An Efficient Privacy-Preserving Ranked Keyword Search Method

Nagapathmashree V[1] Varshini K[2] Udhaya R[3]
[1,2,3]Student
[1,2,3]Department of Information Technology
[1,2,3]Sri Krishna College of Engineering and Technology, Coimbatore, India

Abstract— In this paper a different product rating approach for analytically and visually analyzing sales of similar kind of products from various manufactures with repeated mixture of products is considered. There is no particular rating for products of same type and combination of product purchasing pattern in the market. Using this we regain the perfect mixture of products with analytically rating. Visual representation of rating and mixture of product of similar kind is made by using this rating and pattern to contrast with each other. Data mining gives more conceptual knowledge to identify business processes. The main use of this is to satisfy the requirements of customers. By identifying it analytically the perfect one is studied such as user fulfillment, product productivity and acceptance.

Key words: Information Regains, Related Suggestions, Query Vector

I. INTRODUCTION

Nowadays terabytes of data are produced word-wide in this big data period. In order to decrease data management cost and storage facility large amount of data which is usually owned by the ventures and users they prefer to obtain their valuable data to cloud facility. As a result, volume of data in cloud storage facilities is undergoing a considerable increase. Even though the cloud service provided by the cloud server providers (CSPs) state that their cloud service is equipped with high security measures, security and privacy are major drawbacks preventing the wider assumption of cloud computing service.

Data encryption is a conventional way to decrease the information leakage. However, it will make effective use of data in the server-side, such as searching on encrypted data, becomes a very difficult task. In the recent years many cipher text search schemes suggested by researchers is done by including the cryptography techniques.

These methods have been produced with expected security, but their methods need huge operations and high time complexity. In this big data era where data size is very big and it needs online data processing therefore previous methods are not suitable. Also, the relationship between documents is hidden in the above methods.

Maintaining the relationship between the documents is essential to fully express a document. For example, the relationship can be used to identify its category. This important property has been hidden in the conventional methods due to blind encryption. Therefore, a method which can maintain and use this relationship to speed the search phase is recommended.

Due to failure of software/hardware and storage duplicity, the search results received to the users may have harmful data or have been changed by the malicious administrator. To verify the accuracy and perfectness of the search results an accurate mechanism must be provided for users.

II. LITERATURE SURVEY

Many ventures and customers are moving their precious data to the cloud with the advantage of storage as a service because it costs less, easily changed and can be accessed from anywhere any time. The most important thing here is the trust between cloud user and provider by using security as a parameter.

Cryptography is a way of initiating trust. Searchable encryption provides security which is a cryptographic method. Many researchers have been working to provide an effective searchable encryption schemes in literature. This paper examines some efficient cryptographic techniques build on data structures like B-Tree and CRSA to extend the level of security [1].

Cloud computing is creating great interest to supply solution for outsourcing of data and data services of high quality. More number of institution, organizations and corporations are examining the chances of having their applications, IT resources and their data in cloud [2].

Nowadays, more number of people is influenced to outsource their local data to public cloud servers for great satisfaction and minimized costs in data management. But when it comes to privacy issues, before outsourcing easily damageable data should be encrypted, which results in conventional data utilization like document retrieval based on keyword [3].

This paper present a secure and effective ranked keyword search technique on encrypted data, which helps in update operations like insertion and deletion of products and also giving ranking and feedback to the products [4].

Particularly, we build an index tree to provide ranked keyword search based on vector space model, which helps flexible update operations. A search algorithm which is based on "Greedy Depth first Traverse Strategy" is examined to improve search efficiency. To protect the privacy of search, examine a secure method to meet many privacy requirements in the cipher text threat model [5].

III. OUR CONTRIBUTION

In this paper, to maintain the relationship between various plain text documents over the encrypted one we examine a multi-keyword ranked key search method over encrypted data which is based on the hierarchal clustering index (MRSE-HCI) to increase the search efficiency.

In the present architecture, accompanying with a growing size of data collection the search time has a linear growth. We obtain this idea from the examination that customer's retrieval needs usually focus on a particular field. So the searching process can be speeded up by computing related score between the documents and query which belong to the same particular field with the query.

As a result, the documents which are classified in the particular field by the users query will be evaluated to obtain their relevance score. By this only the user specified documents are searched, the rest are ignored. Thus the search efficiency is enhanced.

IV. MODULE DESCRIPTION

A. Register

In this module the user has to provide the basic information like name, mobile number, email address, address to get registered.

B. Login

The registered users must provide their username and password to sign into the account. The users who have logged in is provided a session for further reference.

C. View products

The products available in the cart are viewed in this module. The products along with the full specification can be viewed by the users after successful login in this module.

D. Post Review

The users who viewed the products can post their rating in this module. The users can also provide the rating on five star levels. The review of the products can be posted by the users in this module.

E. Manager Side

In this module manager will offer particular products. It means manager check the review of products. And which products review is low stars means he/she will be offer that particular products.

F. Graph Result

The sentiment of the reviews posted by the users is identified in this module. The sentiment of the review is identified using sentiment analysis from the comments posted by the users. The user review sentiment of each product is analyzed in graphical representation.

V. RESEARCH METHODOLOGIES

A. Existing System

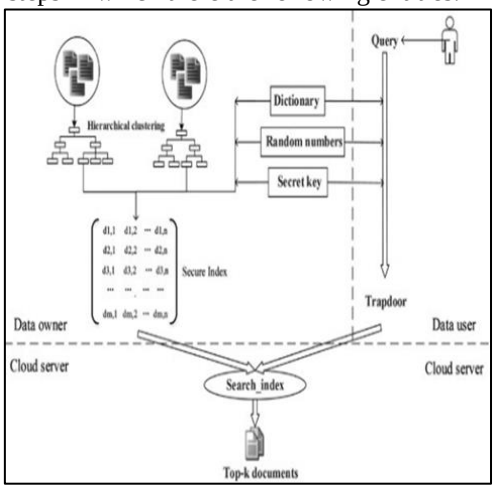
In existing system, the organization only has the production report. In this report, we get the information about the quantity of products that are sold on daily basis. But as new customers come in market, they don't have an idea of which product to be picked from the collection of products of the same type.

Thus the customer picks random products and after using it if person does not find it efficient and this is the drawback of existing system.

B. Proposed System

In our System, we take the feedback and ratings from the customer and also Generate rating from system by taking this further we calculate the average mathematical rating for a specific product.

We also obtain which product is sold more in the particular category, by using the choices of customer and sales report we can give recommendation to the future customers and it will be very helpful to them for buying the products. The implementation of our project will go through various steps in which there are following entities.



We introduce the MRSE-HCI scheme. The vector space model adopted by the MRSE-HCI scheme is same as MRSE but slightly differs on the process of building index. Instead of sequence index the hierarchal index structure is introduced into the MRSE-HCI.

In MRSE-HCI, each document is indexed by a vector. Each part of the vector defined for a keyword and represents a value whether the keyword is present or not in the document.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, in the scenario of cloud storage we examined the cipher text. Maintaining the close relationship between the documents over the encrypted documents is vital. We introduced a design method which is given to enhance the efficiency of the search. Two main operations are performed by the users, one is rating and the other is feedback. Users can give their rating to the products and also write feedback about the products listed.

In addition, by using the two widely used threat models we studied the search efficiency and security. To study the search efficiency, accuracy, and rank security a platform is built to experiment the above qualities. The results of the experiment shows us that the present system not only solves the problem of multi-keyword ranked search, but also gives an enhanced search efficiency, rank security, and the relevance between retrieved documents.

In this paper, we have used the semantic search method which is it shows the only related documents which is specified by the user the other documents are ignored and thus it saves the search time and increases the efficiency of search.

REFERENCES

[1] E.-J. Goh, Secure Indexes, IACR Cryptology ePrint Archive, vol. 2003, pp. 216. 2003.
[2] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and effi- ciently searchable encryption," in Proc. 27th Annu. Int. Cryptol. Conf. Adv. Cryptol., Santa Barbara, CA, 2007, pp. 535–552.

[3] C. Wang, N. Cao, K. Ren, and W. J. Lou, "Enabling secure and effi- cient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug. 2012.
[4] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean que-ries," in Proc. Adv. Cryptol,. Berlin, Heidelberg, 2013, pp. 353–373.
[5] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. Conf. Comput. Commun. Secur., 2012, pp. 965–976
[6] M. Chase and S. Kamara, "Structured encryption and controlled disclosure," in Proc. Adv. Cryptol., 2010, pp. 577–594.
[7] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M. C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation," in Proc. Netw. Distrib. Syst. Security Symp., vol. 14, 2014, Doi: http://dx.doi.org/ 10.14722/ndss.2014.23264.
[8] R. X. Li, Z. Y. Xu, W. S. Kang, K. C. Yow, and C. Z. Xu, "Efficient Multi-keyword ranked query over encrypted data in cloud computing, Futur. Gener. Comp. Syst., vol. 30, pp. 179–190, Jan. 2014.

