International Journal of Computational Science, Mathematics and Engineering
Volume-4-Issue-4-April-2017
ISSN-2349-8439

Enhanced Secure Ranked Search Using Multi-Keyword In Cloud Computing

Dr.S.Jumlesha [1]*,Chanu V S Divya [2],K.Manohar [3]

Abstract
Cloud computing provides various computing over the internet. Data owners are induce to store their data from local sites to the commercial public cloud for great flexibility and economic savings. But for providing security for sensitive data is challenging issue. To provide security for data have to be encrypted before storing data into the cloud, the conventional data usage service based on plaintext keyword search. Regarding the large number of data users and documents in the cloud, we use several multi keyword semantics and choose an effective similarity measure of “Coordinate matching” .The more number of matches gives the related data documents to the search query. In this paper we propose a novel approach Enhanced Secure Ranked Search using multi keyword over encrypted cloud data (MRSE) scheme for effective search. The complete analysis of these schemes provides efficient search.

Keywords
multi keyword over encrypted cloud data (mrse), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)

[1] *Professor in CSE,VITS-Hyderabad*
[2] *PG Scholar, Department of CSE,SANK-Gudur, Nellore*
[3] *Assistant Professor (SL), Department of CSE, SANK-Gudur, Nellore.*

Contents

1. Introduction

Cloud computing is an emerging computing standard, in which resources of the computing infrastructure are provided as services. The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.
The cloud is usually opaque to the end uas the end user does not have to manage the core technology. The end user’s only duty is to use the resources from the cloud on demand and upon predefined terms.

Figure 1. Cloud Computing

Cloud computing enables companies to consume compute resources as a utility just like electricity rather than having to build and maintain computing infrastructures in-house.

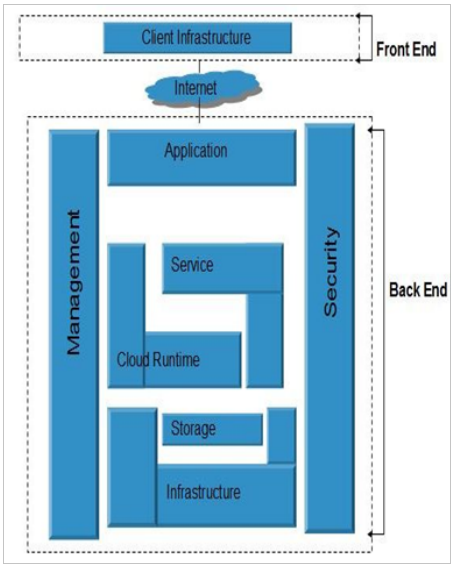

Figure 2. Architecture of cloud computing

2. ARCHITECTURE OF CLOUD COMPUTING

The Cloud Computing architecture comprises of many cloud components, each of them is loosely coupled. We can broadly divide the cloud architecture into two parts:

* Front End
* Back End

Each of the ends is connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:

Front End

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.

Back End:

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

• It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.

• The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.

3. CLOUD DEPLOYMENT MODELS

Deployment models define the type of access to the cloud, i.e., how the cloud is located. Cloud can have any of the four types of access:

* Public
* Private
* Hybrid
* Community

Figure 3. Cloud deployment Models

Public Cloud: The Public Cloud allows systems and services to be easily accessible to general public, e.g., Google, Amazon; Microsoft offers cloud services via Internet. A public cloud is a publicly accessible cloud environment owned by a third-party cloud provider. The resources are generally offered to cloud consumers at a cost. The cloud provider is responsible for the creation and on-going maintenance of the public cloud and its IT resources.

Benefits: * Cost Effective
* Reliability
* Flexibility
* Location Independence
* Utility style costing
* High Scalability

In public cloud model, data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.

Private Cloud: The Private Cloud allows systems and services to be accessible within an organization. The Private Cloud is operated only within a single organization. However, it may be managed internally or by third-party.A private cloud is owned by a single organization.

Private clouds enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different parts, locations, or departments of the organization. There are many benefits of deploying cloud as private cloud model. Private clouds have more control on its resources and hardware than public cloud because it is accessed only within an organization.

Hybrid Cloud: The Hybrid Cloud is a mixture of public and private cloud. Non-critical activities are performed using public cloud while the critical activities are performed using private cloud.

The hybrid cloud model is dependent on internal IT infrastructure; therefore it is necessary to ensure redundancy across data centers.

Community Cloud: The Community Cloud allows system and services to be accessible by group of organizations. It

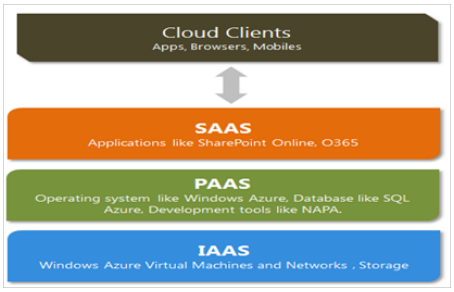

Figure 4. Cloud Service Models

shares the infrastructure between several organizations from a specific community. It may be managed internally or by the third-party. Community cloud provides an infrastructure to share cloud resources and capabilities among several organizations. Community cloud is comparatively more secure than the public cloud.

* Since all data is housed at one location, one must be careful in storing data in community cloud because it might be accessible by others.
* It is also challenging to allocate responsibilities of governance, security and cost.

4. CLOUD SERVICE MODELS

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Infrastructure as a Service (IaaS):
IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Platform as a Service (PaaS):
PaaS provides the runtime environment for applications, development & deployment tools, etc.

Software as a Service (SaaS): SaaS model allows using software applications as a service to end users.

5. Implementation

Implementation is an important phase in the system development process. The goal is to translate the design of the system produced during the design phase into source code.

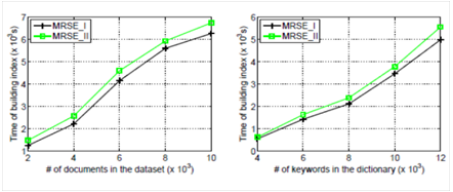

Figure 5. a) Time cost of building Index for n=400 b) Time cost of building Index for m=1000

Algorithm:

Notation-

Step 1:F—the plaintext document collection, denoted as a set of m data documents **F=(F_1,F_2,...., Fm).**

Step 2:C—the encrypted document collection stored in the cloud server, denoted as **C=(C_1, C_2, . . . , Cm).**

Step 3:W—the dictionary, i.e., the keyword set consisting of n keyword, denoted as **W =(W_1,W_2,...,Wn).**

Step 4:I—the searchable index associated with **C**, denoted as **(I_1,I_2,... Im)** where each sub index **Ii** is built for **Fi**.

Step 5: $\widetilde{W}$ the subset of W, representing the keywords in a search request, denoted as f $\widetilde{W}$=(W_{i1};W_{i2} ; . . . ;W_{it}). .

Step 6:T $\widetilde{W}$ —the trapdoor for the search request $\widetilde{W}$. .

Step 7:F $\widetilde{W}$ —the ranked id list of all documents according to their relevance to $\widetilde{W}$.

6. EXPERIMENTAL RESULTS

The major computation to generate a sub index in MRSE I includes the splitting process and two multiplications of a (n + 2) × (n + 2) matrix and a (n + 2) 2). Fig.5(a) shows that the time to generate a trapdoor is greatly affected by the number of keywords in the dictionary. Like index construction, every trapdoor generation incurs two multiplications of a matrix and a split query vector, where the dimensionality of matrix or query vector is different in two proposed schemes and becomes larger with the increasing size of dictionary. Fig.5(b) demonstrates the trapdoor generation cost in the MRSE II scheme is about 20 percentages larger than that in the MRSE I scheme. Like the sub index generation, the difference of costs to generate trapdoors is majorly caused by the different dimensionality of vector and matrices in the two MRSE schemes. More importantly, it shows that the number of query keywords has little influence on the overhead of trapdoor generation, which is a significant advantage over related works on multi-keyword searchable encryption.

7. Conclusion

In this paper, a new framework is proposed for the problem of multi-keyword ranked search over encrypted cloud

data, and to establish a variety of privacy requirements. Among various multi-keyword semantics, the efficient similarity measure is "coordinate matching", i.e., as many matches are possible, to effectively capture the relevance of outsourced documents to the query keywords, and use "inner product similarity" to quantitatively evaluate such similarity measure. For meeting the challenge of supporting multi-keyword semantic without privacy breaches, MRSE framework is proposed using secure inner product computation. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset shows our proposed scheme introduces low overhead on both computation and communication.

References

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

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, 2010.

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

[7] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive http://eprint.iacr.org/2003/216. 2003

[8] 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.

[9] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous Ibe, and Extensions," J. Cryptology, vol. 21, no. 3, pp. 350- 391, 2008.