Encryption: Multi Keyword Search over Outsourced Cloud Data Using N-Gram

SUNITHA PACHALA[1],DANDU KARISHMA[2],KAVILIKATTA BHARATH KUMAR[3] AKULA DIVYA[4]

[1]Assistant Professor, Department of Computer Science and Engineering, PhD Scholar, (JNTUK),Dhanekula Institute of Engineering and Technology, A.P., India.

[2]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.

[3]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.

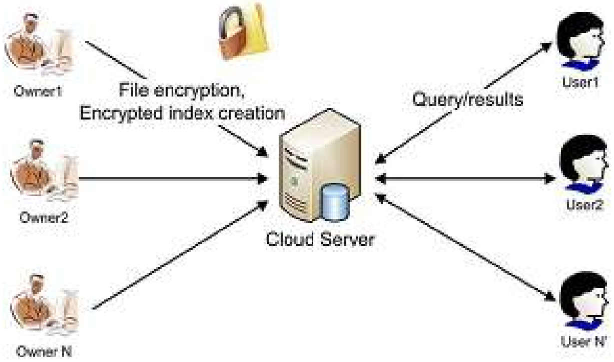
[4]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.

Abstract — Cloud computing has been envisioned as the next generation information technology architecture for enterprises, due to its long list of unprecedented advantages in the IT history. Data ownership in the cloud with increasing performance and range of offering, more and more enterprises is opting to take their services into the cloud. They are motivated to outsource their complex data management systems from local sites to commercial public cloud for more flexibility and economic savings. To protect the data privacy, cloud providers to build services that protect integrity of systems and the data itself. The perceptive data has to be encrypted before outsourcing for privacy, in which data utilization based on plaintext keyword search. To enable the data encryption in cloud, multi keyword search scheme is proposed. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results. In this paper, we proposed cloud based multi keyword search and privacy requirement for secure cloud data.

Keywords — *keyword search, ranked search, encryption, Cloud computing.*

INTRODUCTION

In cloud computing, A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability. Searchable encryption schemes enable the client to store the encrypted data to the cloud and execute keyword search over cipher text domain. The works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword boolean search, ranked search, multi-keyword ranked search, etc. Among them, multi-keyword ranked search achieves more and more attention for its practical applicability. Recently, some dynamic schemes have been proposed to support inserting and deleting operations on document collection. These are significant works as it is highly possible that the data owners need to update their data on the cloud server. But few of the dynamic schemes support efficient multi-keyword ranked search. Cloud is a enrollment which can be accessed from everywhere if deployed in that fashion. It causes jillion of parties or persons by it for their purpose. The keyword track method works certainly well if small number modifications will be done. So this paper also used the keyword accompany method.



In this paper, for the first time, we define and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system wise privacy in the cloud computing paradigm. Among various multi-keyword semantics, we choose the efficient similarity measure of “coordinate matching,” i.e., as many matches as possible, to capture the relevance of data documents to the search query. Specifically, we use “inner product similarity” , i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query. During the index construction, each document is associated with a binary vector as a sub index where each bit represents whether corresponding keyword is contained in the document. The search query is also described as a binary vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by the inner product of the query vector with the data vector. However, directly outsourcing the data vector or the query vector will violate the index privacy or the search privacy. To meet the challenge of supporting such multi-keyword semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner product computation, which is adapted from a secure k-nearest neighbor (kNN) technique , and then give two significantly improved MRSE schemes in a step-by-step manner to achieve various stringent privacy requirements in two threat models with increased attack capabilities. Our contributions are summarized as follows:

For the first time, we explore the problem of multi-keyword ranked search over encrypted cloud data, and establish a set of strict privacy requirements for such a secure cloud data utilization system.

We propose two MRSE schemes based on the similarity measure of "coordinate matching" while meeting different privacy requirements in two different threat models.

We investigate some further enhancements of our ranked search mechanism to support more search semantics and dynamic data operations.

Thorough analysis investigating privacy and efficiency guarantees of the proposed schemes is given, and experiments on the real-world data set further show the proposed schemes indeed introduce low overhead on computation and communication.

Compared with the preliminary version of this paper, this journal version proposes two new mechanisms to support more search semantics. This version also studies the support of data/index dynamics in the mechanism design. Moreover, we improve the experimental works by adding the analysis and evaluation of two new schemes. In addition to these improvements, we add more analysis on secure inner product and the privacy part.

IMPLEMENTATION

Admin Module:

This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart.

Client Module:

This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query. The user is going to select the required file and register the user details and get activation code in mail from the "customer service" email before enter the activation code. After user can download the Zip file and extract that file.

Multi keyword Module:

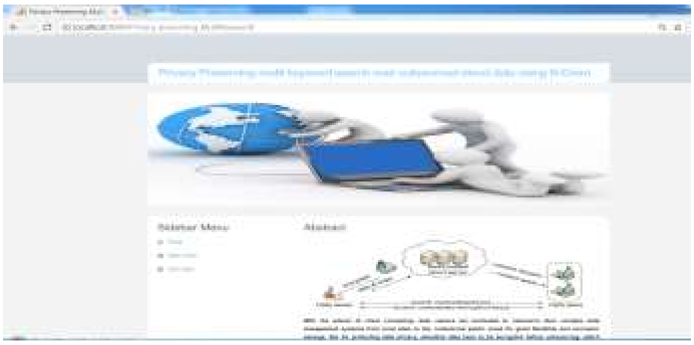
This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list.

Encrypt Module:

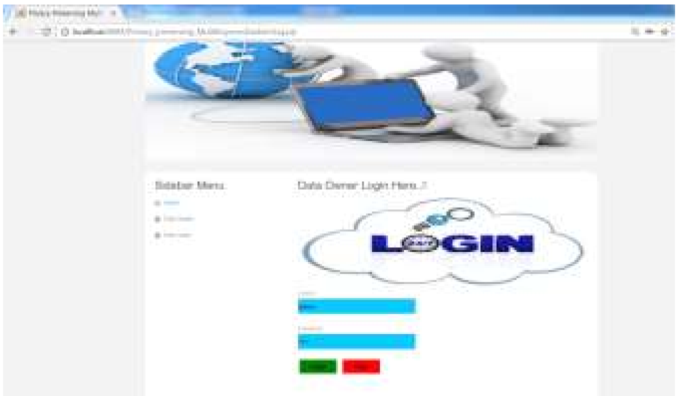
This module is used to help the server to encrypt the document using RSA Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.

OUTPUT SCREENS

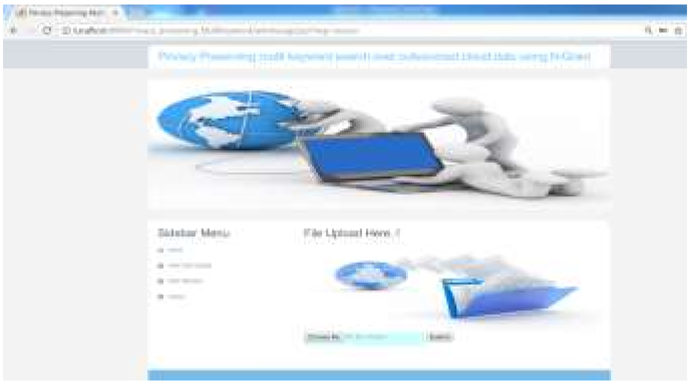
Index page



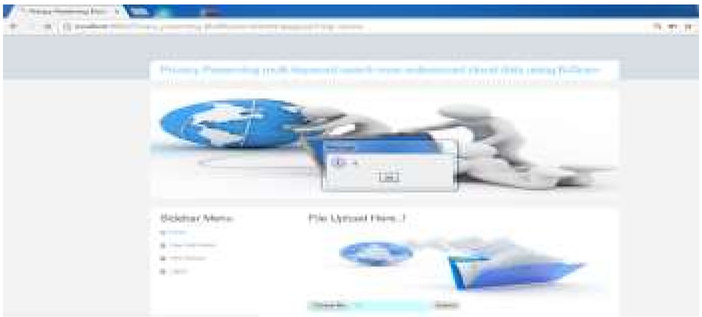
Admin Page:



File upload Page:



File upload success Page



CONCLUSION

In this paper, multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Dynamic secret key generation and a new data user authentication algorithms are use to authenticate data users and detect attackers who perform illegal searches. Secure search protocol is use to enable the cloud server to perform secure search among multiple owners data encrypted with different secret keys.

We developed a novel method of keyword transformation and introduce the stemming algorithm. With these techniques, the proposed scheme is able to efficiently handle more misspelling mistake. Our proposed scheme takes the keyword weight into consideration during ranking.

REFERENCES

Good Teachers are worth more than thousand books, we have them in Our Department.

[1] Wei Zhang, Yaping Lin, Sheng Xiao, Jie Wu, Siwang Zhou, "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing", IEEE Transactions on Computers, Vol. 65, No. 5, May 2016.

[2] Kalyani Sonawane, Rahul Dagade, "A 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.

[3] Ming Li, Shucheng Yu, Ning Cao, Wenjing Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing", 31st International Conference on Distributed Computing Systems, 2011.

[4] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Vol. 62, No. 2, February 2013.

[5] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou, Hui Li, "Verifiable Privacy-Preserving MultiKeyword Text Search in the Cloud Supporting Similarity-Based Ranking", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 11, November 2014.

[6] Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou, "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014.

[7] Zhangjie Fu, Xingming Sun, Zhihua Xia, Lu Zhou, Jiangang Shu, "Multi-keyword Ranked Search Supporting Synonym Query over Encrypted Data in Cloud Computing", 2013.

[8] Zhangjie Fu, Xingming Sun, Nigel Linge, Lu Zhou, "Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query", IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

[9] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li, "Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud", IEEE Transactions on

Parallel and Distributed Systems, Vol. 27, No. 4, April 2016.

[10] Zhangjie Fu, Jiangang Shu, Xingming Sun, Nigel Linge, "Smart Cloud Search Services: Verifiable Keyword-based Semantic Search over Encrypted Cloud Data", IEEE Transactions on Consumer Electronics, Vol. 60, No. 4, November 2014.