ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fine-grained Multi-keyword search for Encrypted cloud data

M.Kanmani[#1],M.Mohanapriya[#1],K.Ramya[#1],Ms.T.G.Ramyapriyatharsini[#2]
#1Bachelor of Computer Science and Engineering.
#2 Assistant professor Department of Computer Science and Engineering
Bharathiyar Institute of Engineering for Women

ABSTRACT

In cloud computing,private data can store in the server and allow to access the public users in the cloud server . outsourced data contain secure message data must be encrypted before uploaded in the internet.When the encrypted data must be search very difficult manner .We are used to develop the fine grained multi keyword search schemes using encrypted cloud data .In this concept include in three fold .First,we introduced in related to one word of one meaning and get the important factors on keywords and enable to search keywords and personalized user experience.Second,It very efficient to search the multi keyword in this scheme .Third, we are classified sub dictionaries to achieve more efficiency on content table,data can send do not block the other data .We analyze the secure the proposed schemes in this document to reliability privacy protection of content table and unlinkability of trapdoor .In this scheme to analysis and practical result to demonstrate the scheme can achieve security level to compare the existing one then the better performance in functionality and query complexity.

INTRODUCTION

THE cloud computing ,individual data can store remotely on the internet.It must be more scalable and low cost for data access through cloud server .Cloud is necessary to encrypted individual data before transmit the cloud and difficulty to search the encrypted data .For SSL,uses to encrypted the connection between user and google server when private data such as document and email to search the result.This approach to enable search over encrypted data on internet must be proceed follows the operation. Firstly , the data owner generated multi keywords to the outsourced data .These keyword encrypted and save from the cloud server then the search user need to access the outsourced data ,it must be select some relevant keyword and passing ciphertext of select keywords in cloud server to match the deployment data in this cloud and then match the result to the user.To achieve search of necessary over encrypted data of plaintext keyword searchthen the proposed system a multi-keyword search scheme to consider the relevance score of keyword utlilizes multidimensional tree to achieve efficient search query.This mainly attribute follows by to issues.Firstly,user important is most popular in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

normal text search and more accurately represent user requirements.It must be supported in encrypted data,Secondly,to improve the user experience for searching to enable the multi-keyword search for comprehensive logic operationsof keywords searching space to quickly identify the desired data .Searchable encryption with "OR","AND"operation.

2 SYSTEM MODEL, THREAT MODEL AND SECURITY REQUIREMENTS

2.1 System Model

Data owner: Dataowner outsourced her data to the cloud for easily access to the search user.Toprotect the data privacy,the data owner encrypted original data through symmetric encryptedowner .

Cloud server: It is an intermediate entity which stores the encrypted document and indexes are received from the data owner, and provide data access and search the services to search user then the keyword trapdoor to the cloud server, it matching documents based on the certain operation

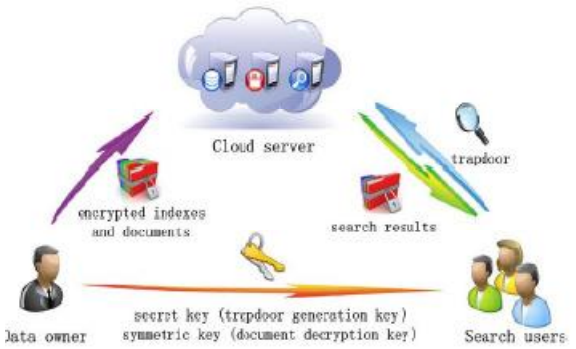
•*Search user*:A search user queries the outsourced document from the cloud server in three steps.Frist,receives both the secret key and symmetric key.Second,searching the keyword.

2.2 Threat Model and Security Requirement.

It must be the same as more related works on secure cloud data search.We have to threat models depend on the information available to cloud server

Known Ciphertextmodel:The internet only Known encrypted document collection and index collection

Known Background model:The server have more knowledge than what can access Known ciphertext model relationship between trapdoor and related statistical of other information



PROPOSED SCHEMES:

In this scheme mainly used to secure KNN computation scheme use for distance to select K nearest database records.We have initially data owner inorder to generate the secret key.In secret key send to data owner in secure channel where the symmetric key used to encrypted documents outsourced cloud server .

Index building:

It is used to utilize the data owner .In this schemes used to encrypted to collection of document and send the cloud server.We have form the content table in the data for cloud it must be easy to identify the encrypted data

Trapdoor generated: The keyword set for searching user in the index number. It send to the keyword in the cloud server.When the data transfer do not blocked the data in the cloud it must be very efficient to generating the trapdoor .In this schemes tosearch for encrypted cloud data use two schemes .

FMS-I

In this FMS-I calculated the importance score of data from thedocument.The choice factor for search keyword fromthedocument and longest preference factor keyword are same thedocument with higher relatedscore of keyword is better matching result

FMS-II

In this schemes to replace the search keyword we can also develop any operation it improve the user need of searching data.It must be support the multi keyword search to support thelogic operation to search"AND","OR","NO"operation of keywords.With"AND"operation to returned document matching all keywordthen the "OR"operation data must be either or not in data incloud to performed.It can only enabled search with single logic operation on keyword

LITERATURE SURVEY:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

1.Secured Multi-keyword Ranked Search over Encrypted cloud data

Data is stored as public or private and different searching strategies are available for types of data. The data are stored in the cloud using encryption technique. So the authenticated members who know the key can access the data. A different type of searching technique is used for encrypted data such as Fuzzy keyword search, conjunction of keyword.
In cloud computing,data management system of local site can be deployed to commercial public cloud for economic savings. To provide security to stored data, it must to encrypt before storing data. To find the solution of multi keyword encrypted cloud data while preserving strict system-wise privacy in the cloud computing. Among various multi-keyword semantics, the efficient measure is coordinate matching, to effectively capture the relevance of deployed documents to the query keywords, and use inner product to quantitatively evaluate such a measure of that document to the search query is used in MRSE algorithm.

PRIVACY PRESERVATION:

Analysis

In our scheme, correlating pseudonyms is infeasible without knowing the secret key used in generating them. Fake packets can make pseudonyms infeasible because the adversary cannot distinguish between event and fake packets. Christo Ananth et al. [6] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder. Sending fake and real packets confuses the adversary and makes time correlation infeasible even if there is only one event transmission.

Illegal Search Detection

Attacker has eavesdropped the secret key. Then he construct the authentication data; if the attacker has not eavesdropped the historical data. Further, if the attacker has successfully eavesdropped all data , the attacker can construct the authentication data and detected by the administration server. However, the legal data user performs the secret key on the administration and then the server side has changed, there will be contradictory secret keys between the administration server and the legal data systems. Therefore, the data user and administration server will soon detect this illegal action.

ENHANCED SCHEME:

It must be the part of dictionary will rapidly increase the dictionary becomes larger and more comprehensive .Fine grained multi keyword search scheme supporting classified sub-dictionary(FMSCS).It must classified total dictionary as common as sub-dictionary and manyprofessional sub-dictionary.The main goal is reduce the computation and communication.

CONCLUSION:

We have fine –grained multi keyword search issues over encrypted cloud data two schemes
FMS-I have relevance score and preference factor of keyword search and better user
FMS-II secure and efficient search with practical “AND”,”OR”,”NO” operation on keyword.In this scheme supporting classified sub-dictionary to improve efficiency.

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, “An smdp- based service model for interdomain resource allocation in mobile cloud networks,” 2012.
[2] M. M. Mahmoud and X. Shen, “A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805–1818, 2012.
[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, “Exploiting geo- distributed clouds for e-health monitoring system with minimum service delay and privacy preservation,” IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430–439, 2014.
[4] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, “Privacy- preserving data aggregation

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

without secure channel: multivariate polynomial evaluation," in Proceedings of INFOCOM. IEEE, 2013, pp. 2634–2642.

[5] Y. Yang, H. Li, W. Liu, H. Yang, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBCOM. IEEE, 2014, to appear.

[6] Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07

[7].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.

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

[9] R. Li, Z. Xu, W. Kang, K. C. Yow, and C.-Z. Xu, "Efficient multi- keyword ranked query over encrypted data in cloud computing," Future Generation Computer Systems, vol. 30, pp. 179–190, 2014.

[10] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage," IEEE Transactions on Emerging Topics in Computing, 2014, DOI10.1109/TETC.2014.2371239.

[11] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proceedings of ICDCS. IEEE, 2010, pp. 253–262.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Order-preserving symmetric encryption," in Advances in Cryptology-EUROCRYPT. Springer, 2009, pp. 224–241.

[13] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems, vol. DOI: 10.1109/TPDS.2013.282, 2013.

[14] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multi- keyword top-k retrieval over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239–250, 2013.

[15] A. Arvanitis and G. Koutrika, "Towards preference-aware relational databases," in International Conference on Data Engineering (ICDE). IEEE, 2012.