International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

Data Search In Cloud Using The Encrypted Keywords

Pranit R.Thite[1], Ganesh M.Suryawanshi[2], Rajesh Mengale[3],Prof. A.M.Ingole[4]

[1,2,3] Student, Dept. Of Computer Engineering, BVCOEL Pune, Maharashtra, India
[4]Professor, Dept. Of Computer Engineering, BVCOEL Pune, Maharashtra, India

---

Abstract – *Information recovery on encrypted Data in cloud Facilitates data privacy with sensing concept of data stored in cloud. Existing encrypted search method support only monogram or bigram keyword search . Expressive keyword search process is computationally ineffective due to bilinear pairing process. Projected research execute skilled search over encrypted data with Boolean expression support . Algorithmic process implements pattern matching. Information retrieval from this process help the user to search in cloud without decrypting data.*

***Key Words*: Searchable Encryption, Cloud Computing, Expressiveness, Attribute-based Encryption**

1. INTRODUCTION

Firstly cloud is defined as the combination of grid computing and cluster computing. And it is a important aspect today as more data is stored on cloud which also is needed to be secured.

And so by using different Encryption Algorithms data is secured and so there are many problems in cloud computing regarding security issues and many more which should be solved accordingly.

Searching any data in the cloud and providing security to the cloud is difficult as the data in cloud is in encrypted form and there is a huge data in cloud which is needed to be decrypted to get it in the readable pattern. But this problem can be solved if there is such an algorithm by which the keyword that will be entered for searching any data will be in the encrypted form and we get the results for entered keywords, which will be the actual documents that are needed.

So such a system can be implemented which takes less time to search any keyword related to the data that is needed which is in the encrypted form stored on cloud.

2.SYSTEMATIC LITERATURE SURVEY

2.1 "Efficient Similarity Search over Encrypted Data" , Mehmet Kuzu, Mohammad Saiful Islam, Murat Kantarcioglu ,ACM publications, 2012

" Ginix: Generalized Inverted Index for Keyword Search ",Hao Wu , Guoliang Li, and Lizhu Zhou, IEEE Transcation, Volume 18, Number 1, February 2013

Cloud computing, a new terminology used to access data remotely from the centralized pool that can be rapidly deployed with great scalability and less computation overhead. Cloud computing comes with lots of advantages such as self-service on need, easy network access, accessing data independent of location, , rapid resource elasticity, low pricing, transference of risk, etc. . Thus we can say that cloud computing is advantageous to its user for avoiding large capital outlays required for deployment and management of software as well as hardware. Thus undoubtly cloud computing comes like a revolution in the field of information technology.

In this era of cloud computing, data owners get attracted to the cloud as it saves there lot of time, space and money. As the cloud computing starts gaining edge over another techniques of storing data, user starts storing large amount of information on cloud such as email ids, passwords, multimedia documents, companies secret data etc. by storing such information on cloud data owners get relief from the storing of their confidential data as cloud gives on demand access to the required things.

But the fact is that the data owners and cloud providers are may not aware of each other regarding trust. SO possibility of hacking or leaking this confidential information is raises. This problem can be easily overcome by the data cloud providers, they allow the users to keep their information in encrypted format so that it is highly secure and chances of getting leaked is get minimized.

Cloud computing offers great data utilization of encrypted data but searching over encrypted data is very challenging task as there are huge numbers of outsource files are presents. However data owners might want selected files related with entered query. So keyword searching over encrypted data emerged as good technique to find the required data from the cloud.

2.2 "K-Gram Based Fuzzy Keyword Search over Encrypted Cloud Computing " Cong Wang1, Qian Wang1, Kui Ren1, and Wenjing Lou2

Presents a real approach having fuzzy logic as base to search data over ciphered cloud data. Here author said that it is the very first approach for the same. Here system returns the file in which exact match of predefined word is get found. System also returns the file if it have close words from the entered query. To accomplish the task author edit distance is used, it helps in finding the similar words based on their semantics. At last authors comes on conclusion that it is the best system which uses fuzzy logic , edit distance to solve the given problem. wildcard-based technique which is a advanced methods is used by the authors to use fuzzy logic more efficiently.

2.3 " Above the clouds : A Berkley view of cloud computing"

Proposed a new technique known as Secured Multikeyword search (SMS) for searching the input query over ciphered data in cloud. To search files containing documents qn efficient rule of coordinate matching is used. Coordinate matching refers to a technique of finding the hugh number of matches as many as possible so that it will become easy to find similarity between the input query and the list of records. To improve further accuracy they developed an alert system, this system will gives an alert whenever an unauthorized users are trying to access the system. This alert isgiven by the emails and messages to the related users.

2.4 "Fuzzy Keyword Search over Encrypted Data in Cloud Computing" Jin Li , Qian Wang , Cong Wang† , Ning Cao, Kui Ren , and Wenjing Lou

Elaborates the concept of semantic relationship (SRL) library to find the search the files. Publishers state that they tested the project with both public and private cloud. To getting things done a two setp process is used. In the first lap, SRL is developed using the entered data in private cloud. The output of first step is given as input to the second step. SRL is used to retrieve the index on public cloud. In final step all the records containing matching words are raised.

2.5 "Secured Multiple-keyword Search over Encrypted Cloud Data." Prof. C. R. Barde1 , Pooja Katkade2 , Deepali Shewale3 , Rohit Khatale4 . www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014

Takes personal health records system (PHR) as a base for the case studies as it is the area which affected greatly due to the less security in cloud system. Here authors develop a framework known as Authorized Private Keyword Search (APKS) which is highly scalable for searching over cloud data. Further they make use of Hierarchical Predicate Encryption (HPE) to solve the problem of searching. Author declares that it is privacy search because it hides the keywords from the server which results in more and more security.

2.6 "Privacy- Preserving Keyword-based Semantic Search over Encrypted Cloud Data" Xingming Sun, Yanling Zhu, Zhihua Xia and Lihong Chen International Journal of Security and Its Applications Vol.8, No.3 (2014),

Makes use of vector space model to retrieve the documents from the cloud. An author states that it is one of the best models for accomplishing the problem definition. For the given keyword a relevant score is find out by the system for each document and from that relevance score files are tanked. And at last those files are raised that have higher rank over another files.

2.7 "Authorized Private Keyword Search over Encrypted Data in Cloud Computing" Ming Li∗, Shucheng Yu†, Ning Cao∗ and Wenjing Lou*

Proposed a new technique of searching which makes use of K gram technique for producing fuzzy logic results. Authors said that previous technique is good for searching when exact match of keyword is found. But if there are some spelling errors or some nearby words are entered then system will fails to give answers. Proposed system developed to overcome the said problem. It makes use of K gram based fuzzy logic to accomplish the task. For more security developers makes use of separate servers which are not related with each other's at all.

3. SYSTEM OVERVIEW

The System Overview is shown in Fig -1, which is composed of four entities: a trusted trapdoor generation centre who publishes the system parameter and holds a master private key and is responsible for trapdoor generation for the system, data owners who outsource encrypted data to a public cloud, data users who are privileged to search and access encrypted data, and a designated cloud server who executes the keyword search operations for data users. To enable the cloud server to search over ciphertexts, the data owners append every encrypted document with encrypted keywords.

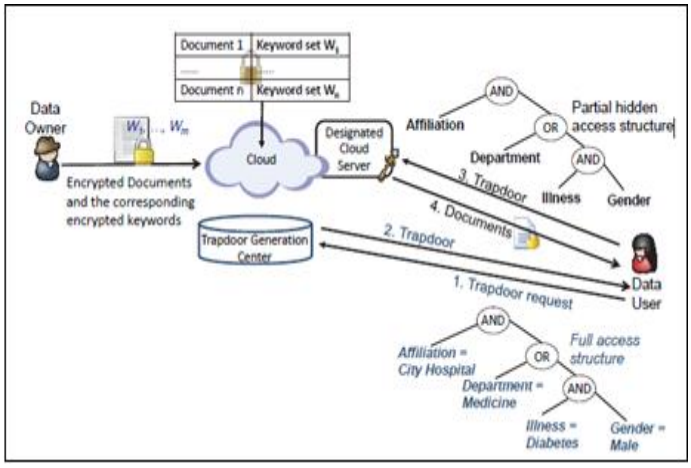

Fig -1: System Overview

A data user issues a trapdoor request by sending a keyword access structure to the trapdoor generation centre which generates and returns a trapdoor corresponding to the access structure. We assume that the trapdoor generation centre has a separate authentication mechanism to verify each data user and then issue them the corresponding trapdoors. After obtaining a trapdoor, the data user sends the trapdoor and the corresponding partial hidden access structure (i.e., the access structure without keyword values) to the designated cloud server. The latter performs the testing operations between each ciphertext and the trapdoor using its private key, and forwards the matching ciphertexts to the data user. As mentioned earlier, a ciphertext created by a data owner consists of two parts: the encrypted document generated using an encryption scheme and the encrypted keywords generated using our SE scheme. From now on, we only consider the latter part of the encrypted document, and ignore the first part since it is out of the scope of this paper. In summary, the design goals of our expressive SE scheme are fourfold.

3.1 Expressiveness

The proposed scheme should support keyword access structures expressed in any Boolean formula with AND and OR gates.

3.2 Efficiency

The proposed scheme should be adequately efficient in terms of computation, communication and storage for practical applications.

3.3 Keyword privacy

First, a ciphertext without its corresponding trapdoors should not disclose any information about the keyword values it contains to the cloud server and outsiders. Second, a trapdoor should not leak information on keyword values to any outside attackers without the private key of the designated cloud server. We capture this notion of security for the SE scheme in terms of semantic security to ensure that encrypted data does not reveal any information about the keyword values, which we call "selective indistinguishability against chosen keyword-set attack (selective IND-CKA security)"

3.4 Provable security

The security of the proposed scheme should be formally proved under the standard model rather than the informal analysis.

4. ADVANTAGES

4.1 Use of Trapdoor
4.2 No Redundant Decryption
4.3 Secured
4.4 Time Saving
4.5 Expressive Boolean predicate support for search.
4.6 Hidden Data Identification with pattern matching

5. CONCLUSIONS

Proposed system should be implemented to overcome the drawbacks which were introduced in the previous system while searching data in cloud .The system can assist user to perform expressive Boolean search finding hidden underived search pattern from cloud Algorithmic approach is scalable pattern using the encrypted pattern search.

ACKNOWLEDGEMENT

This paper is been completed under the guidance of Mrs.Aniket Kadam Sir who have explained us the need for implementation of this system, like how it will be processed and what mechanism should be actually used. We have also referred many papers and Wikipedia for the completion of this paper.

The work wouldn't get completed if we would not get precious help of Prof. A.M.Ingole sir BVCOE Lavale, Pune who supported us at every stage during the completion.

REFERENCES

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in 2000 IEEE Symposium on Security and Privacy, Berkeley,

California, USA, May 14-17, 2000. IEEE Computer Society, 2000, pp. 44–55.

[3] E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003. [4] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication," in Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes in Computer Science, vol. 1592. Springer, 1999, pp. 402–414.

[4] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single database private information retrieval implies oblivious transfer," in Advances in Cryptology - EUROCRYPT 2000, International Conference on the= Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, ser. Lecture Notes in Computer Science, vol. 1807. Springer, 2000, pp. 122–138.

[5] W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity, vol. 20, no. 2-3, pp. 356–371, 2004.

[6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3027. Springer, 2004, pp. 506–522.

[7] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE Y.. Springer-Verlag, 2007, pp. 2–2

[8] 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.

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

[10] 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