Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Multi Keyword Ranked Search for Preserving Privacy in Cloud Computing

[1]Bhavya N Javagal,[2]Nidhi, [3]Shivam Panwar, [4]Rizwan Shariff, [5]Arpan Das

Abstract

As the popularity of cloud computing has increased, we saw a rapid growth among the data owners uploading the data to the cloud servers and later retrieving them according to their convenience Now to provide security to the data, secure searches over encrypted cloud data has inspired many research work over single owner model. However there are more than one owners sharing the cloud.So in this paper we provide a scheme to deal with multi keyword ranked search for preserving privacy in cloud computing.It enables the cloud servers to perform safe search without knowing the actual data and also setting up an order for privacy preserving function family.To safeguard the user data from a third party dynamic secret key generation protocol is used and new login id authentication protocol is used.

Keywords: Cloud computing, ranked keyword search, multiple owners, privacy preserving, dynamic secret keys.

INTRODUCTION

Cloud computing is no doubt an effective approach to deal with big data, through providing on-demand high quality services from powerful and configurable computing resources. One application of cloud computing is database as a service". where the data owner outsources complex database management systems into the cloud server. To protect data privacy against attacks from the cloud server, confidential data must be encrypted before being uploaded to the cloud server. This, however, makes it difficult to perform traditional query processing operations. This problem faces two challenges. First, the confidentiality requires hiding the values and the relative order of the attribute in records from the cloud server, but computing a range query requires comparing the values of this attribute. We will discuss the reason why protecting the relative order is important soon in the following context. Second, since the encrypted data does not preserve the closeness of plaintext values (for privacy reasons), a straightforward search has to scan the entire encrypted data to retrieve wanted records, which is not scalable for data of the cloud scale. In this work, we present a novel searchable encryption/index scheme to address these challenges.

To improve the search result accuracy as well as to enhance the user searching experience, it is also necessary for such ranking system to support multiple keywords search, as single keyword search often yields far too coarse results. As a common practice indicated by today's web search engines (e.g., Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. And each keyword in the search request is able to help narrow down the search result further. "Coordinate matching", i.e., as many matches as possible, is an efficient similarity measure among such multi-keyword semantics to refine the result relevance, and has been widely used in the plaintext information retrieval (IR) community. However, how to apply it in the encrypted cloud data search system remains a very challenging task because of inherent security and privacy obstacles, including various strict requirements like the data privacy, the index privacy, the keyword privacy, and many others.

ABOUT SYSTEM

EXISTING SYSTEM

Encryption is a flawless approach to secure information protection which likewise offers ascend to the trouble in executing normal question on such scrambled information. To keep the upside of preparing limit on the server side, it is not sensible to download the entire encoded data and execute the request on the data in the wake of unscrambling, the cloud server should have the capacity to execute address direct over the mixed data and give back the

correct results to the customer.There have been extensive interests in questioning encoded information and different inquiries are considered. Rapidly, the works consolidate correspondence test, go request look for, aggregate question count and furthermore watchword based question interest or comparability request look.To improve look functionalities, conjunctive watchword look for over mixed data have been proposed. These arrangements gain far reaching overhead achieved by their key primitives, for instance, computation brought by bilinear guide, for example, or correspondence inflicted significant damage by puzzle sharing, for example, As a more expansive chase approach, predicate encryption arrangements are starting late proposed to reinforce both conjunctive and disjunctive request. Conjunctive catchphrase look gives back win enormous or forget about it," suggests it just returns those documents in which each one of the watchwords dictated by the request address appear; disjunctive catchphrase look for returns undifferentiated results, which infers it gives back each record that contains a subset of the specific watchwords, even only a solitary watchword of interest. Basically, none of existing Boolean catchphrase searchable encryption arranges support different watchwords situated look for over encoded cloud data while shielding security as we propose to research in this paper.

DISADVANTAGES

The primary disadvantage is information encryption just make on prior framework, so security less.
The catchphrase segregation couldn't be secured in people in general key setting since server could encode any watchword advance.
This structure depend on the exorbitant number of coordinating methodology on elliptic twists.
The balanced secure inside thing number arrangement is not well satisfactory for our MRSE plot.The put stock in equipment, which is put at the server side and is alter safe, has constrained limit away and handling power

PROPOSED SYSTEM

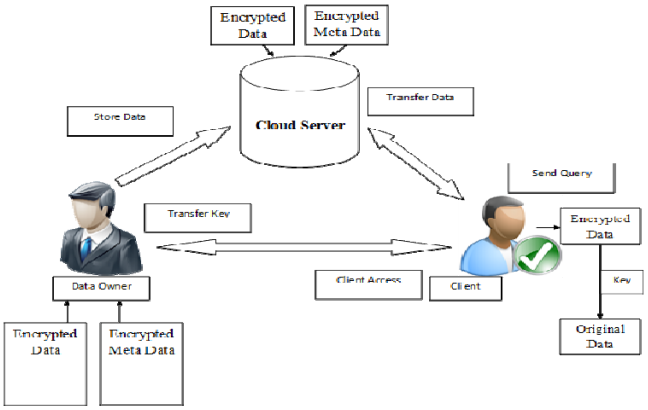

Figure1: Proposed system

The first occasion when, we characterize and take care of the issue of multi-watchword positioned seek over encoded cloud information (MRSE) while protecting strict systemwise security in the distributed computing worldview. Among different multi-catchphrase semantics, we pick the productive similitude measure of "organize coordinating," i.e., however many matches as could be expected under the circumstances, to catch the significance of information reports to the pursuit inquiry. In particular, we utilize "inward item comparability", i.e., the quantity of inquiry catchphrases showing up in a report, to quantitatively assess such likeness measure of that record to the pursuit question. Amid the file development, each record is related with a twofold vector as a subindex where each piece speaks to whether comparing catchphrase is contained in the archive. The hunt inquiry is likewise depicted as a double vector where each piece implies whether comparing watchword shows up in this pursuit ask for, so the likeness could be precisely measured by the internal result of the question vector with the information vector. Notwithstanding, specifically outsourcing the information vector or the question vector will abuse the file protection or the pursuit security. To address the difficulty of supporting such multikeyword semantic without protection breaks, we propose a fundamental thought for the MRSE utilizing secure internal item calculation, which is adjusted from a safe k-closest neighbor (kNN) strategy and after that give two essentially enhanced MRSE plots in a well ordered way to accomplish different stringent security prerequisites in two danger models with expanded assault capacities. Our commitments are abridged as takes after:

1. Interestingly, we investigate the issue of multikeyword positioned look over encoded cloud

information, and set up an arrangement of strict protection prerequisites for such a safe cloud information use framework.

2. We propose two MRSE plans in view of the similitude measure of "facilitate coordinating" while at the same time meeting diverse protection prerequisites in two distinctive danger models.

3. We explore some further upgrades of our positioned seek component to bolster more inquiry semantics and dynamic information operations.

4. Intensive examination exploring security and proficiency certifications of the proposed plans is given, and investigations on this present reality informational index additionally demonstrate the proposed conspires for sure present low overhead on calculation and correspondence.

ADVANTAGES

Its great flexibility and industrial savings are prompting both individuals and enterprises to source their local complicated data administrated system into the cloud.
MRSE schemes to achieve different stringent privacy requisites in two various threat designs.
Service provider did not know about the original content in the data owner that is the encrypted data most secure.
Standard deviation is normal to be smaller so as to earn high rigor indicating the good purity of reclaimed documents.

Module description

Our paper comprises of four modules namely

2.1 ***Data & Index generation***

In this module the data owner selects the data and creates the bit vector for the datausing the bit vector for the data the binary data can be generated. The bit vector is nothing but the bytes format of the data. In this module, we also generate the index for the data using the record numbers.These bit vector and the binary data are ready for the data ciphering.

2.2 Data ciphering

In this module the binary data is taken as input for encryption algorithm that converts binary data into cipher text.The main objective here is to have privacy on the data that is being stored on the remote computer.The remote computer is supposed to only the encrypted data 'c' and searchable index 'i'.The c and I will be uploaded by the data owner. The data owner then would be confident that the security of the data is achieved on the server side where attackers cant use the data.

2.3 ***Data User Access Control***

The user needs the data from the server. The user has different choices and the user can spend the query to the server or the service provider accessing the data but before the user sends the request to the service provider the user must send his details the owner. Only then the data owner receives the information from the client and is ready to send the decryption key. The access control mechanism is employed to manage the decryption capabilities given to the user and securely managing the encrypted data on the cloud server.

2.4 ***Data User Query***

The data user query is processed by the service provider. For any given query or keyword the service provider generates the bit vector and searches the date based on the query or the keyword. The encrypted data then would be sent to the data user which is in turn can be decrypted using the decryption key, which was shared by the data owner earlier. The query is designed in such a way that it allows multi keyword search and provide results based on ranking for effective data retrieval. The data users can then use the results of the query for his purpose.

Conclusion

A noteworthy test or worry in the distributed computing worldview is information protection. On one hand, there is a request to use the effective assets of the cloud server to give administrations to customers. Then again, the cloud server must not take in any delicate data about the information being overseen and the questions being replied. We consider the administration of noting the class of range inquiry look over numerical information and propose an information encryption plan to address these necessities. To portray and take care of the issue of multi-watchword positioned look over encoded cloud information, and set up an alternate of security needs. This proposed an essential arrangement of MRSE utilizing ensure inward work calculation. It additionally question some further change of our positioned seek device, contains supporting more inquiry definition. There is an interest to make advantage the intense wellsprings

of the cloud server to create administrations to customers.

References

[[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *Proc. IEEE INFOCOM*, pp. 829-837, Apr, 2011.
[2] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50-55, 2009.
[3] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," *Proc. IEEE INFOCOM,* pp. 693-701, 2012.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security*, Jan. 2010.

[5] A. Singhal, "Modern Information Retrieval: A Brief Overview," *IEEE Data Eng. Bull.*, vol. 24, no. 4, pp. 35-43, Mar. 2001.

[6] I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. *Morgan Kaufmann Publishing*, May 1999.

[7] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," *Proc. IEEE Symp. Security and Privacy*, 2000.

[8] E.-J. Goh, "Secure Indexes," *Cryptology ePrint Archive* /2003/216. 2003.

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," *Proc. Third Int'l Conf. Applied Cryptography and Network Security*, 2005.

[10] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," *Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06*), 2006.

Author's details

1 Bhavya N Javagal, Teacher,Computer science department, T. John Institute Of Technology, Karnataka, India, bhavya@tjohngroup.com
2 Nidhi,Student, Computer science department, T. John Institute Of Technology, Karnataka, India,chandelnidhi15@gmail.com
3Shivam panwar, Student, Computer science department, T. John Institute Of Technology, Karnataka, India, Shivampanwar365@gmail.com
4Rizwan sheriff Student, Computer science department, T. John Institute Of Technology, Karnataka, India, rizwansharif@gmail.com
5 Arpan das, Student, Computer science department, T. John Institute Of Technology, Karnataka, India, das.5arpan@gmail.com