ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Secure Plan: Encryption with the Rank of a Dynamic Multi-Keyword

I Surya Prabha
Associate Professor
Department of IT,
Institute of Aeronautical Engineering,
Hyderabad, India.

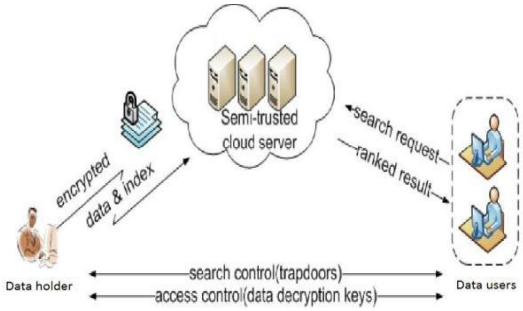
Dr Mohammed Ali Hussain
Professor,
Department of ECM,
K L University,
Vijayawada, India.

ABSTRACT

The main purpose of this article is, encrypted cloud data (mrse), where the exact method of privacy protection as the concept of cloud computing to solve the multi-keyword search problems classified. Holders of data to the public cloud for business flexibility and financial savings to their management systems to link data from local sites are encouraged to outsource. However, to protect the confidentiality of data, sensitive data should be encrypted before delivery, clearly based on keyword research uses traditional data. Accordingly, a search service to allow encrypted data to the cloud is extremely important. The larger number of users and documents in the cloud, it is important to allow some of the keywords in the query and location of these keywords in order to provide documentation. Encryption similar mechanisms for individual keywords or Boolean keyword research after, and as a result rarely out. Among several significant multi-word terms, choose well-organized similarity measure "in the coordination", is that many games as possible in the search bar to capture the record means. In particular, we have "similar domestic product", considering that a document showing the amount of keywords in the query quantitative degree of compatibility, the document estimates the search query. Construction index each document for each bit to mark whether a keyword is included in the document as well, as part of the index is coupled into a binary vector. For each bit is shown that these requirements appears in the appropriate keyword means available as a binary vector, so that the right domestic product by the query vector with vector data. On the other hand, outsourcing or vector data can be customized directly measured motion vector index is breaking research intimacy or private life. For the convenience of the vector space model for sufficient accuracy and DES encryption ranking allows them to take, while the popularity of the cipher process of computing work is done on the server side through the offer. As a result, the data can leak protection is suppressed, and data.

INTRODUCTION

Cloud computing is a conversational rake ideas to express a variety of different types of real-time means that a large number of computers are connected to the Internet communication network used phrase to fill. In science, cloud computing multiple computers connected to each other are more likely to run a program. The fame of the period of service provisioning application hosting services to sell advertising that can be recognized for its use in a remote location, client-server software is running on. Cloud computing resources on a network to achieve stability and financial system and a utility (like the electricity grid) depends on sharing. Cloud centers maximize the effectiveness of shared resources. Cloud resources only used as a rule, are not shared by many users, but as needed as a dynamically allocated. The different time zones can allocate resources to users. of service (such as web servers).



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This mechanism, in order to reduce energy, air-conditioning, as the power of the computer and all the benefits of reducing environmental damage and so on, as well as, the need to act. The word "move to the cloud," This is a traditional model of an organization's capital expenditure from the purchase price of materials and describe OPEX ie, a model had been used and as a cloud infrastructure using less pay Use it in the period. Supporters argue that cloud computing infrastructure costs and direct social projects as an alternative infrastructure to enable their companies to avoid differences in concentrateisSearch by keyword for information on existing techniques which are used widely in the clear data, the encrypted data can not be applied directly. Download all data from the cloud and locally decrypt obviously impractical. The existence of keywords in all major research programs, which can not provide acceptable results ranking based on the multi functionality to retrieve search results. However, sensitive data should be encrypted before outsourcing confidentiality requirements, the old document by keyword, dynamic multi-key scheme using the data as encrypted data on research safe retrieval.A cloud we build a special tree index structure and a " Deep search greedy "algorithm proposes efficient multi-keyword searches are classified. The proposed scheme to achieve sublinear search time and flexibility with the removal and insertion of documents can deal with. Many experiments to demonstrate the effectiveness of the proposed system are held. I do a lot of different functions for different models was in danger. Recently, some dynamic systems have been proposed, and support the introduction of a collection of documents on the actions proposed to delete this article for multiple keywords search system tree a secure encrypted data to the cloud, provides classified research and documentation supports dynamic operation of the collection. Key word search algorithm to provide efficient multi-classed. KNN index and query vectors to encrypt secure algorithm is used. A "depth first search Greedy" proposed algorithm based on the index tree. The algorithm performs better than linear search effectiveness, however, is a loss of accuracy. LSH similar research but not available to the classification algorithm is suitable. {East; CI} ← GenUpdateInfo (S t, i, the type)) {I created this algorithm update information; } Will be sent to the cloud server. Cloud services, such as email, personal health records, financial company data, government documents, etc. Despite the various benefits of outsourcing of sensitive information. KNN algorithm to encrypt and securely index and query vectors simultaneously encrypted and index vectors between the questions to ensure accurate calculation of the relevance score is used. Many words for dynamic discovery classified (BDMRS) model cryptogram is known and known background correction model more dynamic keyword ads Research (EDMRS) Basic rule: to attack various different risk model, we build two secure web systems. Our contributions are as follows: we find one encryption system design, particularly for multi-keyword search, classify and supports dynamic action, flexible to collect documents. Our tree index, search complexity of the proposed scheme in principle, because of the special structure of the logarithm. And in practice, the proposed rule our "depth first search greedy" algorithm by applying research to achieve high efficiency. In addition, the parallel flexible search time to reduce the cost of the research process will be carried out. This paper is organized as a memory. Similar works are in of this section, a brief introduction to the model of the system, the risk, the model provides the initial design goals. describes in detail the plans. presents the experience and performance analysis.

SYSTEM PRELIMINARIES

1. Server:

The following process shows server maintainace

Network checking: Server initialization, cloud server and the user to check the network connection. Connections are correct and processes are running.

Data encrypt: Saved data from the primary server first and then the cloud server encrypts. Cloud servers as "honest but curious" Our model, which is consistent with the work related to the searched encryption is on. In particular, the cloud server correctly an "honest" and is identified in the protocol specification.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Store to cloud server: Some encrypted cloud server collects various documents. In this method, the encrypted data will be stored with the cloud server. Search results should be chosen from the clouds. Cloud servers after some ranking criteria.

Send decrypted key to user: The main server is encrypted documents. It is used by the encryption key. Finally, users of cloud server for documents.

II. Cloud server:

The cloud server maintain the process

Retrieve request from user: User to the server sending the file to someone then wants to be able to request the user's request. Recovery of data from the server to the user.

Searching index/rank calculation: On the one hand, effective data recovery requirements, a large number of documents in the cloud application server to perform relevance ranking to lead earnings, rather than undivided result. Research also ranked as the most important data back elegant unnecessary network traffic can end.

Response to user: Post assessment of the index servers in the clouds with a document seeking feedback from early users.

III. User

The user maintain the following process

Requesting File to cloud server using multi keyword: By mentioning several keywords in the cloud server for the needs of users to send to customer demand. In particular, the cloud server correctly an "honest" and is identified in the protocol specification.

Retrieve decrypted key from admin & document from cloud server: All the major figures in the cloud server administrator to send encrypted data to the administrator. All data are stored in the cloud server.

Decrypt file

Trivial solution to download all data and decryption systems at the local level clearly above the clouds due to a large amount of bandwidth costs is impossible. Decryption capabilities for users to manage access control system is used for.

CONCLUSION AND FUTURE WORK

In this article we describe, and classify the cloud encrypted data on research to solve the problem of multi-touch is the word, and established a number of confidentiality requirements. Among several significant multi-word terms, we effective equality "coordinate matching" to choose to measure, so as efficiently as possible for the query keywords to outsource the relevance of the documents recognized as equivalent is obtained, and quantitative benchmark "equality of GDP" calculation using. Without violating privacy means more keywords acquisition support testing, we mrse secure domestic product is calculated with a basic idea. Then we have two systems in two models of different hazards mrse various improvements give strict confidentiality. _ TF IDF and dynamic process data words, including support for more research of other enhancements to our search methods listed.

REFERENCES

[1] K. Ren, C.Wang, Q.Wang et al., "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security. Springer, 2010, pp. 136– 149.

[3] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," ournal of the ACM (JACM), vol. 43, no. 3, pp. 431–473, 1996.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in Advances in Cryptology-CRYPTO 2007. Springer, 2007, pp. 50–67.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44– 55.

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

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proceedings of the Third international conference on Applied Cryptography and Network Security. Springer-Verlag, 2005, pp. 442–455.

[10] 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.

[11] 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. IEEE, 2010, pp. 1–5.

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

[13] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451–459. 1045-9219 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See

[14] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, 2014.

[15] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.

[16] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proceedings of the First international conference on Pairing-Based Cryptography. Springer-Verlag, 2007, pp. 2–22.

[17] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches ver encrypted data," in Proceedings of the 7th international conference on Information and Communications Security. Springer-Verlag, 2005, pp. 414–426.

[18] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proceedings of the 4th conference on Theory of cryptography. Springer-Verlag, 2007, pp. 535–554.

[19] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 262–267, 2011.

[20] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Advances in Cryptology–EUROCRYPT 2008. Springer, 2008, pp. 146–162.