cloud computing," Future Generation Computer Systems, vol. 30, no. 1, pp. 179–190, 2014.

[7]C.Orencik,M.Kantarcioglu,andE.Savas,"Apractica landsecure multi-keyword search method over encrypted cloud data," in IEEE Sixth International Conference on Cloud Computing (CLOUD), 2013, pp. 390–397.

[8] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Toward secure multikeywordtop-kretrievaloverencryptedclouddata,"IEEETransactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239–250, 2013.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," inIEEE30thInternational Conference on Cloud Computing Systems (ICDCS), 2010, pp. 253–262.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in ACM SIGMOD International Conference on Management of Data, 2004, pp. 563–574.

[11] 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 Cloud Systems, vol. 27, no. 4, pp. 951–963, 2016.

[12] X.Sun,Y.Zhu,Z.Xia,andL.Chen,"Privacy-preserving keyword based semantic search over encrypted cloud data," International Journal of Security & Its Applications, vol. 8, no. 3, pp. 9–20, 2014.

[13] Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," J. Cloud Comput., vol. 3, no. 1, pp. 8:1–8:11, 2014.

[14] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol. 60, no. 1, pp. 164–172, 2014.

[15] Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data," IEEE Transactions on Consumer Electronics, vol. 60, no. 4, pp. 762–770, Nov 2014.

Mr.G.Manikanta is a student of Ideal college of Arts & Sciences, Kakinada Presently he is pursuing his MSc(Computer Science) from this college and he passed BSc(MECs) from P.R Govt College(A)Kkd, affiliated to Adhikavi Nannaya University, Rajamahendravaram in the year 2017. His areas of interest includes Information security&Cryptograpy, all current trends and techniques in Computer Science.

Mrs. P. Radhika Krupalini is an Associate Professor ofComputerScience Department at Ideal College of Arts & Sciences, Kakinada, AP, INDIA. She obtained her MCA from Andhra University M.Tech (CSE) from University College of Engineering, JNTUK. She qualified AP SET in Computer Science and Applications. She has 13+ years of teaching experience at Post Graduate Level. Her areas of interest are Operating Systems, Network Security & Cryptography, Artificial Intelligence, Cloud computing and Data Mining.