Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

PRIVACY PRESERVING SEARCH OVER ENCRYPTED DATA ON CLOUD.

Rajendra Hiray1st, Kedar Jangam2nd, Ajinkya Ingle3rd , Ravina Dhage4th , Prof. R.T.Umbare

JSPM Rajarshi Shahu College of Engineering Tathawade, Pune

Abstract:- *Cloud computing provides individuals and enterprises Brobdingnagian computing power and scalable storage capacities to support a variety of big information applications in domains like health care and scientific analysis, therefore extra and extra information owners unit involved to to supply their information on cloud servers for wonderful convenience in information management and mining. However, information sets like health records in electronic documents usually contain sensitive information, that brings relating to privacy issues if the documents unit free shared to partly untrusted third-parties in cloud. a wise and wide used technique for information privacy preservation is to inscribe information before outsourcing to the cloud servers, that however reduces information utility and makes several ancient information analytic operators like keyword-based top-k document retrieval obsolete. throughout this paper, we tend to tend to analyze the multi-keyword top-k search downside for enormous cryptography against privacy breaches, associated decide to verify Associate in Nursing efficient and secure answer to the present disadvantage. Specifically, for the privacy concern of question information, we tend to tend to construct a special tree-based index structure and magnificence a random traversal formula, that makes even the same question to produce whole completely different visiting ways that on the index, and may also maintain the accuracy of queries unchanged beneath stronger privacy. For up the question efficiency, we tend to tend to tend to propose a gaggle multi-keyword top-k search theme supported set up of partition where a gaggle of tree-based indexes unit created for all documents. Finally, we tend to tend to combine these ways that on into Associate in Nursing efficient and secure approach to handle our projected top-k similarity search. thorough experimental results on real-life information sets demonstrate that our projected approach can significantly improve the potential of defensive the privacy breaches, the quality and also the time efficiency of question method over the progressive ways that.*

Keywords:- *Cloud data sharing, CP-ABE, Key management, Security, efficiency.*

I INTRODUCTION

CLOUD computing has emerged as a troubled trend inboth IT industries and analysis communities recently,its salient characteristics like high measurability and pay-asyou-gofashion have enabled cloud customers to buy the powerful computing resources as services accordingto their actual needs, such cloud users haveno longer got to worry regarding the wasting on computingresources and also the quality on hardware platform management. Nowadays, a lot of and a lot of corporations and people from an oversized range of huge information application shave source their information and deploy their services into cloud servers for simple information management, efficient data {processing} and question processing tasks. encryption has been wide used for information privacy preservation in information sharing situations, it refers to mathematical calculation and algorithmic theme that rework plaintext into cypher text, that could be a non-readable kind to unauthorized parties. a spread {of information|of knowledge|of information} secret writing models are planned and that they square measure accustomed encryptthe data before outsourcing to the cloud servers. However, applying these approaches for encryption sometimes causetremendous price in terms of knowledge utility, that makes ancient processing strategies that square measure designed forplaintext information not work spill encrypted information .

Data encryption has been wide used for data privacy preservation in data sharing things, it refers to mathematical calculation and algorithmic theme that transform plaintext into cyphertext, which will be a non-readable sort to unauthorized parties. a variety of information secret writing models are planned [3], [4], [5] which they unit accustomed write in code the information before outsourcing to the cloud servers. However, applying these approaches for secret writing generally cause tremendous value in terms of information utility, that creates ancient process ways that unit designed for plaintext data not work spill encrypted data.Data encryption has been wide used for data privacy preservation in data sharing things, it refers to mathematical calculation and algorithmic theme that transform plaintext into cyphertext, which will be a non-readable sort to unauthorized parties. a variety of information secret writing models are planned [3], [4], [5] which they unit accustomed write in code the information before outsourcing to the cloud servers. However, applying these approaches for secret writing generally cause tremendous value in terms of information utility, that creates ancient process ways that unit designed for plaintext data not work spill encrypted data.

Actually sizable amount of on-demand information users and big amount of knowledge documents within the cloud, this problem is challenging. it's essential for the search facility to allow multi keyword search question and create accessible result comparison ranking to visualize the effective information retrieval requirement. To develop the search result accuracy yet as to enrich the user looking expertise, it is also essential for such ranking system to support multiple keywords search, as single keyword search frequently yields extreme coarse results. The searchable cryptography method supports to present encrypted information as documents and agrees a user to firmly search over single keyword and retrieve documents of concern.

II LITERATURE SURVEY

Paper1:A Secure and Dynamic Multi Keyword Ranked Search Scheme over encrypted.

The major aim of this paper is to resolve the matter of multi-keyword hierarchal search over encrypted cloud information (MRSE) at the time of protecting actual technique wise privacy inside the cloud computing construct. information holders unit impressed to supply their powerful information management systems from native sites to the business public cloud for large flexibility and financial savings. except for protective information privacy, sensitive information ought to be encrypted before outsourcing, which performs ancient information utilization supported plaintext keyword search. As a result, allowing Associate in Nursing encrypted cloud information search service is of supreme significance. visible of the huge vary of knowledge users and documents inside the cloud, it's essential to permit several keywords inside the search demand and are available back documents inside the order of their acceptable to those keywords. Similar mechanism on searchable cryptography makes centre on single keyword search or Boolean keyword search, and sometimes sort the search results. inside the center of assorted multi-keyword linguistics, deciding the well-organized similarity live of coordinate matching, it means that as many matches as achievable, to capture the appropriate information documents to the search question. notably, we have a tendency to think about real similarity i.e., the amount of question keywords shows in a very document, to quantitatively estimate such match live that document to the search question. Through the index construction, every document is connected with a binary vector as a sub index where as characterize whether or not or not matching keyword is contained inside the document.

Paper2: Privacy-Preserving Multi-keyword Ranked Search Over Encrypted Cloud Data,

The innovation in cloud computing has encouraged the data owners to outsource their data managing system from local sites to profitable public cloud

for excessive flexibility and profitable savings. But people can like full benefit of cloud computing, if we are able to report very real secrecy and security concerns that come with loading sensitive personal information. Allowing an encrypted cloud data search facility is of great significance. In view of the huge number of data users, documents in the cloud, it is important for the search facility to agree multi keywords query and arrange for result compare.

-Paper3: Secure Indexes.

A secure index could be a arrangement that enables a speaker with a trapdoor for a word x to check in O(1) time providing the index contains x; The index reveals no data concerning its contents while not valid trapdoors, and trapdoors will solely be generated with a secret key. Secure indexes ar a natural extension of the matter of constructing information structures with privacy guarantees like those provided by oblivious and history freelance information structures. during this paper, we tend to formally outline a secure index and formulate a security model for indexes referred to as linguistics security against adaptive chosen keyword attack (ind-cka). we tend to conjointly develop associate economical indcka

secure index construction referred to as z-idx victimisation pseudo-random functions and Bloom filters, and show the way to use z-idx to implement searches on encrypted information. This search theme is that the best encrypted information search theme presently known; It provides O(1) search time per document, and handles compressed information, variable length words, and Boolean and sure regular expression queries. The techniques developed during this paper also can be accustomed build encrypted searchable audit logs, personal info question schemes, accumulated hashing schemes, and secure set membership tests.

Paper4: Fuzzy Identity-Based Encryption.

A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

III EXISTING SYSTEM

In existing System, the keyword-based search is such one widely used applications, and its traditional processing methods cannot be directly applied to encrypted data. Therefore, howto process such queries over encrypted data and at the same time guarantee data privacy becomes a hot research topic. Fortunately, many methodologies based on searchable encryption have been studied. the single keyword search is not smart enough to support advanced queries and the boolean search is unrealistic since it causes high communication cost. Therefore,more recent works like focus on the multi keyword ranked search, which is more practical in pay-asyou-go cloud paradigm

Existing System Disadvantages:

- Single keyword search is not smart enough to support advanced queries .
- Boolean search is unrealistic since it causes high communication cost

IV OBJECTIVE

1. Big data encryption against privacy break.
2. Improve the capability of defending the privacy break.
3. Improve scalability and the time efficiency of query processing.

V PROPOSED SYSTEM

we investigate the multi-keyword top-k search disadvantage for big cryptography against privacy break, associated plan to confirm Associate in Nursing efficient and secure answer to this disadvantage. Specifically, for the privacy concern of question data, we have a tendency to tend to construct a special tree-based index structure and elegance a random traversal formula, that creates even a similar question to provide wholly completely different visiting ways that on the index, and will in addition maintain the accuracy of queries unchanged below stronger privacy. For rising the question efficiency, we have a tendency to tend to propose a gaggle multi-keyword top-k search theme supported the thought of partition, where a gaggle of tree-based indexes ar created for all documents. Finally, we have a tendency to tend to combine these ways on into associate efficient and secure approach to handle our planned top-k similarity search. full experimental results on real-life data sets demonstrate that our planned approach can significantly improve the potential of defensive the privacy breaches, the quality and so the time efficiency of question method over the progressive ways.

Proposed System Advantages:

1. Multi-keyword top-k Search.
2. Search efficiency.
3. Privacy Preserving.
4. Index security and Query security.

V ALGORITHMS

Algorithm 1: AES Algorithm
Alogrithm Steps

Step 1: Start

Step 2: Derive the set of round keys from the cipher key.

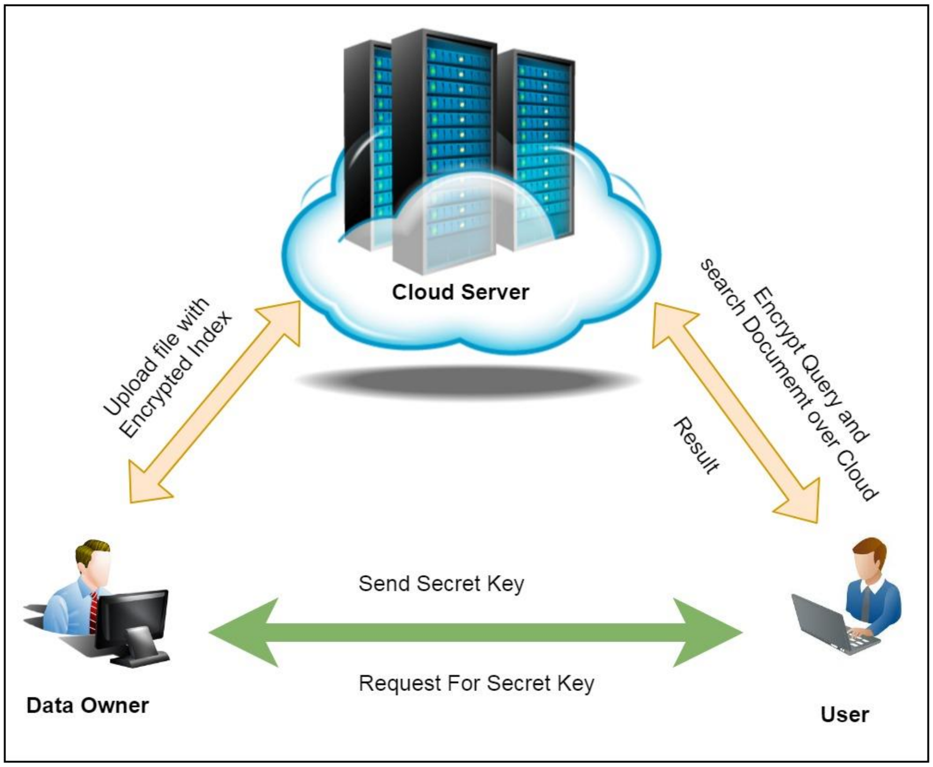
Step 3: Initialize the state array with the block data (plaintext). .

Step 4:Add the initial round key to the starting state array.

Step 5: Add the initial round key to the starting state array.

Step 6:Perform the tenth and final round of state manipulation..

Step 7: Copy the final state array out as the encrypted data (ciphertext).


Cloud Server
Upload file with Encrypted Index
Encrypt Query and search Document over Cloud
Result
Send Secret Key
Request For Secret Key
Data Owner
User

System Requirement and Specification

Hardware resources required

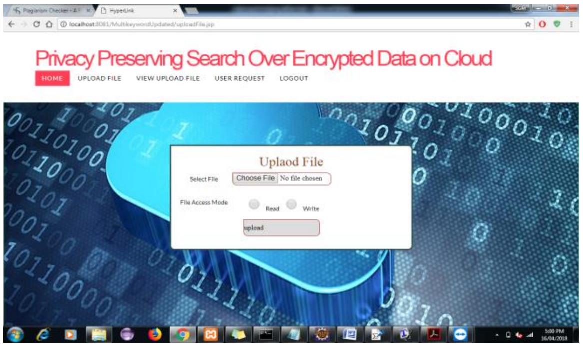
1.	Processor	:	Pentium –IV
2.	Speed	:	1.1 GHz
3.	RAM	:	256 MB(min)
4.	Hard Disk	:	20 GB
5.	Key Board	:	Standard Windows Keyboard
6.	Mouse	:	Two or Three Button Mouse
7.	Monitor	:	SVGA

Software resources required

1.	Operating System	:	Windows 07/08/Above
2.	Programming Language	:	JAVA/J2EE/XML
3.	Database	:	MY SQL

VI CONCLUSION AND FUTURE SCOPE

we target rising the efficiency and the security of multi-keyword top-k similarity search over encrypted information. At first, we have a tendency to propose the random traversal formula which might bring home the bacon that for 2 identical queries with completely different keys, the cloud server traverses different paths on the index, and also the information user receives different results however with constant high level of question accuracies within the unit of time.

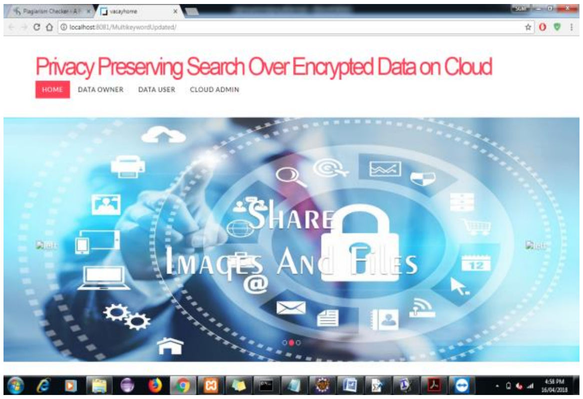


Privacy Preserving Search Over Encrypted Data on Cloud

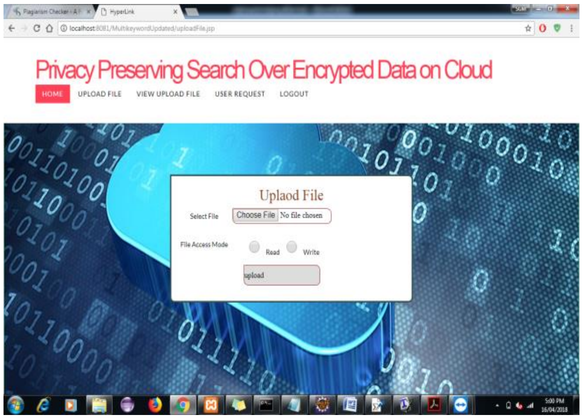
Uplaod File

Select File: No file chosen

File Access Mode: ○ Read ○ Write



Privacy Preserving Search Over Encrypted Data on Cloud

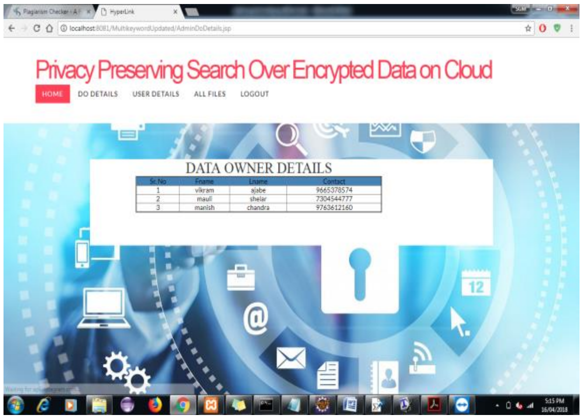


Privacy Preserving Search Over Encrypted Data on Cloud

Uplaod File

Select File: No file chosen

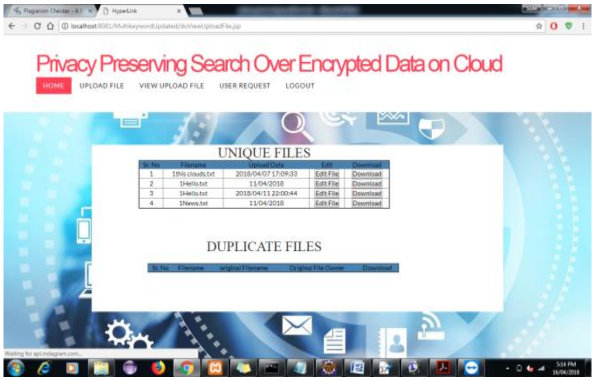
File Access Mode: ○ Read ○ Write



Privacy Preserving Search Over Encrypted Data on Cloud

DATA OWNER DETAILS

Sr.No	Fname	Lname	Contact
1	vikram	ajabe	9665378574
2	mauli	shelar	7304544777
3	manish	chandra	9763612160



Privacy Preserving Search Over Encrypted Data on Cloud

UNIQUE FILES

Sr. No	Filename	Upload Date	Edit	Download
1	1this clouds.txt	2018/04/07 17:09:33	Edit File	Download
2	1Hello.txt	11/04/2018	Edit File	Download
3	1Hello.txt	2018/04/11 22:00:44	Edit File	Download
4	1News.txt	11/04/2018	Edit File	Download

DUPLICATE FILES

Sr. No	Filename	original Filename	Original File Owner	Download

VII ACKNOWLEDGEMENTS

This work is supported by Prof. R.T.Umbare
(JSPM Collage,Tathawade,pune)

VIII REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,”in Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006, pp. 79–88.

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

[3] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[4] 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 Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[5] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016

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

[7] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive,vol. 2003, p. 216, 2003.

[8] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keywordsearches on remote encrypted data,” in Applied Cryptography andNetwork Security. Springer, 2005, pp. 442–455

[9] Y. H. Hwang and P. J. Lee, “Public key encryption with conjunctivekeyword search and its extension to a multi-user system,” inPairing-Based Cryptography–Pairing. Springer, 2007, pp. 2–22.

[10] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keywordsearch over encrypted data,” in Applied Cryptography and NetworkSecurity. Springer, 2004, pp. 31–4