International Journal of Research in Engineering, Science and Management
Volume 4, Issue 11, November 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

A Novel Feature Matching Ranked Search Mechanism Above Encrypted Cloud Data

M. Parkavi[1*], Sumalatha[2]
[1]*Research Scholar, Department of Computer Science, Swami Vivekananda College Arts & Science, Villupuram, India*
[2]*Assistant Professor, Department of Computer Science, Swami Vivekananda College Arts & Science, Villupuram, India*

***Abstract*: Encrypted seek generation has been studied notably in current years. With an increasing number of facts being saved in cloud, developing indexes with impartial key phrases has ended in extensive garage value and coffee seek accuracy, which has end up a pressing trouble to be solved. Thus, on this paper, we endorse a brand new characteristic matching ranked seek mechanism (FMRSM) for encrypted cloud data. This mechanism makes use of characteristic rating set of rules (FSA) to create indexes, which permits multi-key phrases which can be extracted from a file as a characteristic to be mapped to 1 size of the index. Thus, the garage value of indexes may be decreased and the performance of encryption may be improved. Moreover, FMRSM makes use of an identical rating set of rules (MSA) in producing trapdoor process. With the assist of FSA, the matching rating set of rules can rank the hunt effects in step with the sort of healthy and the wide variety of matching key phrases, and consequently it could go back effects with better rating accuracy. Comprehensive evaluation show that our mechanism is greater viable and effective.**

***Keywords*: Encrypted search, Matching score, Storage cost.**

1. Introduction

Cloud computing is that the usage of computing assets (hardware and software) that rectangular degree brought as a provider over a community (usually the Internet). The call comes from the not unusual place use of a cloud-formed photo as Associate in Nursing abstraction for the complex infrastructure it incorporates in machine diagrams. Cloud computing entrusts far flung offerings with a user's facts, code and computation. Cloud computing includes hardware and code assets created available in the marketplace at the internet as controlled third-celebration offerings. These offerings typically provide get right of entry to superior code programs and high-give up networks of server computers.

A. Purpose

The aim of cloud computing is to apply historic supercomputing, or advanced computing energy, commonly hired through navy and evaluation facilities, to carry out tens of trillions of computations according to second, in purchaser-orientated programs like financial portfolios, to supply personalized info, to supply facts garage or to energy big, immersive computer games. The cloud computing makes use of networks of great groups of servers typically walking less expensive consumer pc era with specialized connections to spread records-processing chores throughout them. This shared IT infrastructure incorporates big swimming pools of structures that rectangular degree joined along. Often, virtualization strategies rectangular degree accustomed maximize the ability of cloud computing.

2. Literature Survey

A. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers

Q. Chai and G. Gong Outsourcing records to cloud servers, even as growing provider availability and decreasing users' burden of handling records, necessarily brings in new worries along with records privateness, for the reason that server can be honest-but-curious.

To mediate the conflicts among records usability and records privateness in this sort of scenario, studies of searchable encryption is of growing interest. Motivated through the truth that a cloud server, except its curiosity, can be egocentric on the way to shop its computation and/or down load bandwidth, on this paper, we look at the searchable encryption hassle with inside the presence of a semi-honest-but-curious server, which may also execute best a fragment of seek operations absolutely and go back a fragment of seek final results absolutely.

B. Designated cloud server public key encryption with keyword search from lattice in the standard model

X. Zhang, C. Xu, R. Xie, and C. Jin, Recently, a way to retrieve the encrypted facts correctly from a cloud garage machine will become a warm topic. Public key encryption with key-word seek (PEKS) can permit one to go looking the encrypted facts with a key-word correctly. Due to the booming of post-quantum cryptography, we suggest public key encryption with key-word seek from lattice assumption, that may withstand quantum laptop attacks.

C. Privacy preserving keyword searches on remote encrypted data

Y. Chang and M. Mitzenmacher We take into account the subsequent trouble: a person U desires to save his documents in an encrypted shape on a far-flung document server S. Later the

*Corresponding author: parkavikala199@gmail.com

person U desires to successfully retrieve a number of the encrypted documents containing (or listed through) precise key phrases, retaining the key phrases themselves mystery and now no longer jeopardizing the safety of the remotely saved documents.

D. Practical techniques for searches on encrypted data

D. X. Song, D. Wagner, and A. Perrig It is ideal to keep statistics on statistics garage servers inclusive of mail servers and document servers in encrypted shape to lessen protection and privateness risks.

E. SSARES: Secure Searchable Automated Remote Email Storage

A. J. Aviv, M. E. Locasto, S. Potter, and A. D. Keromytis The growing centralization of networked offerings locations person statistics at enormous risk. For example, many customers save electronic mail on far off servers in preference to on their nearby disk.

F. Problem Formulation

The encrypted seek device is proven the statistics proprietor first regards all types of statistics as files, then extracts key phrases from every file to shape an encrypted index, and finally uploads the encrypted files and indexes to the cloud server. While querying, the statistics person first generates a trapdoor thru seek manage operation, then submits it to the cloud server for retrieval. After receiving the trapdoor, the cloud server calculates the similarity rating of the trapdoor and every file index, then returns copies of encrypted files to the statistics person in accordance the rating.

3. Modules

- Data owner
- Data user
- Cloud server

A. Data Owner

In the first module, we develop data owner module, where the data owner uploads his/her file to the cloud. The data owner first regards all kinds of data as documents (only .txt).

B. Data User

In the next module we develop Data user part. While querying, the data user first generates a trapdoor through search control operation, and then submits it to the cloud server for retrieval.

C. Cloud Server

After receiving the trapdoor, the cloud server calculates the similarity score of the trapdoor and each document index, and then returns copies of encrypted documents to the data user according the score.

4. Experiment and Result

A. Multi – key - word Ranked Search

To fashion seek schemes which allow multi-key-word question and deliver end result similarity rating for powerful statistics retrieval, in place of returning undifferentiated effects.

B. Privacy – Preserving

To prevent the cloud server from mastering extra facts from the dataset and consequently the index, and to fulfill privateness necessities specified.

5. Conclusion

In this paper, we advise a novel function matching ranked search mechanism for encrypted cloud data. In this mechanism, a characteristic rating algorithm is used to create indexes so that a plurality of key phrases extracted from a file are solely mapped to one dimension of the index. Comparing with developing indexes with impartial keywords, this mechanism can decrease the index dimension. In addition, a matching rating algorithm is designed in the producing trapdoor technique of FMRSM. This algorithm can provide the question request a correct rating based totally on the kind of fit and the variety of matching keywords, so that the question consequences are greater in line with user's proper search requests. It can be viewed from the scan effects that our mechanism can velocity up the advent of index, the technology of trapdoor, and the search process. Moreover, our mechanism reduces storage price and enhance the rating accuracy.

This set of rules can deliver the question request and correct rating primarily based totally on the form of healthy and the quantity of matching keywords, in order that the question effects are extra in keeping with users real seek requests. It may be visible from the test effects that our mechanism can accelerate the introduction of index, the era of trapdoor, and the quest process. Moreover, our mechanism can keep garage fee and enhance the rating accuracy.

References

[1] Q. Chai and G. Gong, "Variable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Proc. IEEE Int. Conf. Commun. (ICC), Ottawa, ON, Canada, Jun. 2012, pp. 917-922.

[2] X. Zhang, C. Xu, R. Xie, and C. Jin, "Designated cloud server public key encryption with keyword search from lattice in the standard model,'" Chin. J. Electron., vol. 27, no. 2, pp. 304-309, Mar. 2018.

[3] Y. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., vol. 5. Berlin, Germany: Springer, 2005, pp. 442-455.

[4] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy (S&P), Berkeley, CA, USA, May 2000, pp. 44-55.

[5] A. J. Aviv, M. E. Locasto, S. Potter, and A. D. Keromytis, "SSARES: Secure searchable automated remote email storage," in Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Miami Beach, FL, USA, Dec. 2007, pp. 129-139.

[6] M. Raykova, B. Vo, S. M. Bellovin, and T. Malkin, "Secure anonymous database search," in Proc. ACM Workshop Cloud Comput. Secur. (CCSW), New York, NY, USA, 2009, pp. 115-126.

[7] S. M. Bellovin and W. R. Cheswick, "Privacy-enhanced searches using encrypted Bloom lters," IACR Cryptol. ePrint Arch., Tech. Rep., 2004, vol. 22.

[8] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546-2559, Sep. 2016.

[9] Z. Fu, X. Sun, Z. Xia, L. Zhou, and J. Shu, "Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing," in Proc. IEEE 32nd Int. Perform. Comput. Commun. Conf. (IPCCC), San Diego, CA, USA, Dec. 2013, pp. 18.

[10] H. Yin, Z. Qin, J. Zhang, W. Li, L. Ou, Y. Hu, and K. Li, "Secure conjunctive multi-keyword search for multiple data owners in cloud computing," in Proc. IEEE 22nd Int. Conf. Parallel Distrib. Syst. (ICPADS), Wuhan, China, Dec. 2016, pp. 276-286.

[11] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp. 2706-2716, Dec. 2016.

[12] Z. Guo, H. Zhang, C. Sun, Q. Wen, and W. Li, "Secure multi-keyword ranked search over encrypted cloud data for multiple data owners," J. Syst. Softw., vol. 137, pp. 380-395, Mar. 2018.

[13] X. Jiang, J. Yu, J. Yan, and R. Hao, "Enabling efficient and variable multi-keyword ranked search over encrypted cloud data," Inf. Sci., vols. 403-404, pp. 2241, Sep. 2017.

[14] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFO-COM, San Diego, CA, USA, Mar. 2010, pp. 15.

[15] M. A. M. Ahsan, F. Z. Chowdhury, M. Sabilah, A. W. B. A. Wahab, and M. Y. I. B. Idris, "An efficient fuzzy keyword matching technique for searching through encrypted cloud data," in Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS), Langkawi, Malaysia, Jul. 2017, pp. 15.

[16] X. Zhu, Q. Liu, and G. Wang, "A novel variable and dynamic fuzzy keyword search scheme over encrypted data in cloud computing," in Proc. IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, Aug. 2016, pp. 845-851.

[17] H. Zhu, Z. Mei, B. Wu, H. Li, and Z. Cui, "Fuzzy keyword search and access control over cipher texts in cloud computing," in Proc. Australia's. Conf. Inf. Secur. Privacy. Cham, Switzerland: Springer, 2017, pp. 248-265.

[18] Y. Tang, D. Gu, N. Ding, and H. Lu, "Phrase search over encrypted data with symmetric encryption scheme," in Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops, Macau, China, 2012, pp. 471-480.

[19] E. J. Goh, "es," IACR Cryptol. ePrint Arch., Tech. Rep., 2003, p. 216.

[20] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. Skeith, III, "Public key encryption that allows PIR queries," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2007, pp. 50-67.