2019 International Conference on Information Science, Medical and Health Informatics (ISMHI 2019)

Research on Ciphertext Query Method of Searchable Encrypted Database Based on Cloud Computing

Chen Mingdong

Aba Normal University, Wenchuan, Sichuan, China

Keywords: Cloud Computing, Encrypt Database, Ciphertext Query, Method Study

Abstract: in Recent Years, with the Rapid Development of Computer Technology, the Application Process of Cloud Computing Technology is Also Advancing. At Present, Cloud Computing Has Been Widely Used in Related Technology Industries, Providing Information Services for Many Users. However, Because the Data is Stored in the Cloud Server, the Authorized Users Are Limited by the Encryption Database Key When They Acquire the Data, So They Cannot Achieve Efficient Query. Based on This, This Paper Studies the Ciphertext Query of Searchable Encrypted Database, and Proposes Keyword Query, Public Key Encryption Query, Semantic Association Keyword Ciphertext Query and Other Ways, Hoping to Make the Search More Effective and Improve the Data Utilization Rate.

1. Introduction

1.1 Literature Review

As a new technology in the field of computer, cloud computing plays an important role in e-commerce, social networking, information storage and so on. At present, data searching in encrypted databases in cloud computing has been paid more attention by relevant scholars (Yuan and Liu, 2014). When Chen Cuiyi and Wu Shangkun studied the efficient query method of ciphertext, they summarized the index mechanism of ciphertext data and concluded three mechanisms: direct index of ciphertext data, address encrypted ciphertext index and dynamic secure ciphertext index. It also summarizes query efficiency, query function, network load, security and other related issues (Cheng and Wu, 2013). Meng Kai and Yan Hongyin, on the other hand, designed a two-dimensional array ciphertext index scheme by studying the mainstream database. To query the index value, they need to use the hash algorithm to get the primary key according to the result so as to decrypt and get the plaintext information (Meng and Yan, 2012). Zhang Kejun and other scholars put forward data security and retrieval efficiency based on cloud computing, which can use full-text retrieval scheme, which is applicable to massive data encrypted storage and efficient security retrieval (Zhang et al, 2017). Wang Guowei and other scholars think that the encrypted database will store the privacy encrypted in the database, this scheme will make the plaintext data lost, and the scheme has defects. Based on this, the researcher designed the encryption system for statement rewriting, plaintext data encryption and information query processing (Wang et al, 2017). Based on the problem of high search complexity of cloud computing encryption scheme, Jia Qiang and other scholars proposed to optimize the index value by using block structure, specifically divided into three categories: small, medium and large. With the increase of index value, the linear limit of key words decreased significantly (Jia, 2019).

1.2 Purpose of Research

Cloud computing, as a computing model, has made rapid development in recent years with the advantages of convenient management and fast computing. Based on this, many users use encrypted database to store data information. In order to ensure the security, they will also encrypt. However, the massive data stored in cloud computing increases many difficulties for authorized users to retrieve information, and even suffer from external attacks to steal customer information. However, when combing the relevant research, the author found that the research of multiple mathematicians

DOI: 10.25236/ISMHI.2019.090

is one-sided, unable to give consideration to both search efficiency and security. Based on this, on the premise of ensuring data security, this paper studies retrieval methods in order to enrich relevant research theories.

2. Analysis of Cloud Computing Related Technologies

At this stage, cloud computing is a new Internet computing system that adapts to the development of the Internet, and is widely used in e-commerce, social networking and other fields. At present, there are four kinds of cloud computing facilities. The first is the public cloud that serves the public and supports a large number of data operations. The second is to only serve enterprises or individuals for data information, not for external resource sharing. The third type is the community cloud where multiple enterprises or individual customers provide unified services within the local area. The last is the more convenient hybrid cloud. This cloud computing model extracts the unique advantages of public cloud and private cloud, which not only improves the computing capability, but also ensures the security performance of the computing process. Generally speaking, cloud computing is mostly used for searchable encrypted database and ciphertext query, which is a platform for complex information processing and data calculation. There are three general computing methods: grid, utility, parallel and distributed computing (Wan, 2017). The first kind of grid computing, which has strong data processing ability, can divide the data to be processed into blocks according to the data range, and calculate the data block through programming, so as to achieve the final purpose of data processing. The second way of utility calculation, the so-called utility calculation, is to reduce the cost of service, on the basis of customer service, to achieve the optimal utilization of resources. However, this calculation method is mostly to provide resource services for customers and charge different fees according to different resource occupancy. The last kind of parallel and distributed computing is an effective way to improve the computing speed. Specifically, it uses the computer to divide the subsystem and uses the multiprocessor to realize the serial computing. This kind of algorithm can use programming language to realize thread parallel and improve computer processing ability. When users use computers to query ciphertext of searchable encrypted database, they should consider data security. Based on the background of cloud computing, the current security issues involved in retrieval are divided into the following five categories: security standards, network security, access control, cloud infrastructure, data security, etc. Under the standard requirements of service level agreement, the total dos and protocol vulnerabilities are denied. Under the unauthorized state, the user access rights are controlled to protect the user data from being leaked. Although cloud computing provides many conveniences in ciphertext query and improves resource utilization, the corresponding security solutions are also indispensable for data protection in searchable encrypted database at this stage.

3. Ciphertext Query Method of Searchable Encrypted Database Based on Cloud Computing

3.1 Keyword Query

At present, there are many researches on ciphertext retrieval in searchable encrypted database. Many scholars at home and abroad have done in-depth research on ciphertext query, among which the most commonly used query technology is keyword query. This query method is to search the article word matching after the user submits the data, and the ECS will perform the matching operation to get the corresponding data. However, this query method is single linear search, and the retrieval efficiency is low in the massive data of cloud server. However, this method will greatly improve the retrieval efficiency when using multiple keywords for search. In the case of searchable encrypted database, it requires cooperation between data owners and authorized users to provide multiple keywords, so that authorized users can improve the query efficiency. Alternatively, BLOOM filter can be used for query filtering. This filtering will filter the same keywords encrypted by private key or public key in the encrypted database and merge them to obtain correct matching.

However, the encrypted storage used by Bloom filter will produce a small probability of query errors. Keyword index is generally aimed at data information query open to multiple users in encrypted database. Generally, the data required for such query is less encrypted and the user authorization is more extensive.

3.2 Public Key Encryption Query

Encryption is a retrieval method that encrypts the data owner and the data receiver at the same time. The data owner encrypts the transmitted content during retrieval and the receiver decrypts the data after receiving the information. This kind of public key encryption method avoids the problem of key disclosure, but it can only be used when the two keys are interrelated. Specifically, the data owner can add a key to the plaintext, and the attacker wants to get the specific data by unlocking the private key, but when the public key is encrypted, the data in the database can be double protected to avoid the direct disclosure of plaintext. Based on this public key encryption method, there are three requirements for data handling. The first is the data owner's encryption of plaintext. The data owner needs to integrate the required documents, use psks algorithm to encrypt the search keywords, and then upload them to the cloud server. Through the second entity, that is, the cloud server for cloud computing, the uploaded data needs to be transmitted so that the receiver can fully receive the transmitted data, and during this period, the data will not be intercepted. The last part is to authorize users to use the private key and keywords to calculate and obtain the key trap value, and search the ciphertext in the searchable encrypted database through the trap algorithm. In the process of public key encryption query, a large number of decryption processes will also reduce the functionality of ciphertext database. Therefore, public key encryption is only used when there are hard requirements for file security.

3.3 Semantic Association Keyword Ciphertext Query

At present, ciphertext retrieval is limited by encrypted database query, and most of them can only carry out exact keyword matching to realize query. However, the semantic association of some words is not the same in the process of query, which means that some related documents may not be retrieved. Some users may know little about their own retrieval field when they query the required data, and the keywords that can be submitted cannot be recognized by the encrypted database, resulting in incomplete search results. The semantic association keyword ciphertext query avoids this misunderstanding. This query method will automatically associate according to the user's query keywords, display the relevant keywords, let the user more specifically express the data information to be queried, and improve the accuracy of data query. However, at present, only plaintext retrieval can be used to query ciphertext with semantic association keywords. When multiple encryption or more strict encryption is used for documents in encrypted database, this ciphertext query method will play a very small role. Most of the existing ciphertext retrieval technology and the implementation of keyword Association query, but the multi encryption ciphertext retrieval rarely consider the semantic association of the words, resulting in the search results can not fully meet the needs of users.

4. Conclusion

Encrypted database ciphertext query method is an important research direction in related fields. Encrypted database provides many conveniences for data storage and extraction. However, compared with plaintext database data retrieval, data retrieval in ciphertext database will have problems of low efficiency, incomplete function, fuzzy query and low security. With the development of cloud computing technology, the importance of retrieval method becomes more and more obvious. In order to improve the retrieval efficiency and information utilization rate, it is urgent to study the query methods in depth, and to find a suitable retrieval method for encrypted database is an urgent problem. With the rapid development of computer technology and the deepening of cloud computing, based on the current retrieval method, it is of great practical significance to explore the query method.

References

[1] Yuan H., Liu Z.F. (2014). Research on Data Search and Encryption Scheme Based on Cloud Computing, Silicon Valley, 7(5), 63-63.

[2] Cheng C.Y., Wu S.K. (2013). Research on Query Technology of Ciphertext Database, Modern Computer Xunkan, 30(4), 13-16.

[3] Meng K.,Yan H.Y. (2013). Fast Query of Ciphertext Database, Computer Development and Application, 25(4), 82-84.

[4] Zhang K.J., Zhang G.L., Jiang C,. et al. (2017). Research on Ciphertext Full-text Retrieval Based on Searchable Encryption Technology in Cloud Environment, Computer Application and Software, 34 (04), 41-47.

[5] Wang H.W., Yang G., Liu G.X,. et al. (2017). Design and Implementation of Searchable Database Encryption System, Computer Technology and Development, 26(08), 136-140.

[6] Jia Q., Zhang S., Zhou F.C,. et al. (2019). A Searchable Encryption Scheme for Ciphertext Large Data Sets, Journal of Northeast University (Natural Science Edition), 40 (7), 913-919.

[7] Wan M.J. (2017). Research on Query Algorithm Based on Matrix Encryption in Cloud Computing Environment, Science and Technology Bulletin, 33(7), 125-128.