

# A Survey on Phrase Search over Encrypted Cloud Storage with Multiple Data Owners

<sup>[1]</sup> Pavan Kumar Kandukuri, <sup>[2]</sup> G. Vishnu Murthy  
<sup>[2]</sup> Professor,

<sup>[1]</sup> Dept. of Computer Science & Engineering, Anurag Group of Institutions, Hyderabad.

**Abstract:** The basic advantage of cloud computing is giving of data benefit, by which the data proprietors stores their information in general data server farms by financially sparing their capital venture towards data management. Distributed cloud storage gives clients enormous storage room and makes it easy to use for prompt necessity of data, which is the establishment of a wide range of cloud based applications. Data giving in the business open cloud additionally raises the issue for unapproved data get to and the distributed cloud storage would not be commendable if the outsourced data isn't viably used. The challenge is on the most proficient method to influence successful data to access in the public cloud storage aiming at change of different searching procedures for expanding the data usage. In this paper, an endeavour is made to review different searching procedures for the powerful data use in cloud storage and is talked about in detail.

**Keywords:** Cloud computing, data usage, data management, distributed cloud storage.

## I. INTRODUCTION

Cloud computing is an expanding model of huge business framework that gives on request astounding applications and administrations from a common pool of design processing assets. The cloud clients, people or endeavours, can outsource their neighbourhood complex data framework into the cloud to keep away from the expenses of building and keeping up a private storage framework. The organization or association's private data like individual documents, organization records, messages, and so on which is to be shared among the chosen organization workers is put away and concentrated into cloud server however for the most part with an unreliable inclination that anybody may hack these data that might be exceptionally risky for that organization.

In the earlier works which support the single-proprietor model, in which a data proprietor needs to remain online to create indirect access to data client. Along these lines, this proposes a multi-proprietor model to beat the constraints of the prior techniques, where encrypted data is put away by different data proprietors and at the same time data proprietors remain online to produce in direct access. Various data proprietors share distinctive secret keys to encrypt their data with the various keys.

## 2. LITERATURE SURVEY

D. Boneh [1] has proposed one of the most punctual chips away at key phrase searching. Their plan utilizes open key encryption to enable key words to be accessible without

uncovering data content. Waters. [2] explored the issue for looking over encoded review logs. A large number of the early works concentrated on single key phrase findings. As of latest, scientists have proposed arrangements on conjunctive key phrase searches, which includes different keywords [3], [4]. Other fascinating issues, for example, the positioning of indexed lists [5], [6], [7] and looking with key phrases that may contain faults [8], [9] named fuzzy keyword search, have additionally been considered. The capacity to scan for phrases was likewise as of examined [10], [11], [12], [13]. Some [14] have inspected the security of the proposed arrangements and, where defects were discovered, solutions were proposed with the explanations [15].

Accessible encryption systems [16], [17] can somewhat satisfy the requirement for secure given file search. Secure search over the encoded cloud data which diminishes the calculation. The privacy preserving search of records strategies and client authorization system are utilized to take care of the issue of secure multi-level keyword scan for different data owners and multi level data clients in distributed cloud computing.

Depending on PEKS plot [18], a great deal of works have generally flow around the criteria of conjunctive keywords search. If at all that the client is keen on a few key phrases of report, the client may either depend on a convergence estimation to decide the right arrangement of archives or store extra data on the server to encourage

such pursuits. Thus, open key encryption with conjunctive keyword search (PECK) method is efficient to refer.

Normally, PEKS and PECK [18], give a sort of system that enables recipient to acquire messages that contain one or a few specific keywords by giving an indirect access comparing to the keywords from email server, while the email server and various other beneficiary can't pick up whatever else about the email.

A privacy-preserving query framework for encrypted cloud storage was proposed in Phrase Search for Encrypted Cloud Storage [22]. The framework adopts symmetric-key encryption and a tree-based search structure to maintain query performance and ensure query privacy. The secure searchable index (BFEST) in the framework is jointly operated by the EU and the CSS to reduce computation and network communication costs of the EU.

In terms of query format, queries in the form of phrases were supported. The framework is flexible enough to suit real-world applications, such as supporting searches in encrypted corporate event logs. The experimental results indicate that the framework can effectively protect the user data and the privacy of user queries. The computation overhead on the EU was negligible, and the communication overhead can be minimized by tuning BFEST parameters to limit the number of candidate data objects returned by the CSS.

**3. COMPARATIVE STUDY**

S.NO	Paper/ Publication	Author	Observations
1.	“Public Key Encryption with Keyword Search,” in proceedings of Eurocrypt, 2004, pp. 506–522. D. Boneh [1]	D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano.	Constructing a PEKS implies and is related to Identity Based Encryption (IBE). Here, constructions for PEKS are based on recent Identity

			Based Encryption (IBE). The security is proved by exploiting properties of IBE based PEKS.
2.	“Fast Phrase Search for Encrypted Cloud Storage”, 10.1109/TCC.2017. 2709316, IEEE Transactions on Cloud Computing. [19]	Hoi Ting Poon, Member, IEEE and Ali Miri, Member, IEEE.	Bloom filters are used to test if a keyword is associated with a document. Here, an approach is described using Bloom filters to support functionality with an emphasis on response time. Multiple n-gram Bloom filters are used to provide phrase search and conjunctive keyword search.

3.	<p>“An Effective Fuzzy Keyword Search Scheme in Cloud Computing,” in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786–789. [8]</p>	<p>He Tuo and Ma Wenping, Xidian University, Xi'an, China.</p>	<p>Fuzzy identity encryption scheme was extended to a fuzzy keyword search scheme that can efficiently fetch over encrypted data along with keyword. Dual encryption concept is also used in this scheme. The server provider is required in order to participate in partial decipherment before user's recovery of the plain-text.</p>	Conference on Cloud Computing, 2015. [12]	Canada.	capable of basic ranking and has the ability to search for non indexed keywords. Conjunctive search and phrase search algorithms were provided. The results of scheme were presented and were applied to a database of text documents.	
4.	<p>“An Efficient Conjunctive Keyword and Phrase Search Scheme for Encrypted Cloud Storage Systems,” in IEEE International</p>	<p>Hoi Ting Poon and Ali Miri, Department of Computer Science, Ryerson University, Toronto, Ontario,</p>	<p>Conjunctive keyword and phrase search scheme with low storage requirement were presented. This is</p>	5.	<p>“Secure Ranked Keyword Search over Encrypted Cloud Data”, in Proc. IEEE Distributed Computer System, Genoa, Italy, Jun. 2010, pp. 253262. [17]</p>	<p>Cong Wang, Ning Cao, Jin Li, Kui Ren and Wenjing Lou, Department of ECE, Illinois Institute of Technology, Chicago, IL</p>	<p>Problem of secure ranked keyword search over encrypted cloud data is solved. Definition for ranked searchable symmetric encryption was proposed, and gave an efficient design by properly</p>

			utilizing the Order Preserving Symmetric Encryption (OPSE). Proposed solution enjoys security guarantee compared to previous schemes.
--	--	--	---

**4. CONCLUSION**

Here, this paper outlines different types of search procedures in the encrypted form of cloud storage data. The overview on various procedures to look over the encoded information takes care of the issue of positioned search over encrypted cloud data. Performing such sort of search causes an expansion in the computational cost and the cost related with correspondence. Every one of these search techniques enables clients to perform key phrase searching while at the same time enhancing the security of the client query. The cloud server performs search over the encrypted information yet server does not know the private data behind the data accumulation. The fundamental objective of every one of these techniques is to keep the cloud server from taking in the private data from the record set, the file document, and the client queries in this way securing the privacy of the client.

**5. REFERENCES**

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in In proceedings of Eurocrypt, 2004, pp. 506–522.

[2] B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Network and Distributed System Security Symposium, 2004.

[3] M. Ding, F. Gao, Z. Jin, and H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in IEEE International Conference on Network Infrastructure and Digital Content, 2012, pp. 526–530.

[4] F. Kerschbaum, "Secure conjunctive keyword searches for unstructured text," in International Conference on Network and System Security, 2011, pp. 285–289.

[5] C. Hu and P. Liu, "Public key encryption with ranked multi keyword search," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109–113.

[6] 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, pp. 164–172, 2014.

[7] C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, "Relevance ranking for one to three term queries," Information Processing and Management: an International Journal, vol. 36, no. 2, pp. 291–311, Jan. 2000.

[8] H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786–789.

[9] M. Zheng and H. Zhou, "An efficient attack on a fuzzy keyword search scheme over encrypted data," in International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing, 2013, pp. 1647–1651.

[10] S. Zittrower and C. C. Zou, "Encrypted phrase searching in the cloud," in IEEE Global Communications Conference, 2012, pp. 764–770.

[11] Y. Tang, D. Gu, N. Ding, and H. Lu, "Phrase search over encrypted data with symmetric encryption scheme," in International Conference on Distributed Computing Systems Workshops, 2012, pp. 471–480.

[12] H. Poon and A. Miri, "An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems," in IEEE International Conference on Cloud Computing, 2015.

[13] "A low storage phrase search scheme based on bloom filters for encrypted cloud services," to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.

[14] H. S. Rhee, I. R. Jeong, J. W. Byun, and D. H. Lee, "Difference set attacks on conjunctive keyword search schemes," in Proceedings of the Third VLDB International Conference on Secure Data Management, 2006, pp. 64–74.

[15] K. Cai, C. Hong, M. Zhang, D. Feng, and Z. Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.

[16] R. Curtmola, J. A. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions", In Proc. of ACM CCS 06, 2006.

[17] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, "Secure ranked keyword search over encrypted cloud data", in Proc. IEEE Distributed Computer System, Genoa, Italy, Jun. 2010, pp. 253262.

[18] Maozhen Ding, Fei Gao, Zhengping Jin, Hua Zhang, "Efficient Public Key Encryption with Conjunctive Keyword Search Scheme Based on Pairings" 978-1-4673-2204-1/12, 2012 IEEE, Proceedings of IC-NIDC2012

[19] Hoi Ting Poon, Member, IEEE, and Ali Miri, Member, IEEE, "Fast Phrase Search for Encrypted Cloud Storage", DOI 10.1109/TCC.2017.2709316, IEEE Transactions on Cloud Computing.

[20] Kalyani Sonawane, Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, "Survey on Multi-Keyword Ranked Search over Encrypted Cloud Data with Multiple Data Owners", International Journal of Computer Applications (0975 – 8887) Volume 162 – No 11, March 2017.

[21] Ms. Jabeen Akkalkot, Ms. S. Shanmug Priya PG Student, Department of Computer Science and Engineering New Horizon College of Engineering, Bangalore, Karnataka, India, "Survey On Keyword-Based Search Mechanism For Data Stored In Cloud", IJCSMC, Vol. 5, Issue. 5, May 2016.

[22] Yen Chung Chen, Yu-Sung Wu and Wen- Guey Tzeng, Department of Computer Science National Chiao Tung University Hsinchu, 300 Taiwan, "Phrase Search for Encrypted Cloud Storage" Journal of Information Science and Engineering 32, 2016.