ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Content Aware User Data Sharing and Anonymous Authentication on Public Cloud

[1]Ms. Saranyaa T, [2]Ms. Sangeetha S., [3]Mr.Vivek. M, [4]Mr. E. Mohanraj
Department of Computer Science and Engineering,
K.S.Rangasamy College of Technology, Tiruchengode
[1-3]UG Student, [4]Associate Professor

Email id: saranyaa96thiyagu@gmail.com

ABSTRACT

Cloud computing provides all types of resources as services. Hardware and software resources are shared with reference to the user demands. Service components are deployed to support the enterprise applications. It define and solve the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM), and establish strict privacy requirements for a secure cloud data utilization system to become a reality. The loosely coupled content-based provides an expressive form of communication for large-scale distributed systems. To avoid third party deployment confidentiality plays a major role for challenge over multiple administrative domains. Reduction of misunderstands by the usage of bloom filter and Enhanced Association rule mining.Among various multi-keyword semantics, the user choose the efficient principle of "**Enhanced Association Rule Mining".**

KEYWORDS

Multi-Keyword Query, Encrypted Cloud Data, Content Based Publish, Loosely Coupled, Enhanced Rule Association Rule Mining and Bloom Filter Algorithm

1. INTRODUCTION

The cloud stores a major storing data in which information system contrasted with continuous function . The physical storing multiple servers and the physical environment is typically owned and managed by hosting company. In the cloud, providers are responsible for keeping the data available and accessible. The physical environment protected on running. The capacity from the provider are used to storethe user data and application data in the cloud mechanism. Cloud storage services are accessed through computer service, and the user services application programming interface (API). It is used in cloud storage gateway or user based content management systems.

NETWORK SECURITY

Network is a group of computer systems and other computing hardware devices that are linked to computer networks and their management. It is used to communicate with the resources of the user and sharing the data among a wide range of users. In the Network security the action refers to any activity designed to protect the data from the usability criteria and integrity of the network and data used in the management of cloud databases. It includes both hardware and software technologies to design the protecting networks. The network security effectively manages the accessment to the network. The variety of thread management and stops them from entering or spreading on your network.

2. EXISTING SYSTEM

A prefilter doesn't store the elements themselves, this is the crucial point. Don't use a prefilter to test if an element is present, you use it to test whether it's certainly not present, since it guarantees no false negatives. Prefilter use *in conjunction* with a structure like a hash table, once you're certain the element has a chance of being present.We propose a joint semantic-visual space for web image indexing. In contrast to existing methods, the latent space is seamlessly modeled and alleviates the semantic gap between visual features in the continuous space and semantic attributes in the discrete space.We develop an iterative optimization algorithm for the proposed space formulation based on two constraints on predicted attributes and redundant features in their original spaces.

3. DRAWBACKS

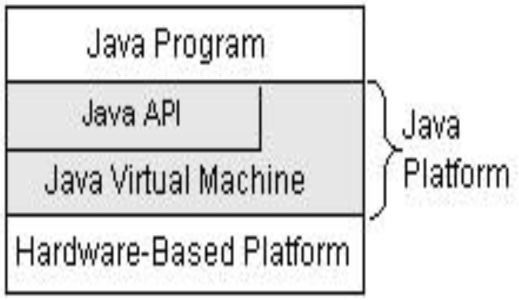
Multiple files are accessed by the middleware users are used in the implementation of existing system and to overcome this drawback, in the proposed system Enhanced Association Rule Mining Algorithm(EARM). Authentication problem occur and this is the drawback.

4. PROPOSED SYSTEM

It is defined and solved the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, user can choose the efficient principle of "coordinate matching". Construct a privacy policies for such a secure cloud data utilization system. From number of multi-keyword semantics, It select the highly efficient rule of coordinate matching, i.e., as many matches as possible, to identify the similarity batten search query and data, and for further matching It use inner data correspondence to quantitatively formalize such principle for similarity measurement. It first proposed a basic Secured multi keyword ranked ontology keyword mapping and search scheme using secure inner product computation, and then improve it to meet different privacy requirements.

FEATURES

The software components provides useful capabilities with the help of java API in large collection, such as graphical user interface(GUI) widgets. Software components are grouped into large libraries(packages) of related data's in the software pool. As java is a platform-independent environment, Java can be a bit than native code. Tuned interpreters and smart compilers and just-in-time byte code compiler can bring native code closer to the java object oriented language without threatening portability.



JAVA ARCHITECTURE

5. MODULES

5.1 Cloud Setup Module

The multi-keyword query which enhances the schemes and provide result for the module and allow for similarity ranking for effective data retrieval, instead of returning undifferentiated results. Privacy-Preserving: To prevent the cloud server from learning additional information from the dataset and the index, and to meet privacy. Efficiency and the above goals on functionality and privacy should be achieved with low communication and computation overhead.

5.2 Prefiltering And Security Management Module

The user can get the accurate result by using this modulebased 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, prefilter the matched word list from the database and the user gets the file from that list. The search query is also described as a binary vector association rule each bit means whether corresponding

keyword appears in this search request. The similarity could be exactly measured by inner product of query vector with data vector.

5.3 Encrypt Module

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

5.4 Client Module

The module are used to check the client valid username and password of the file using multiple keyword search concepts 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 "customerservice404" email before enter the activation code. After user can download the Zip file and extract that file.

5.5 Multikeyword Module

The module are used to check the client valid username and password of the file using multiple keyword search concepts and get the accurate result list based on the user query.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. 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 inner product of query vector with data vector. user directly outsourcing data vector or query vector will violate index privacy or search privacy. To meet the challenge of supporting such multikeyword semantic without privacy breaches, It propose a basic SMS scheme using secure inner product computation, which is adapted from a secure k-nearest neighbor (kNN) technique, and then improve it step by step to achieve various privacy requirements in two levels of threat models.Propose two schemes following the principle coordinate matching and inner product similarity.

5.6 File Upload Module

It is used to view the details of the server and upload the secured files using this module. 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. The admin can upload the file after the conversion of the Zip file format.

6. CONCLUSION

The first time we define and solve the problem of multi-keyword ranked ontology keyword mapping and search over encrypted cloud data, and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient principle of “coordinate matching”, i.e., as many matches as possible, to effectively capture similarity between query keywords and outsourced documents, and use “inner product similarity” to quantitatively formalize such a principle for similarity measurement.

For meeting the challenge of supporting multi-keyword semantic without privacy breaches, we first propose a basic EARM scheme using secure inner product computation, and significantly improve it to achieve privacy requirements in two levels of threat models. The proposed system analyse the investigating privacy and efficiency of this module develops the authentication process and introduces thelow overhead on both computation and communication. As our future work, we will explore supporting other multi-keyword semantics (e.g., weighted query) over encrypted data, integrity check of rank order in search result and privacy guarantees in more stronger threat model.

REFERENCES

1 L. M. Vaquero and L. Rodero-Merino “A breal in the clouds: towards a cloud definition,” ACM SIGCOMM Comput. Commun. Rev., vol. 39 no. 1, pp. 50–55, 2015.

2]S. Kamara and K. Lauter, “Cryptographic cloud storage,” in RLCPS, January 2016, LNCS. Springer, Heidelberg.

3 A. Singhal “Modern information retrieval: A brief overview,” IEEE Data Engineerin Bulletin, vol. 24, no. 4, pp. 35–43, 2014.

4 I. H. Witten, A. Moffat, and T. C. Bell “Managing gigabytes: Compressing anc indexing documents and images,” Morgai Kaufmann Publishing, San Francisco, May 2016

5 D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. of S&P, 2015

6 E.-J. Goh, “Secure indexes,” Cryptology ePrint Archive, 2016, http:// eprint.iacr.org/2016.

7 Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remot encrypted data,” in Proc. of ACNS, 2015.

8 R. Curtmola, J. A. Garay, S. Kamara, and R Ostrovsky, “Searchable symmetric encryption improved definitions and efficien constructions,” in Proc. of ACCCS
2014.

9 D. Boneh, G. D. Crescenzo, R. Ostrovsky, anc G. Persiano, “Public key encryptionwitl keyword search,” in Proc. of EUROCRYPT 2015.

10 M. Bellare, A. Boldyreva, and A. ONeill, “Deterministic and efficiently searchable encryption,” in Proc. of CRYPTO, 2016.