IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101270

Multikeyword Searching Over Encrypted Data With Privacy Preserving

Mrs.Vijaya Sayaji Chavan[1], Mr.Mohan Kashinath Mali[2]

Professor, Computer Technology Department , Bharati Vidyapeeths Institute of Technology, Navi, Mumbai, India[1]

Professor, Information Technology Department , Bharati Vidyapeeths Institute of Technology, Navi, Mumbai, India[2]

Abstract: In cloud computing, most of the data owners keeps their sensitive data on cloud. With this lot of data files stored in the cloud server, it is important to provide keyword based search service to data user. Now in order to protect the data privacy, sensitive data is usually encrypted before sent to the cloud server, which makes the search technologies on plaintext unusable. The system preserves the high search efficiency inherited from the inverted index while lifting the one-time-only search .limitation of the previous solutions which simultaneously meets a set of strict privacy requirements. A major challenge exposed from the existing efforts is the difficulty to protect user's query privacy so this challenge is faced and tried to remove in this scheme.

Keywords: Keword,Encription.

INTRODUCTION

Privacy and security are the most important issues in cloud computing. To achieve high flexibility and to reduce cost, many data owners are outsourcing their data management system to public cloud. However, data utilization, e.g. keyword search, is a challenging problem due to the data encryption. Downloading the entire encrypted data set first then searching over the decrypted data is difficult task. Therefore, the search operation must be done at the cloud side and over the encrypted data. First of all, the keyword privacy is compromised once a keyword is searched. As a result, the index must be rebuilt for the keyword once it has been searched. Obviously, such a solution is counterproductive. Secondly, the existing inverted index based search-able schemes do not support conjunctive multi-keyword search, which is the most common form of queries nowadays. So this solution solves the problem of building a search-able encryption scheme based on the inverted index to over-come the above limitations. This scheme proposes a practical inverted index based public-key searchable encryption scheme. This overcomes the one-time-only search limitation in the existing schemes. This scheme supports conjunctive multi-keyword search using only one trapdoor while the existing invert index based searchable encryption schemes only support single keyword search.A probabilistic trapdoor generation algorithm is used to break the trapdoor link ability. So it preserves the index and trapdoor privacy. To provide stronger security guarantee, this scheme uses an efficient oblivious transfer protocol to hide the access pattern. Comparing with the existing public-key searchable encryption schemes which use expensive pairing operations, this scheme is more efficient because it only need multiplication and exponentiation.

LITERATURE SERVEY

Generalized INverted IndeX (Ginix)[1], presents index structure, which merges consecutive IDs in inverted lists into intervals to save storage space. With this index structure, more efficient algorithms can be devised to perform basic keyword search operations, i.e., the union and the intersection operations, by taking the advantage of intervals. Specifically, these algorithms do not require conversions from interval lists back to ID lists. As a result, keyword search using Ginix can be more efficient than those using traditional inverted indices. The performance of Ginix is also improved by reordering the documents in datasets using two scalable algorithms.

Table 1 sample dataset of 7 paper titles.
(a)Dataset content.

ID	Content
1	Keyword querying and ranking in databases
2	Keyword searching and browsing in databases
3	Keyword search in relational databases

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101270

4	Efficient fuzzy type-ahead search
5	Navigation system for product search
6	Keyword search on spatial databases
7	Searching for hidden-web databases

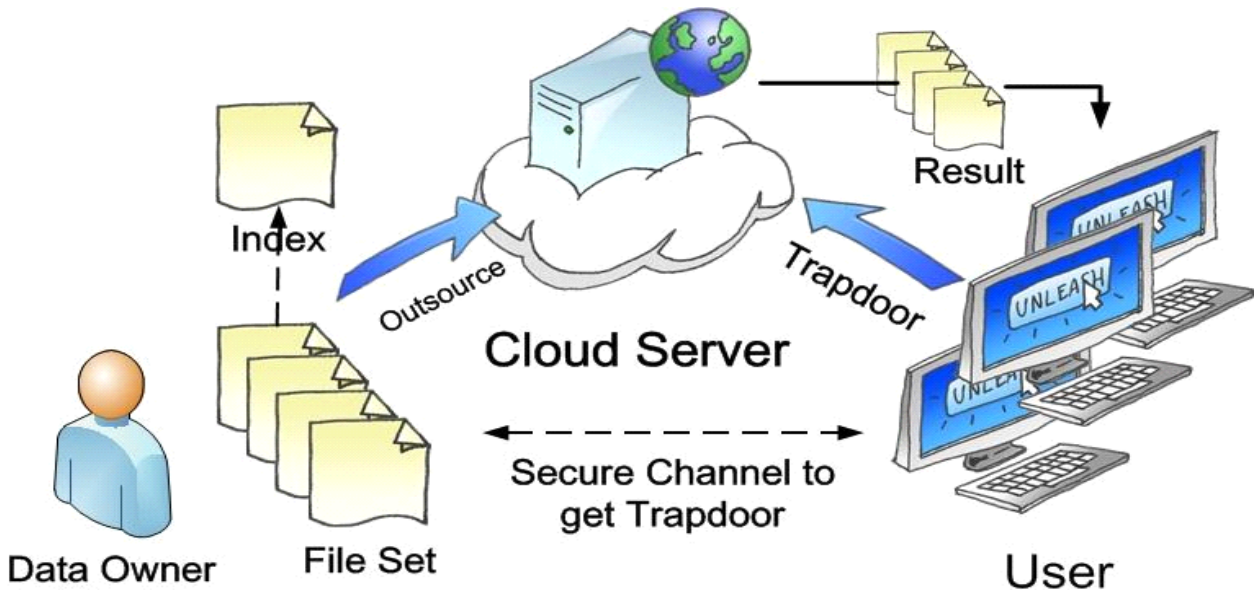
Table 2 (b) InvIndex

Words	ID
Keyword	1,2,3,6
1,2,3,6	1,2,3,6,7
Searching	2,7
Search	3,4,5,6

Table 3 (c) Ginix

Words	Intervals
Keyword	[1,3],[6,6]
Databases	[1,3],[6,7]
Searching	[2,2],[7,7]
Search	[3,6]

DESCRIPTION



System Model:

Fig 1 .System architecture of search over encrypted data in cloud computing

System Architecture:

The system model in this work is shown in Fig.1. There are three entities in the system, a cloud server, a data owner and multiple users. The data owner generates the encrypted index and outsources it along with the encrypted data into the cloud. An authorized user submits a query request to the server in the form of a trapdoor which he gets from the data owner through a secure channel. After receiving the trapdoor, the cloud server matches the encrypted index with the trapdoor. Finally, the cloud server returns the matching documents as the search result. The access control between data owner and the users can be achieved using existing protocols

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101270

CONCLUSION

This system proposed a multikeyword searching over encrypted data with Privacy Preserving on inverted index. This scheme overcomes the one-time-only search limitation in the previous schemes used in Ginix[1]. The probabilistic trapdoor generation algorithm prevents the cloud server from linking the trapdoors. This scheme also hides the number of keywords in the query. Additionally, this scheme supports multi-keywords conjunctive search. This scheme uses the blind storage technique to protect the access patterns.

REFERENCES

[1] Hao Wu_, Guoliang Li, and Lizhu Zhou "Ginix: Generalized Inverted Index for Keyword Search "knowledge and data mining vol no:8 Year 2013.

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

[3] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security, ser. Lecture Notes in Computer Science, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 442–455.

[4] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in Advances in Cryptology - CRYPTO 2007, ser. Lecture Notes in Computer Science, A. Menezes, Ed. Springer Berlin Heidelberg, 2007, vol. 4622, pp. 535–552.

[5] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE, March 2010, pp. 1–5.